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»

ТРИНАДЦАТАЯ
ВСЕРОССИЙСКАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 30 октября – 1 ноября 2024 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИИ

МГТУ им. Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2024

УДК 003.26.7:004.05
ББК 32.937.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов XIII всероссийской научно-технической конференции "Безопасные информационные технологии" – М.: МГТУ им. Н.Э.Баумана, 2024. 237 с. – илл.

ISBN 978-5-6045553-9-2

Сборник содержит тезисы докладов, представленных на XIII всероссийской научно-технической конференции "Безопасные информационные технологии" (БИТ-2024), проходившей 30 октября – 1 ноября 2024 г. в рамках всероссийского конгресса с международным участием «Русский инженер» 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;
Вареница 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 004.056.5

Правовые и организационно-технические меры информационной безопасности применительно к разработке и внедрению медицинских систем с технологиями искусственного интеллекта

Аксенов К.Д.[1]

Медицинские информационные системы (МИС), в которые встроены технологии искусственного интеллекта, собирают, обрабатывают и хранят конфиденциальные данные пациентов, включая медицинские изображения и результаты диагностики, в связи с чем защита данных является критическим аспектом при разработке и внедрении медицинских информационных систем. В настоящей работе приводится обзор существующих правовых и организационно-технических мер обеспечения информационной безопасности для медицинских информационных систем, а также результат проектирования системы безопасности платформы EyeTech для скрининга и диагностики офтальмологических заболеваний с использованием технологий искусственного интеллекта.

Ключевые слова: медицинская информационная система (МИС), информационная безопасность, медицинские данные, шифрование данных

Введение

Цифровое здравоохранение может революционизировать способ оказания медицинских услуг, особенно в условиях ограниченных ресурсов. Однако для успешного внедрения необходимо решать проблемы безопасности данных, конфиденциальности, цифрового неравенства и регулирования [1]. цифровые решения в области здравоохранения включают в себя телемедицину, мобильное здравоохранение, носимые технологии и биосенсоры, электронные медицинские карты, искусственный интеллект и машинное обучение [2-4]. Медицинские информационные системы (МИС), позволяют осуществлять мониторинг и проверку состояния пациентов, а также управлять медицинскими данными [5]. В то же время внедрение цифровых медицинских решений приводит к увеличению рисков в области безопасности конфиденциальных данных пациентов. Согласно данным HIPAA Journal, только в 2020 году в Соединенных Штатах было зарегистрировано 642 утечек медицинских данных, что привело к несанкционированному доступу к более чем 30 миллионам медицинских записей [6]. В конце октября 2023 года стало известно об утечке данных одной из клиник сети «РЖД-Медицина», а также таких сетей медлабораторий, как «Хеликс», KDL, «Ситилаб», сети аптек «Вита». Кроме того, киберпреступниками в интернет были выложены сотни документов, связанных с разработкой и клиническими испытаниями вакцины «Спутник V» [7]. Защита данных является критическим аспектом при разработке и внедрении медицинских информационных систем в виду того, что отсутствие доверия, вызванное подобными инцидентами, может привести к снижению заинтересованности пациентов к организации [8]. Таким образом, защита данных является критическим аспектом при разработке и внедрении медицинских информационных систем и включает использование безопасных технологий для хранения и передачи данных, внедрение контроля доступа и обучение медицинских работников передовым практикам обеспечения безопасности и конфиденциальности пациентов. Кроме того, обеспечение безопасности и конфиденциальности медицинских данных, включая конфиденциальность, целостность и доступность, являются необходимым условием для достижения высококачественных медицинских услуг.

Предыдущими этапами настоящего исследования являлось создание цифровой платформы EyeTech для скрининга и диагностики офтальмологических заболеваний с использованием технологий искусственного интеллекта [9-11]. Целью настоящей работы является разработка системы безопасности медицинской платформы EyeTech. Для осуществления поставленной цели были решены такие задачи, как: обзор существующих правовых и организационно-технических мер

[1] Аксенов Кирилл Дмитриевич, CCNP Security, Microsoft Certified: Security Engineer, ООО "Пространство интеллектуальных решений", Новороссийск, axenov.kir@gmail.com

обеспечения информационной безопасности, а также проектирование системы безопасности платформы.

Правовые аспекты обеспечения информационной безопасности

Разработка и внедрение медицинских систем должны соответствовать ряду нормативных актов в области защиты персональных данных и медицинской информации. Ключевые законы и стандарты включают:

- Федеральный закон №152-ФЗ "О персональных данных" — регламентирует обработку персональных данных, включая обязательные меры по их защите.
- Федеральный закон №149-ФЗ "Об информации, информационных технологиях и о защите информации" — касается вопросов правовой охраны информации, включая медицинские данные.
- ГОСТ Р 57580-2017 — стандарт по защите персональных данных при их обработке в информационных системах.
- Приказы ФСТЭК и ФСБ России по защите информации.
- Международные стандарты (ISO/IEC 27001, GDPR и другие).
- Указ Президента Российской Федерации от 01.05.2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

Кроме того, согласно законам РФ и международным стандартам, медицинские данные относят к категории особо защищаемой информации, в связи с чем, внедрение платформы EyeTech требует строгого соблюдения законодательства и нормативных документов [12, 13]. Сертификация платформы организациями, которые уполномочены на проведение аттестации, а именно - ФСТЭК России и Федеральной службой безопасности Российской Федерации, позволяет подтвердить соответствие системы безопасности платформы требованиям.

Еще одним правовым аспектом обеспечения информационной безопасности является политика конфиденциальности, которая четко определяет порядок сбора, хранения и обработки медицинской информации. Кроме того, в медицинских организациях важной составляющей является повышение осведомленности персонала об информационной безопасности путем проведения регулярных тренингов и семинаров, распространения информационных материалов и руководств по информационной безопасности.

Организационно-технические меры для обеспечения информационной безопасности

К организационным мерам можно отнести внедрение политики безопасности, назначение ответственных лиц и обеспечение регулярных аудитов безопасности. Техническими мерами обеспечения информационной безопасности являются шифрование данных, многофакторная аутентификация и разграничение прав доступа. Использование перечисленных мер будет зависеть от этапа жизненного цикла продукта (табл. 1). Так, на стадии разработки важно провести анализ требований безопасности и построить архитектуру системы, которая бы учитывала все необходимые меры защиты, включая шифрование данных и стеганографию. На этапе внедрения основной акцент делается на тестирование системы на уязвимости, включая выполнение внешних и внутренних проверок безопасности. Кроме того, внедрение системы безопасности должно сопровождаться обучением персонала. Основное внимание на этапе эксплуатации готового решения уделяется поддержке системы безопасности в актуальном состоянии, мониторингу инцидентов и проведению регулярных аудитов. важными аспектами также являются резервное копирование и управление инцидентами информационной безопасности.

Таблица 1.

Применение мер защиты информации на разных этапах жизненного цикла медицинской информационной системы

Меры защиты информации	Разработка	Внедрение	Эксплуатация
Разработка политики безопасности	+	+	+
Назначение ответственных лиц	+	+	+
Обучение персонала	+	+	+
Безопасное проектирование (Secure Design)	+		
Разработка с учетом безопасности	+		
Тестирование безопасности	+	+	+
Интеграция инструментов безопасности	+	+	
Планирование развертывания		+	

Меры защиты информации	Разработка	Внедрение	Эксплуатация
Контроль доступа к инфраструктуре		+	+
Конфигурация системы безопасности	+	+	
Тестирование перед запуском	+	+	
Шифрование данных		+	+
Алгоритмы стеганографии	+	+	+
Механизмы аутентификации и авторизации			+
Резервное копирование и восстановление			+
Обновление и управление патчами			+
Управление инцидентами			+
Периодическое тестирование			+
Мониторинг и аудит			+

Проектирование системы обеспечения информационной безопасности медицинской платформы EyeTech.

Цифровая медицинская платформа EyeTech позволяет получать данные с офтальмологических приборов, из медицинских информационных систем, а также обеспечивает ручной ввод данных (рис. 1). Встроенные технологии ИИ реализуют автоматизированный анализ данных и помогают врачам в постановке диагнозов (рис. 2). Также одним из компонентов является чат-бот, основанный на LSTM, который помогает пациентам получать предварительные консультации. Таким образом, разработанный прототип МИС позволяет:

- Снизить риск причинения вреда пациентам за счёт ускоренного предоставления актуальной информации.
- Обеспечить преемственность медицинской помощи, за счет доступа к данным предыдущих посещений.
- Снизить стоимость медицинской помощи, за счет исключения дублирования услуг.
- Увеличить пропускную способность медицинских учреждений.
- Повысить достоверность данных за счёт автоматизации процесса ввода и обработки данных.
- Сократить время на оформление медицинской документации.

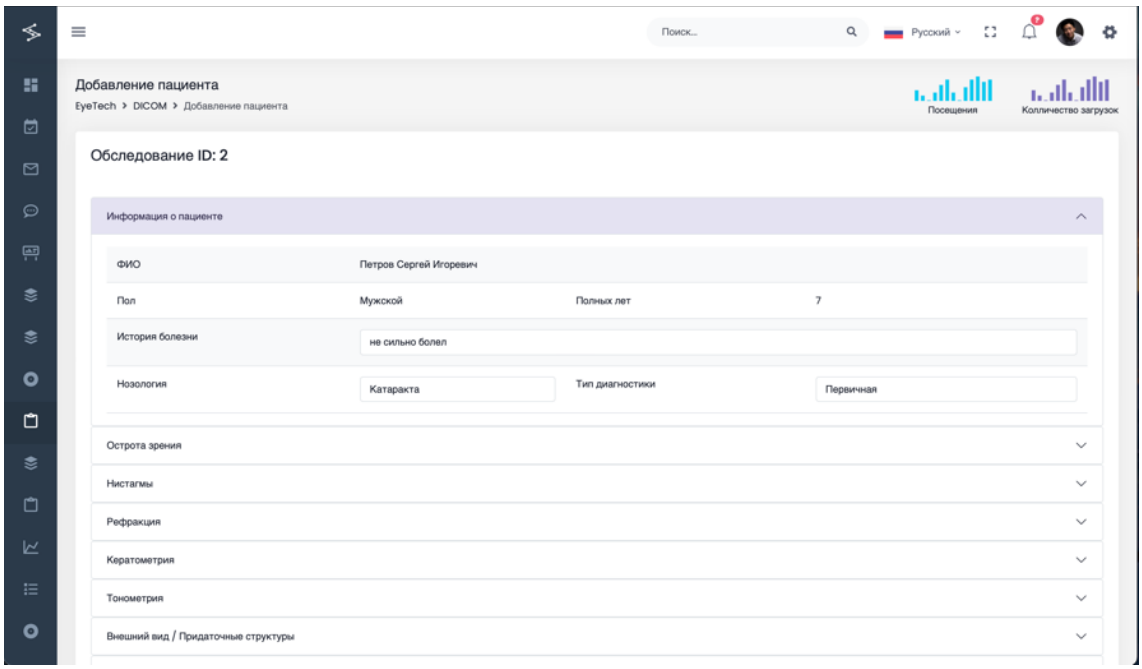


Рис.1. Интерфейс формы ввода данных обследования пациента платформы EyeTech.

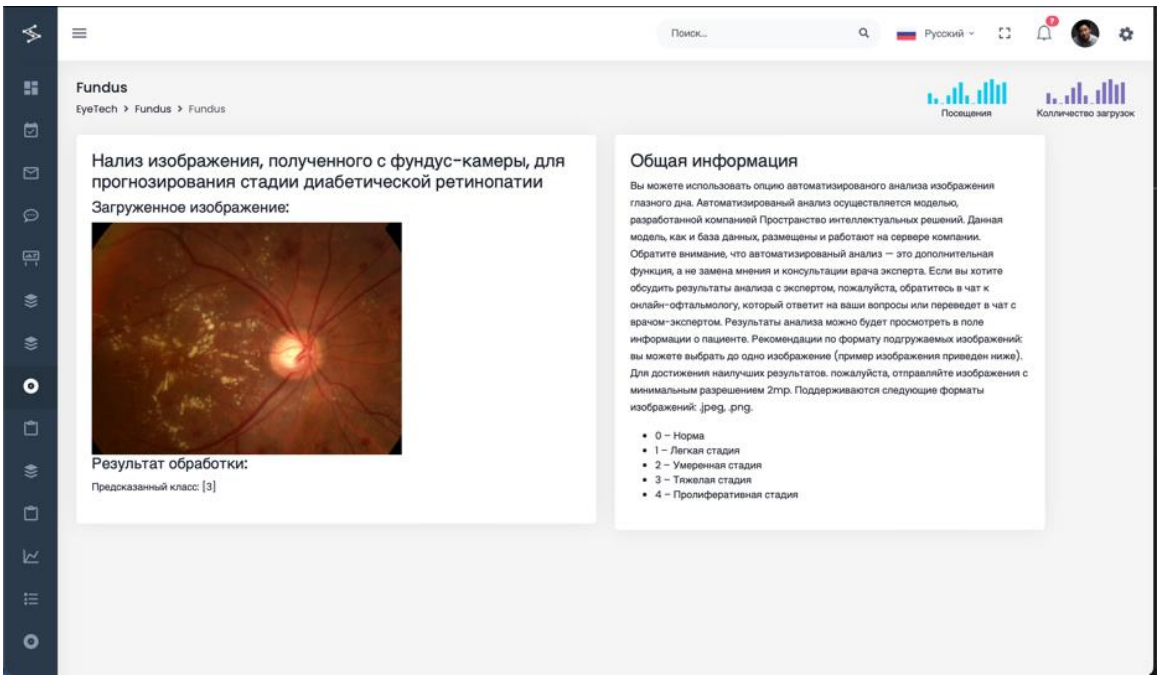


Рис.2. Интерфейс модуля оценки диабетической ретинопатии с использованием технологий искусственного интеллекта по изображению глазного дна.

Для обеспечения безопасности платформы была разработана система безопасности, которая включает защищенный канал связи, модуль деперсонализации, а также аутентификацию пользователя в системе с разграничением прав доступа. На рисунке 3 отображен процесс передачи данных в платформе. Посредством модуля получения данных, данные с медицинских диагностических приборов, МИСа и данные, введенные врачом вручную, передаются по защищенному каналу связи в модуль оценки качества данных, где происходит автоматическое распознавание типов данных, фильтрация данных по значимости, идентификация конфиденциальной информации, деперсонализация данных и оценка полноты данных. Затем данные передаются в систему хранения данных, где, после обработки модулем деперсонализации, хранятся в обезличенном виде. Хранилище данных позволяет получить доступ к данным по запросу, который реализуется согласно ролевому доступу. При этом уровень доступа определяется по средством аутентификации пользователя в системе. Данные из системы хранения могут поступать в витрину приложений, где может быть произведена их маркировка в модуле маркировки данных, визуализация, а также обработка с помощью моделей машинного обучения в сервисах на основе технологий искусственного интеллекта. Система аутентификации пользователей позволяет, в зависимости от прав доступа, получать и загружать данные в систему, обрабатывать данные и использовать сервисы.

Выводы

Внедрение и эксплуатация медицинских информационных систем, таких как EyeTech, требуют комплексного подхода к обеспечению информационной безопасности, включающего как правовые, так и организационно-технические меры. Эффективная защита медицинских данных на всех этапах жизненного цикла медицинских информационных систем достигается за счёт использования современных методов шифрования, аутентификации, регулярного тестирования безопасности и мониторинга системы. В настоящей работе была разработана схема обеспечения информационной безопасности платформы EyeTech, которая включает защищенный канал связи, модуль деперсонализации, а также аутентификацию пользователя в системе с разграничением прав доступа.

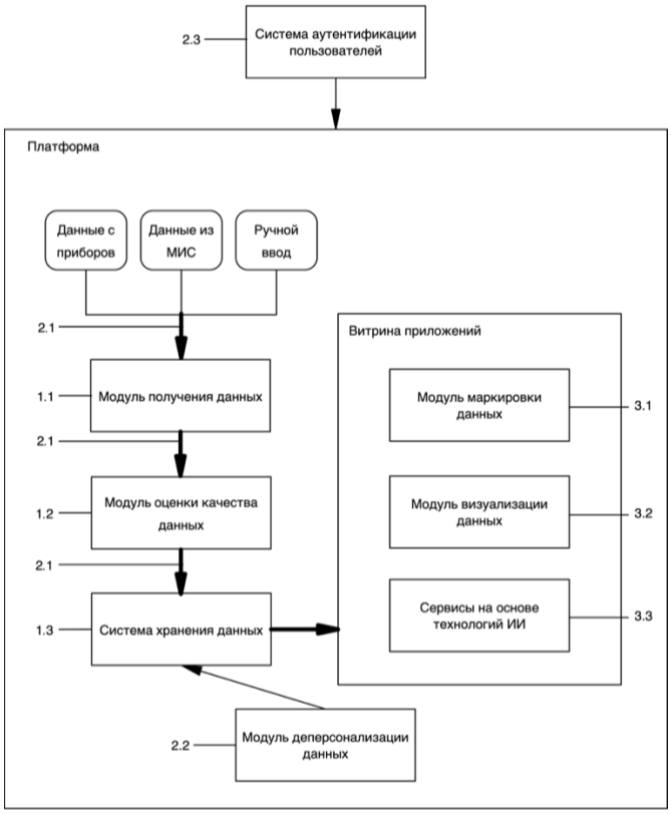


Рис 3. Схема взаимодействия модулей платформы EyeTech.
(1.1) модуль получения данных, (1.2) модуль оценки качества данных, (1.3) система хранения данных, (2.1) защищенный канал связи, (2.2) модуль деперсонализации, (2.3) система аутентификации пользователей, (3.1) модуль маркировки данных, (3.2) модуль визуализации, (3.3) модуль обработки данных с помощью моделей машинного обучения.

Литература

1. *Hill C, Martin JL, Thomson S, Scott-Ram N, Penfold H, Creswell C. Navigating the challenges of digital health innovation: considerations and solutions in developing online and smartphone-application-based interventions for mental health disorders. Br J Psychiatry. 2017 Aug;211(2):65-69. doi: 10.1192/bjp.bp.115.180372. Epub 2017 May 18. PMID: 28522435.*
2. *Применение смарт-карт в телемедицинских системах / Булдакова Т.И., Ланцберг А.В., Смолянинова К.А. // Вопросы кибербезопасности. 2017. № 4 (22). С. 40-46.*
3. *Система телемедицины с предварительным шифрованием биометрической информации / Горшков Ю.Г., Каиндин А.М., Веряев А.С. и др. // Вопросы кибербезопасности. 2015. № 5 (13). С. 63-69.*
4. *Fagherazzi G, Goetzinger C, Rashid MA, Aguayo GA, Huiart L. Digital Health Strategies to Fight COVID-19 Worldwide: Challenges, Recommendations, and a Call for Papers. J Med Internet Res. 2020 Jun 16;22(6):e19284. doi: 10.2196/19284. PMID: 32501804; PMCID: PMC7298971.*
5. *R. Dadlani, S. Mani, G A UJ, et al. The impact of telemedicine in the postoperative care of the neurosurgery patient in an outpatient clinic: a unique perspective of this valuable resource in the developing world--an experience of more than 3000 teleconsultations // World Neurosurg, 82 (3–4) (2004), pp. 270-283, 10.1016/j.wneu.2014.05.027*
6. *J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marques. Setting Privacy by Default in Social IoT: Theorizing the Challenges and Directions in Big Data Research// Big Data Research.vol. 25, p. 100245, Jul. 2021, doi:10.1016/j.bdr.2021.100245*

7. Утечки данных в медицинских учреждениях. [Электронный ресурс] / Режим доступа: https://www.tadviser.ru/index.php/Статья:Утечки_данных_в_медицинских_учреждениях. – Дата доступа: 9.09.2024.

8. Qayyum, A. : Qadir, J. ; Bilal, M. ; Al-Fuqaha, A Secure and Robust Machine Learning for Healthcare: A Survey. IEEE Rev. Biomed. Eng. 2020, 14, 156-180.

9. Malyugin B, Sakhnov S, Izmailova S, Boiko E, Pozdeyeva N, Axenova L, et al. Keratoconus diagnostic and treatment algorithms based on machine-learning methods. Diagnostics (Basel). 2021;11(10):1933. DOI: 10.3390/diagnostics11101933 EDN: QMZRYU

10. Разработка модели скрининга катаракты с использованием открытого набора данных и алгоритмов глубокого машинного обучения / С. Н. Сахнов, К. Д. Аксенов, Л. Е. Аксенова [и др.] // Офтальмохирургия. – 2022. – № S4. – С. 13-20. – DOI 10.25276/0235-4160-2022-4S-13-20. – EDN VEGPAW.

11. Разработка и тестирование автоматизированной системы анализа ОКТ изображений сетчатки / Л. Е. Аксенова, К. Д. Аксенов, Е. В. Козина, В. В. Мясникова // Доклады Российской академии наук. Математика, информатика, процессы управления. – 2023. – Т. 514, № 2. – С. 169-176. – DOI 10.31857/S2686954323601938. – EDN XQPVTL.

12. Гулиев, Я. И. Обеспечение информационной безопасности в медицинских организациях / Я. И. Гулиев, А. А. Цветков // Врач и информационные технологии. – 2016. – № 6. – С. 49-62. – EDN XBSEWL.

13. Гусев А.В., Морозов С.П., Кутичев В.А., Новицкий Р.Э. Нормативно-правовое регулирование программного обеспечения для здравоохранения, созданного с применением технологий искусственного интеллекта, в Российской Федерации. Медицинские технологии. Оценка и выбор. 2021;(1):36-45.

Legal and organizational-technical measures of information security applicable to the development, implementation, and use of EyeTech systems

Aksenov K.D.[2]

Abstract. Medical information systems (MIS), which integrate artificial intelligence technologies, collect, process, and store patients' confidential data, including medical images and diagnostic results. As a result, data protection becomes a critical aspect in the development and implementation of medical information systems. This paper provides an overview of the existing legal and organizational-technical measures to ensure information security in medical information systems, as well as the result of designing the security system for the EyeTech platform for screening and diagnosing ophthalmic diseases using artificial intelligence technologies.

Keywords: medical information system (MIS), information security, medical data, data encryption

[2] Aksenov Kirill Dmitrievich, CCNP Security, Microsoft Certified: Security Engineer, LLC "Predict space", Novorossiysk, axenov.kir@gmail.com

УДК 004.4

Контур разработки безопасного программного обеспечения

Арустамян С.С.[3], Антипов И.С.[4]

В данной статье представлен подход к созданию контура разработки безопасного ПО, который применяется для создания инфраструктуре по разработке ПО, предусматривающая предотвращение появления проблем безопасности, а также их эффективное обнаружение и устранение. Разработка безопасного ПО на данный момент в Российской Федерации применяется в соответствии с требованиями ГОСТ Р 56939-2016.

Ключевые слова: Разработка безопасного ПО, статический анализ, динамический анализ, фаззинг-тестирование, композиционный анализ.

Введение

В настоящее время разработка безопасного ПО становится все более актуальной задачей. Это связано с тем, что все больше разработчиков обращают внимание не только на оптимизацию и функциональные возможности продуктов, но и о их безопасности. Данная проблема широко освещается в различных источниках. Например, в источниках [1-4] подробно расписываются конкретные методики внедрения процессов разработки безопасного ПО. В работах [2, 5-11] отмечается необходимость минимизации различных проблем безопасности, которые возникают на этапе разработки.

Циклы SDLC и SSDLC

SDLC (Software Development Life Cycle) – это процесс разработки программного обеспечения, который включает в себя последовательность этапов, начиная от планирования и заканчивая тестированием и сопровождением продукта.

Цикл SDLC состоит из следующих этапов:

- анализ требований;
- проектирование архитектуры;
- разработка ПО;
- тестирование;
- развертывание;
- эксплуатация.

Анализ требований подразумевает процесс выявления, определения и документирования требований к разрабатываемому продукту. Планирование подразумевает процесс определения требований к проекту, подготовки бюджета и составление плана разработки. Проектирование архитектуры подразумевает процесс продумывания всей архитектуры продукта в детализированном виде. Разработка программного обеспечения подразумевает процесс написания кода и создания системы на основе требований и архитектуры. Тестирование подразумевает процесс проверки продукта на предмет несоответствий заявленным требованиям. Развертывание подразумевает процесс установки и настройки программного обеспечения, создание баз данных, конфигурирование сетевых настроек и другие действия, необходимые для работы приложения или системы. Эксплуатация подразумевает процесс технической поддержи ПО, а также процесс обновления ПО в случае внесения изменений.

Как можно заметить, в данном цикле упор делается, в первую очередь, на саму разработку, так как она и является основной задачей. Вопросы информационной безопасности отдельно не рассматриваются. Соответственно, если мы говорим про разработку безопасного ПО, то этот цикл необходимо доработать, добавив в него аспекты, связанные с безопасностью. Таким образом, цикл SSDLC – это цикл SDLC, в который добавили специфические методы, которые связаны с обеспечением безопасности. Более подробно данные методы указаны в таблице ниже (табл. 1).

[3] Арустамян Сас Сергеевич, старший преподаватель, МГТУ им. Н.Э.Баумана, НПО «Эшелон», Москва, sa@cnpo.ru

[4] Антипов Илья Сергеевич, аспирант, МГТУ им. Н.Э.Баумана, НПО «Эшелон», Москва, i.antipov@npo-echelon.ru

Таблица 1.

Дополнительные меры в цикле SSDLC в соответствии с ГОСТ Р 56939-2016

Этап ЖЦ ПО	**№ меры**	**Описание меры**
Анализ требований	1.1	Разработчик ПО должен определить требования по безопасности к разрабатываемому ПО
Проектирование архитектуры	2.1	Разработчик ПО должен реализовать моделирование угроз безопасности информации
	2.2	Разработчик ПО должен реализовать проект архитектуры программы с учетом результатов моделирования угроз безопасности информации
Разработка ПО	3.1	Разработчик ПО должен идентифицировать каждое инструментальное средство, используемое при разработке ПО, и определить его настройки (опции), применяемые при создании программы
	3.2	Разработчик ПО должен создавать программу на основе проекта архитектуры программы, определенного в ходе выполнения процессов проектирования архитектуры программы
	3.3	Разработчик ПО должен создать (выбрать) и использовать при создании программы порядок оформления исходного кода программы, содержащий перечень правил и рекомендаций, направленных на устранение недостатков программы (потенциально уязвимых конструкций) в исходном коде программы
	3.4	Разработчик ПО должен обеспечить проведение статического анализа исходного кода программы с целью выявления недостатков программы (потенциально уязвимых конструкций) в исходном коде программы
	3.5	Разработчик ПО должен обеспечить проведение периодической экспертизы исходного кода программы
Тестирование	4.1	Разработчик ПО должен проводить функциональное тестирование программы для того, чтобы определить, выполняются ли требования безопасности, идентифицированные в процессе анализа требований к ПО
	4.2	Разработчик ПО должен обеспечить проведение тестирования на проникновение в отношении программы с целью выявления ее уязвимостей
	4.3	Разработчик ПО должен обеспечить проведение динамического анализа кода программы с целью выявления уязвимостей программы
	4.4	Разработчик ПО должен обеспечить проведение фаззинг-тестирования программы с целью выявления уязвимостей программы
Развертывание	5.1	Разработчик ПО должен применять технические и организационные меры, необходимые для обнаружения модификации ПО или любого расхождения между оригиналом и версией, полученной пользователем

Этап ЖЦ ПО	№ меры	Описание меры
	5.2	В состав поставляемого ПО должны быть включены эксплуатационные документы в объеме, достаточном для правильной настройки и безопасного применения программы
Эксплуатация	6.1	Разработчик ПО должен реализовать процедуру, позволяющую выполнять отслеживание и исправление обнаруженных ошибок ПО и уязвимостей программы
	6.2	Разработчик ПО должен предложить пользователю решение проблемы в ситуации, когда неизвестная ранее уязвимость программы используется для проведения компьютерной или сетевой атаки на ИС пользователя
	6.3	В экстренных ситуациях разработчик ПО должен быть способен к выпуску обновлений ПО в обход стандартной процедуры выпуска новых версий ПО
	6.4	Разработчик ПО должен проводить систематический поиск уязвимостей программы
	6.5	При выполнении модернизации ПО (выпуска обновления ПО) в отношении измененного ПО должны выполняться меры по разработке безопасного ПО

Инструменты, применяемые при разработке безопасного ПО

Требования к разработке безопасного ПО подразумевают под собой как организационные, так и технические меры. Помимо регламентов, которые необходимы для каждого из внедряемых мер, контур разработки также должен содержать инструменты для реализации конкретных требований.

Таблица 2.

Используемые инструменты в цикле SSDLC

Этап ЖЦ ПО	№ меры	Используемые инструменты	Пример инструментов
Анализ требований	1.1	–	–
Проектирование архитектуры	2.1	–	–
	2.2	–	–
Разработка ПО	3.1	–	–
	3.2		
	3.3	Линтеры	ESLint, Pylint, Cppcheck
	3.4	Статический анализатор	АК-ВС 3, Sonarqube, Horusec
	3.5	Интегрированная среда разработки	Visual Studio Code, JetBrains IDE, Эшелониум
Тестирование	4.1	–	–
	4.2	Инструменты тестирования на проникновение	Burp Suite, sqlmap, Metasploit
	4.3	Сканеры безопасности, инструменты динамического анализа	Сканер-ВС, Nessus, Nmap, АК-ВС 3
	4.4	Фаззер	АК-ВС 3, AFL, Libfuzzer
Развертывание	5.1	Средства контрольного суммирования	ФИКС, Трафарет, gostsum (Astra Linux)

Этап ЖЦ ПО	№ меры	Используемые инструменты	Пример инструментов
	5.2	–	–
Эксплуатация	6.1	Инструменты отслеживания ошибок	Jira, Redmine, Azure DevOps
	6.2	–	–
	6.3	–	–
	6.4	Инструменты композиционного анализа	OWASP Dependency-Check, OWASP Dependency-Track
	6.5	–	–

Вывод

Контур разработки безопасного ПО подразумевает внедрение в инфраструктуру разработчика инструментов, позволяющих эффективно бороться с различными проблемами безопасности, которые возникают по вине разработчика на этапе создания продукта.

Литература

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

2. Барабанов А.В., Вареница В.В., Марков А.С. Аудит безопасности программ Учебно-методическое пособие / Москва, МГТУ им. Н.Э. Баумана, 2021.

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

4. 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.

5. 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.

6. 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.

7. Марков А.С. Актуальные вопросы разработки безопасного программного обеспечения. // Сб. научных трудов Всероссийской научно-технической конференции «Кибернетика и информационная безопасность «КИБ-2023». Москва, НИЯУ МИФИ, 2023. С. 10–11.

8. 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.

9. 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.

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

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, профессор кафедры ИУ8 «Информационная безопасность» Марков А. С., a.markov@npo-echelon.ru

The secure software development contour

Arustamyan S.S.[5], Antipov I.S.[6]

This article presents an approach to creating a secure software development contour, which is used to create a software development infrastructure that provides for the prevention of security problems, as well as their effective detection and elimination. The development of secure software is currently used in the Russian Federation in accordance with the requirements of GOST R 56939-2016.

Keywords: Secure software development lifecycle, static analysis, dynamic analysis, fuzzing testing, compositional analysis.

[5] Arustamyan Sas Sergeevich, Moscow, Bauman MSTU, sa@cnpo.ru
[6] Antipov Ilya Sergeevich, Moscow, Bauman MSTU, i.antipov@npo-echelon.ru

УДК 004.056

Метод защиты облачной платформы «ГосТех» на основе кибериммунитета

Балябин А.А.[7]**, Петренко С.А.**[8]

В настоящей работе представлен и обоснован авторский метод защиты облачной платформы «ГосТех» на основе кибериммунитета. Этот метод позволяет не только обнаруживать и нейтрализовать ранее неизвестные компьютерные атаки злоумышленников в нотации MITRE ATT&CK, но и впервые восстанавливать цифровые сервисы упомянутой платформы в реальном масштабе времени.

Ключевые слова: облачные платформы, кибербезопасность, киберустойчивость угрозы безопасности информации, уязвимости облачных вычислений, компьютерные атаки злоумышленников, остаточные риски безопасности, управление рисками, противодействие кибератакам злоумышленников, кибериммунная система защиты, кибериммунитет.

Введение

Современные информационно-вычислительные системы развиваются в направлении внедрения облачных, туманных и пограничных вычислений, технологий интернета вещей (IoT) и иных технологий SmartGrid [1]. Растет и сложность программного обеспечения (ПО). Так ПО облачных платформ зачастую обладает сложной, многоуровневой, архитектурой (2/3/N-Tier), что может затруднить обеспечение его информационной безопасности [2-4].

Усложнение программного обеспечения неизбежно приводит к возникновению новых, ранее неизвестных уязвимостей «нулевого дня» (0-day). Так общее количество уязвимостей, выявленных в различном ПО за 2024 год, составило более 32 тыс., что на 12% превысило аналогичный показатель предыдущего года [4]. Информационно-технические воздействия (ИТВ), осуществляемые посредством эксплуатации уязвимостей «нулевого дня», представляют значимую угрозу информационной безопасности, поскольку они не могут быть своевременно обнаружены и предотвращены существующими классическими средствами защиты [5, 6].

В случае Российской Федерации отдельное внимание следует уделить объектам информатизации, относящимся к критической информационной инфраструктуре (КИИ), таким как, например, цифровые (облачные) сервисы Единой цифровой платформы (ЕЦП) «ГосТех» [4, 7, 8]. Аппаратно-программное обеспечение облачных платформ характеризуется высокой структурно-функциональной сложностью, что затрудняет обеспечение их информационной безопасности. Серьезную угрозу также представляет использование недоверенных иностранных технологий, потенциально содержащих программные закладки и уязвимости [7].

Анализ ряда научных работ [8-12] показал, что существующие методы и средства защиты зачастую не способны предотвратить возможные катастрофические последствия от реализации ИТВ на цифровые сервисы ЕЦП «ГосТех». В связи с этим возникает необходимость разработки нового интеллектуального метода защиты на основе кибериммунитета [2,3,10,13] для обеспечения требуемой устойчивости цифровых сервисов.

[7] Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», федеральная территория «Сириус», A.A.Balyabin@yandex.ru

[8] Петренко Сергей Анатольевич, руководитель группы, доктор технических наук, профессор, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Petrenko.SA@talantiuspeh.ru

Целью настоящей работы является разработка нового метода проактивной кибериммунной защиты облачной платформы «ГосТех»в условиях роста угроз безопасности.

Постановка задачи

Дано. Вычислительную программу цифрового сервиса платформы «ГосТех» возможно представить в виде машины Тьюринга (МТ) T [2-4]:

$$T = \langle Q, \Sigma, \Gamma, \delta, q_0, q_F \rangle, \quad (1)$$

где Q – конечное множество состояний МТ; Γ – множество допустимых символов ленты; $\Sigma \subseteq \Gamma$ – множество входных символов ленты; δ – функция переходов МТ; q_0 – начальное состояние МТ; q_F – конечное состояние МТ.

Единую цифровую платформу «ГосТех» представим в виде универсальной машины Тьюринга (УМТ) большой вложенности [16]:

$$U_i = \left(\{U_{i-1,j}\}, \{L_{вх_{i-1,j}}\}, \{L_{вых_{i-1,j}}\} \right), \; j = \overline{1..n}, \quad (2)$$

где $\{U_{i-1,j}\}$ – множество МТ $(i-1)$-го уровня; $\{L_{вх_{i-1,j}}\}$ – множество языков входных данных МТ $(i-1)$-го уровня; $\{L_{вых_{i-1,j}}\}$ – множество языков выходных данных МТ $(i-1)$-го уровня. Таким образом, УМТ i-го уровня принимает на вход n УМТ $(i-1)$-го уровня с их входными данными и возвращает выходные данные машин.

Язык входных данных МТ определим как:

$$L_{вх} = \{ w \mid w \in \Sigma^*, (q_0, \alpha, 0) \mapsto_T^* (q_F, \alpha, i) \}, \quad (3)$$

где тройка (q, α, i) обозначает конфигурацию МТ. При этом, будем считать, что $L_{вх}$ содержит подъязык входных данных $L_{вх}^-$, приводящих к нарушениям: $L_{вх} = L_{вх}^+ \bigcup L_{вх}^-$, как показано на рис. 1.

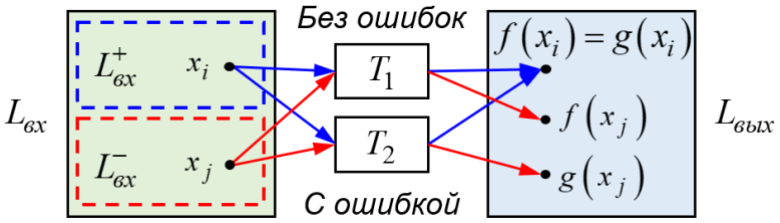


Рис. 1. Графическая интерпретация нарушения семантики

Поскольку МТ реализует алгоритм, а одной из моделей алгоритма является граф потока управления (ГПУ), обозначим его как:

$$\Gamma(B, D), \quad (4)$$

где $B = \{B_i\}$ – множество линейных участков программы; $D = \{B \times B\}$ – множество связей по управлению между линейными участками. При этом каждый линейный участок в свою очередь представляет собой последовательность инструкций $B_i = \{b_{i1}, b_{i2}, ..., b_{im_i}\}$, где b_{im_i} – инструкция, m_i – количество инструкций в i-ом линейном блоке программы. Для простоты будем полагать, что во всех k линейных блоках программы содержится одинаковое количество инструкций m, а в каждой инструкции содержится n параметров. Количество линейных блоков, покрытых механизмами кибериммунитета будем обозначать k'.

Устойчивость цифрового сервиса платформы «ГосТех» оценивается по показателю вероятности $P(t)$ нахождения его в работоспособном состоянии в течение времени t в условиях ИТВ, заключающихся в передаче программе цифрового сервиса входных данных, приводящих к нарушениям $x \in L_{вх}^{-}$ [2]:

$$P(t) = \frac{\mu(t)}{\lambda(t)+\mu(t)}\left(1+\frac{\lambda(t)}{\mu(t)}e^{-(\lambda(t)+\mu(t))t}\right), \quad (5)$$

где $\lambda(t)$ – функция интенсивности нарушений; $\mu(t)$ – функция интенсивности восстановлений.

Требуется. Разработать метод кибериммунной защиты цифровых сервисов платформы «ГосТех», обеспечивающий требуемую их устойчивость:

$$M : \langle UT, Z, E, \{P\}\rangle \to P \mid P \geq P^{треб}, \quad (6)$$

где UT – модель УМТ цифрового сервиса; Z – множество внутренних параметров модели; E – множество параметров воздействия; P – вероятность работоспособного состояния цифрового сервиса платформы «ГосТех».

Ограничение. Максимально допустимое время выполнения программы цифрового сервиса «ГосТех»:

$$T_{выполн} = T_{выч} + T_{обн} + T_{восст} \leq T_{\max}, \quad (7)$$

где $T_{выч}$ – время вычисления программы; $T_{обн}$ – время обнаружения нарушения; $T_{восст}$ – время восстановления штатного функционирования.

Метод кибериммунной защиты цифровых сервисов

Разработанный метод состоит из нескольких шагов, включающих:

- определение необходимого значения коэффициента покрытия кибериммунитета $k'_{необх}$ на основе параметров модели, требуемого значения показателя устойчивости $P^{треб}$, значения параметра воздействия $\left|L_{вх}^{-}\right|$ и значения вероятности обнаружения нарушения $P_{обн}$, задаваемого эталонной моделью программы, посредством решения неравенства, получаемого из формулы (5):

$$\lim_{t\to\infty} P(t) \geq P^{треб}; \quad (8)$$

- определение достаточного значения коэффициента покрытия кибериммунитета $k'_{дост}$ на основе параметров модели и ограничения $T_{\max}$ посредством решения неравенства, получаемого из формулы (7):

$$T_{выполн} \leq T_{\max}; \quad (9)$$

- определение наличия решения в соответствии с критерием:

$$0 \leq k'_{необх} \leq k'_{дост} \leq k; \quad (10)$$

- синтез решения $k \in [k'_{необх}; k'_{дост}]$.

Схема разработанного метода приведена на рис. 2.

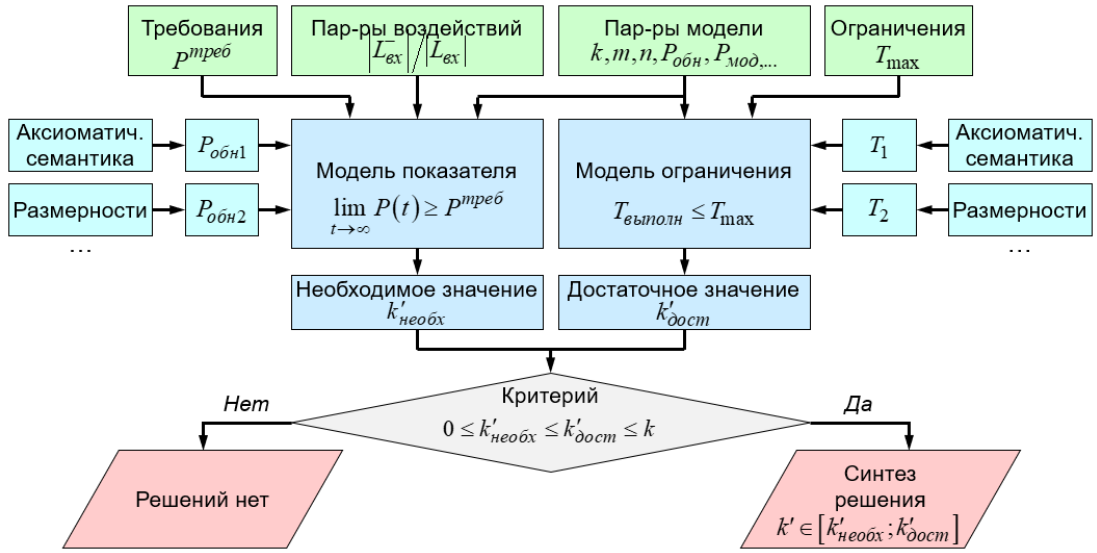


Рис. 2. Схема метода кибериммунной защиты облачных сервисов платформы «ГосТех»

Экспериментальные исследования

Будем оценивать устойчивость цифровых сервисов платформы «ГосТех» на примере типового цифрового сервиса. Зададим начальные значения. Пусть $k=1000$, $m=5$, $n=3$, $\frac{|L_{вх}^-|}{|L_{вх}|}=0,4$, $P_{мод}=0,75$, $T_{\max}=46000$, $P^{треб}=0,85$. Требуется обеспечить $\lim_{t\to\infty} P(t) \ge P^{треб}$.

Результаты моделирования для заданных начальных условий приведены на рис. 3.

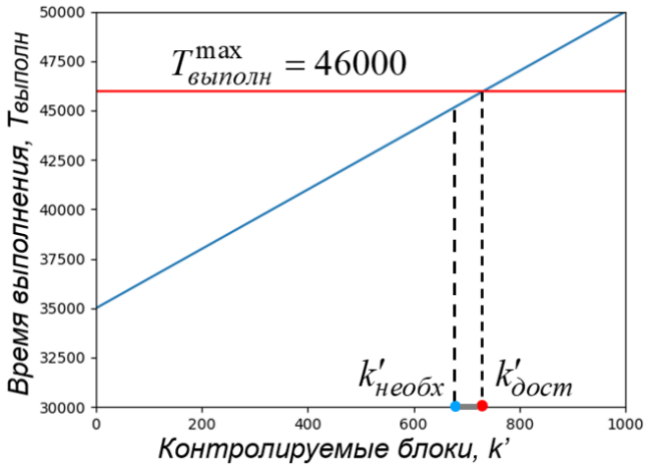


Рис. 3. Результаты моделирования

Значения параметра k', при которых *обеспечивается* требуемое значение $\lim_{t\to\infty} P(t) \ge P^{треб}$ при ограничении на $T_{\max}$ лежат в отрезке $k' \in [695;733]$.

Заключение

В работе предложен метод кибериммунной защиты цифровых сервисов платформы «ГосТех» в условиях ИТВ. Научная новизна предложенного метода заключается в том, что в отличие от существующих во вновь разработанный метод введены новые группы формальных операций синтеза необходимого и достаточного значений коэффициента покрытия линейных блоков программы цифрового сервиса свойствами кибериммунитета, а также учтена вероятность обнаружения нарушений, что обладает положительным теоретическим эффектом в части обеспечения возможности исследования устойчивости цифровых сервисов платформы «ГосТех».

Результаты экспериментальных исследований позволили подтвердить достоверность полученных результатов в части возможности обеспечения требуемой устойчивости функционирования цифровых сервисов платформы «ГосТех».

К направлениям дальнейших исследований можно отнести исследование возможности интеллектуального управления коэффициентом покрытия кибериммунитета $k_{покр}$, например, на основе методов искусственного интеллекта, а также синтез многоуровневой модели цифрового сервиса платформы «ГосТех».

Статья подготовлена по результатам Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус».

Литература

1. *Балябин, А. А. Угрозы устойчивости функционирования облачных платформ / А. А. Балябин // Международная конференция по мягким вычислениям и измерениям. – 2024. – Т. 1. – С. 308-312.*
2. *Балябин, А. А. Обеспечение устойчивости функционирования облачных платформ на основе кибериммунитета / А. А. Балябин // Международная конференция по мягким вычислениям и измерениям. – 2024. – Т. 1. – С. 291-295.*
3. *Балябин, А. А. Метод иммунного ответа на ранее неизвестные вредоносные воздействия / А. А. Балябин, В. А. Новиков, С. А. Петренко // Методы и технические средства обеспечения безопасности информации. – 2022. – № 31. – С. 11-13.*
4. *Бирюков, Д. Н. Порождение сценариев предупреждения компьютерных атак/ Д.Н.Бирюков, А. Г. Ломако, С. А. Петренко // Защита информации. Инсайд. – 2017. – № 4(76). – С. 70-79.*
5. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д. П. Зегжды. - М.: Горячая линия - Телеком, 2021. - 560 с.*
6. *Корниенко, А. А. Модели и методы риск-ориентированного проактивного управления информационной безопасностью железнодорожной транспортной системы / А. А. Корниенко, А.П.Глухов // Бюллетень Объединенного ученого совета ОАО РЖД. – 2018. – № 3. – С. 42-54.*
7. *Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.*
8. *Месарович М., Мако Д., Такахара И. Теория многоуровневых иерархических систем. – М.: Мир – 1973. – 344 с.*
9. *Петренко, С. А. Киберустойчивость индустрии 4.0/ С. А. Петренко. – Санкт-Петербург: Издательский Дом "Афина", 2020. – 256 с.*
10. *Петренко, С. А. Кибериммунология . – СПб.:: Афина, 2021. – 239 с.*

11. Петренко, С. А. Национальная система раннего предупреждения о компьютерном нападении / С. А. Петренко, Д. Д. Ступин; – СПб: Издательский Дом "Афина", 2017. – 440 с.

12. L. Caviglione et al., "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in IEEE Access, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.

13. S. Petrenko, E. Khismatullina. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats. Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.). 420 p. DOI: 10.1007/978-3-030-29852-4.

14. Y. Li, Q. Liu. «A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments», Energy Reports, vol. 7, pp. 8176-8186, 2021, DOI 10.1016/j.egyr.2021.08.126.B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, doi:10.1109/ACCESS.2021.3073203.

Method of Protecting the GosTech Cloud Platform based on Cyber Immunity

Balyabin A.A.[9]**, Petrenko S.A.** [10]

This paper presents and substantiates the author's method of protecting the GosTech cloud platform based on cyber immunity. This method allows not only to detect and neutralize previously unknown computer attacks by intruders in the MITER ATT&CK notation, but also for the first time to restore the digital services of the mentioned platform in real time.

Keywords: cloud platforms, cybersecurity, cyber resilience, information security threats, cloud computing vulnerabilities, cyberattacks by intruders, residual security risks, risk management, counteracting cyberattacks by intruders, cyber immune defense system, cyber immunity.

[9] Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, A.A.Balyabin@yandex.ru

[10] Sergei Petrenko, PhD (Eng., Grand Doctor), Full Professor, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Petrenko.SA@talantiuspeh.ru

УДК 004.056

Методика защиты облачной платформы «ГосТех» на основе кибериммунитета

Балябин А.А.[11], **Петренко С.А.**[12]

В настоящей работе представлена и обоснована авторская методика защиты облачной платформы «ГосТех» на основе кибериммунитета. Для синтеза требуемого киберимунитета были использованы соответствующие методы теории подобия и размерностей. Предлагаемая методика позволяет не только обнаруживать и нейтрализовать ранее неизвестные компьютерные атаки злоумышленников в нотации MITRE ATT&CK, но и впервые восстанавливать цифровые сервисы упомянутой платформы в реальном масштабе времени.

Ключевые слова: облачные платформы, кибербезопасность, киберустойчивость угрозы безопасности информации, уязвимости облачных вычислений, компьютерные атаки злоумышленников, остаточные риски безопасности, управление рисками, противодействие кибератакам злоумышленников, кибериммунная система защиты, кибериммунитет

Введение

В условиях появления новых, ранее неизвестных уязвимостей, роста количества и сложности кибератак, существующие подходы к кибербезопасности, зачастую, уже не способны в полной мере обеспечить требуемую защиту от целенаправленных информационно-технических воздействий (ИТВ) [1-3]. В то же время к объектам информатизации, на базе которых создаются государственные информационные системы (ГИС) и цифровые (облачные) сервисы, относящиеся к критической информационной инфраструктуре Российской Федерации (КИИ РФ), таким как, например, цифровые сервисы Единой цифровой платформы (ЕЦП) «ГосТех», предъявляются повышенные требования в части информационной безопасности и устойчивости [4, 5]. Данное противоречие характеризует проблемную ситуацию, разрешение которой является актуальной научной задачей.

Для решения данной научной задачи необходима разработка новых подходов к кибербезопасности, предполагающих создание адаптивных, самообучающихся систем, способных обнаруживать и своевременно реагировать как на известные, так и на ранее неизвестные киберугрозы [6-9,14]. Одним из перспективных подходов является наделение вычислительных систем свойствами кибериммунитета [2,3, 10,13].

Целью настоящей работы является разработка методики кибериммунной защиты цифровых сервисов платформы «ГосТех» с использованием теории подобия и размерностей.

Постановка задачи

В работах [2,3] представлена модель Ω цифровой платформы «ГосТех» с кибериммунитетом на основе универсальной машины Тьюринга (УМТ) большой вложенности и доказана ее эквивалентность модели на основе единственной машины Тьюринга (МТ). Поскольку МТ реализует детерминированный алгоритм, а алгоритм возможно описать с помощью примитивов последовательности, ветвления и цикла, то программу цифрового сервиса «ГосТех» можно описать графом потока управления (ГПУ):

[11] Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», федеральная территория «Сириус», A.A.Balyabin@yandex.ru

[12] Петренко Сергей Анатольевич, руководитель группы, доктор технических наук, профессор, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Petrenko.SA@talantiuspeh.ru

$$\Gamma = \langle B, D \rangle, \qquad (1)$$

где $B = \{B_i\}$ – множество вершин (линейных участков программы); $D = \{B \times B\}$ – множество дуг (переходов между линейными участками).

Каждый линейный участок ГПУ представляет собой последовательность инструкций $B_i = \{b_{i1}, ..., b_{im_i}\}$, где b_{im_i} – инструкция, m_i – количество инструкций в блоке B_i. Чтобы придать исходной программе облачной платформы свойство кибериммунитета, осуществляется трансляция с внедрением структурно-функциональной избыточности в виде меток контрольных точек в начало и конец линейного блока: $B_i' = \{KT_i, b_{i1}, ..., b_{im_i}, KT_i\}$. Инструкции же сводятся к виду арифметического выражения, для которого в соответствии с положениями теории подобия и размерностей [10, 13] вычисляется семантический инвариант. Правила вычисления инвариантов в терминах абстрактных размерностей приведены в табл. 1.

Таблица 1.

Абстрактные размерности арифметических соотношений

Операция	**Обозначение**	**Условие корректности**	**Линейное однородное уравнение**	**Критерий подобия**
Сложение	R = L + P	[L] = [P]	$[R]^0[L]^1[P]^{-1} = 1$	0 1 -1
Вычитание	R = L – P	[L] = [P]	$[R]^0[L]^1[P]^{-1} = 1$	0 1 -1
Умножение	R = L * P	[R] = [L][P]	$[R]^1[L]^{-1}[P]^{-1} = 1$	1 -1 -1
Деление	R = L / P	$[R] = [L][P]^{-1}$	$[R]^1[L]^{-1}[P]^1 = 1$	1 -1 1
Степень	$R = L^S$	$[R] = [L]^S$	$[R]^1[L]^{-S}[P]^0 = 1$	1 -S 0
Присваивание	R = L	[R] = [L]	$[R]^1[L]^{-1}[P]^0 = 1$	1 -1 0

Для простоты будем считать, что во всех k линейных блоках программы содержится одинаковое количество инструкций m, а в каждой инструкции содержится n параметров. Количество линейных блоков, покрытых механизмами кибериммунитета будем обозначать k'.

Устойчивость функционирования цифрового сервиса ЕЦП «ГосТех» будем оценивать по показателю вероятности $P(t)$ нахождения его в работоспособном состоянии в течение времени t в условиях ИТВ, заключающихся в передаче программе входных данных, приводящих к нарушениям $x \in L_{вх}^-$ [13]:

$$P(t) = \frac{\mu(t)}{\lambda(t) + \mu(t)} \left(1 + \frac{\lambda(t)}{\mu(t)} e^{-(\lambda(t) + \mu(t))t} \right), \qquad (2)$$

где $\lambda(t)$ – интенсивность нарушений; $\mu(t)$ – интенсивность восстановлений.

Выполним формальную постановку задачи.

Дано. Модель цифрового сервиса ЕЦП «ГосТех» с кибериммунитетом [13]:

$$\Omega = \{U, M, D, R, K, L_{вх}, L_{вых}\}, \qquad (3)$$

где M – эталонная модель цифрового сервиса; D – семантический обнаружитель нарушений; R – генератор микропрограмм восстановления; K – восстановитель штатного функционирования цифрового сервиса.

Требуется. Найти методику кибериммунной защиты цифровых сервисов платформы «ГосТех» с использованием теории подобия и размерностей, обеспечивающую требуемую их киберустойчивость:

$$M : \langle \Omega, k', |L_{вх}^-|, \{P\} \rangle \to P \mid P \geq P^{треб}, \qquad (4)$$

где k' – количество линейных блоков программы цифрового сервиса, для которых выполняется контроль семантики; $\left|L_{вх}^{-}\right|$ – мощность подмножества входных данных, приводящих к нарушению; P – вероятность нахождения системы в работоспособном состоянии.

Ограничение. Максимально допустимое время выполнения программы цифрового сервиса «ГосТех»:

$$T_{выполн} = T_{выч} + T_{обн} + T_{восст} \le T_{\max}, \quad (5)$$

где $T_{выч}$ – время вычисления программы; $T_{обн}$ – время обнаружения нарушения; $T_{восст}$ – время восстановления штатного функционирования цифрового сервиса.

Методика кибериммунной защиты цифровых сервисов

Методика предполагает нахождение необходимого $k'_{необх}$ и достаточного $k'_{дост}$ значений количества линейных блоков, для которых выполняется динамический контроль семантики в терминах теории подобия и размерностей, и синтез k' обеспечивающего требуемое значение $P^{треб}$ показателя вероятности нахождения цифрового сервиса облачной платформы «ГосТех» в работоспособном состоянии при ограничении на время выполнения программы $T_{\max}$.

Оценим необходимое значение $k'_{необх}$, решив неравенство $\lim\limits_{t\to\infty} P\left(k',t\right) \ge P^{треб}$ относительно k', исходя из (2), с учетом [2, 10, 13]:

$$\lim_{t\to\infty} P(t) = \frac{\mu}{\lambda(t)+\mu}\left(1+\frac{\lambda(t)}{\mu}\cdot 0\right)\Bigg|_{t\to\infty} = \frac{\mu}{\lambda(t)+\mu}\Bigg|_{t\to\infty} \ge P^{треб}, \quad (6)$$

$$\frac{\mu}{\lambda(t)+\mu}\Bigg|_{t\to\infty} = \frac{\mu}{\frac{P_{мод}}{T_{выч}}\frac{\left|L_{вх}^{-}\right|}{\left|L_{вх}\right|}\left(1-k_{покр}P_{обн}\right)+\mu} \ge P^{треб}, \quad (7)$$

что после ряда преобразований сведется к виду:

$$k' \ge k'_{необх} = \left\lceil \frac{P^{треб}P_{мод}\frac{\left|L_{вх}^{-}\right|}{\left|L_{вх}\right|} + \mu km(n-1)\left(P^{треб}-1\right)}{\frac{P^{треб}P_{обн}P_{мод}}{k}\frac{\left|L_{вх}^{-}\right|}{\left|L_{вх}\right|} + \mu\frac{m(m-1)}{2}(2n-1)\left(1-P^{треб}\right)} \right\rceil. \quad (8)$$

Оценим достаточное значение $k'_{дост}$, исходя из (5) с учетом [10,13]:

$$km(n-1) + k'\frac{m(m-1)}{2}(2n-1) + k'nm + knm \le T_{\max}, \quad (9)$$

что после ряда преобразований сведется к виду:

$$k' \le k'_{дост} = \left\lfloor \frac{T_{\max} - km(n-1) - kmn}{\frac{m(m-1)}{2}(2n-1) + mn} \right\rfloor. \quad (10)$$

Критерием существования решения будет выполнение неравенства $k'_{необх} \le k'_{дост}$, при $k'_{необх} > 0, k'_{дост} > 0$.

Схема разработанной методики представлена на рис. 1.

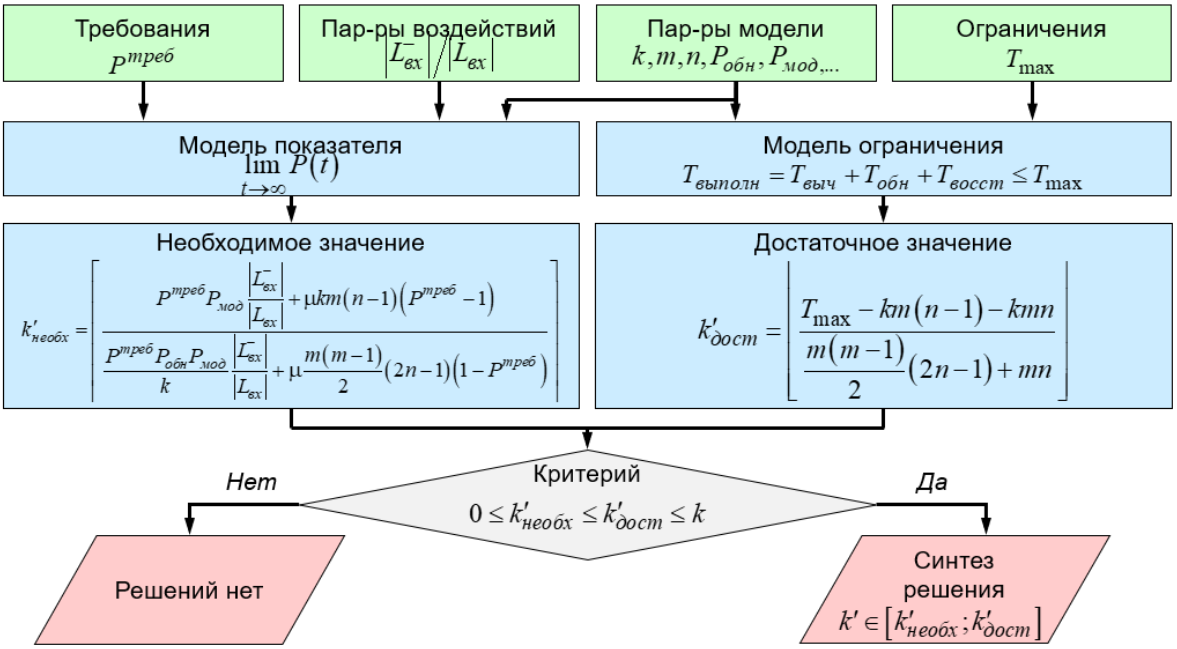


Рис. 1. Схема методики кибериммунной защиты цифровых сервисов «ГосТех»

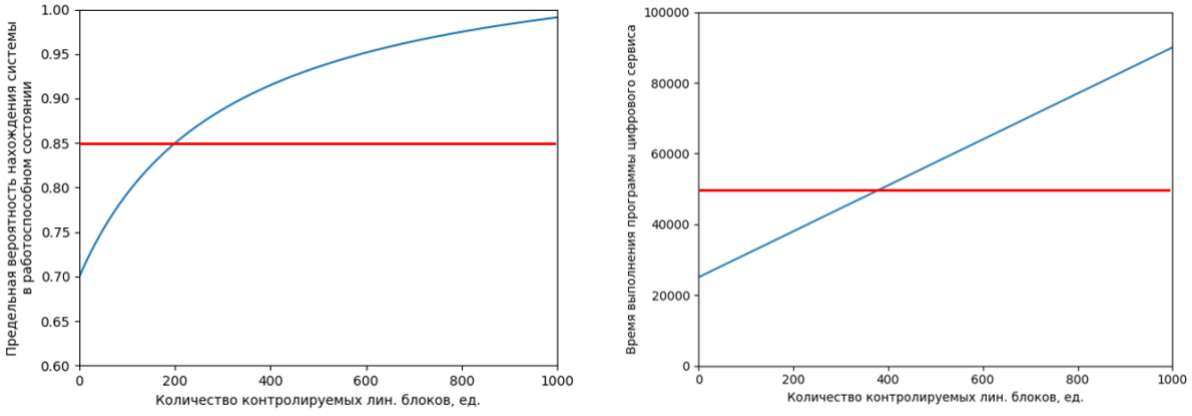
На завершающем этапе необходимо осуществить синтез $k' \in [k'_{необх}; k'_{дост}]$, исходя из требований, ограничений и параметров модели. В случае отсутствия решения, необходимо принять меры по реконфигурации цифрового сервиса.

Экспериментальные исследования

Зададим начальные условия. Пусть $k = 1000$, $m = 5$, $n = 3$, $|L_{вх}^{-}|/|L_{вх}| = 0{,}5$, $P_{мод} = 0{,}75$, $P_{обн} = P_{восст} = 0{,}875$, $P^{треб} = 0{,}85$, $T_{\max} = 50000$.

Исследуем предельную вероятность нахождения типового цифрового сервиса платформы «ГосТех» в работоспособном состоянии в зависимости от значения k'.

Результаты исследования представлены на рис. 2.



а б

Рис. 2. Результаты экспериментальных исследований

Необходимое и достаточное значения количества контролируемых линейных блоков, при которых обеспечивается требуемая устойчивость функционирования цифровых сервисов платформы «ГосТех» при заданных ограничениях, составили соответственно

$k'_{необх} = 201$ и $k'_{дост} = 384$. Критерий существования решения показал, что решение для данной конфигурации существует и лежит в отрезке $k' \in [201; 384]$.

Заключение

В работе предложена и обоснована методика кибериммунной защиты цифровых сервисов платформы «ГосТех» в условиях роста угроз безопасности с применением методов теории подобия и размерностей для синтеза требуемого кибериммунитета.

Результаты экспериментальных исследований позволили подтвердить достоверность полученных результатов в части возможности обеспечения требуемой устойчивости функционирования цифровых сервисов платформы «ГосТех» на основе кибериммунитета.

К направлениям дальнейших исследований можно отнести исследование возможности интеллектуального управления коэффициентом покрытия кибериммунитета $k_{покр}$, например, на основе методов искусственного интеллекта, а также возможностей применения иных математических аппаратов для формирования эталонных моделей программ цифровых сервисов платформы «ГосТех».

Статья подготовлена по результатам Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус».

Литература

1. *Балябин, А. А. Угрозы устойчивости функционирования облачных платформ / А. А. Балябин // Международная конференция по мягким вычислениям и измерениям. – 2024. – Т. 1. – С. 308-312.*

2. *Балябин, А. А. Обеспечение устойчивости функционирования облачных платформ на основе кибериммунитета / А. А. Балябин // Международная конференция по мягким вычислениям и измерениям. – 2024. – Т. 1. – С. 291-295.*

3. *Балябин, А. А. Метод иммунного ответа на ранее неизвестные вредоносные воздействия / А. А. Балябин, В. А. Новиков, С. А. Петренко // Методы и технические средства обеспечения безопасности информации. – 2022. – № 31. – С. 11-13.*

4. *Бирюков, Д. Н. Порождение сценариев предупреждения компьютерных атак/ Д.Н.Бирюков, А. Г. Ломако, С. А. Петренко // Защита информации. Инсайд. – 2017. – № 4(76). – С. 70-79.*

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

6. *Корниенко, А. А. Модели и методы риск-ориентированного проактивного управления информационной безопасностью железнодорожной транспортной системы / А. А. Корниенко, А.П.Глухов // Бюллетень Объединенного ученого совета ОАО РЖД. – 2018. – № 3. – С. 42-54.*

7. *Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.*

8. *Месарович М., Мако Д., Такахара И. Теория многоуровневых иерархических систем. – М.: Мир – 1973. – 344 с.*

9. *Петренко, С. А. Киберустойчивость индустрии 4.0 / С. А. Петренко. – Санкт-Петербург: Издательский Дом "Афина", 2020. – 256 с.*

10. *Петренко, С. А. Кибериммунология / С. А. Петренко. – Санкт-Петербург: Афина, 2021. – 239 с.*

11. Петренко, С. А. Национальная система раннего предупреждения о компьютерном нападении / С. А. Петренко, Д. Д. Ступин; – Санкт-Петербург: Издательский Дом "Афина", 2017. – 440 с.

12. L. Caviglione et al., "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in IEEE Access, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.

13. S. Petrenko, E. Khismatullina. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats. Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.). 420 p. DOI: 10.1007/978-3-030-29852-4.

14. Y. Li, Q. Liu. «A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments», Energy Reports, vol. 7, pp. 8176-8186, 2021, DOI 10.1016/j.egyr.2021.08.126.B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, doi:10.1109/ACCESS.2021.3073203.

Methodology for Protecting the GosTech Cloud Platform based on Cyber Immunity

Balyabin A.A.[13], **Petrenko S.A.** [14]

This paper presents and justifies the author's methodology for protecting the cloud platform "GosTech" on the basis of cyber immunity. The methods of similarity and dimensionality theory were used to synthesize the required cyber immunity. The proposed methodology allows not only to detect and neutralize previously unknown computer attacks of intruders in MITRE ATT&CK notation, but also to restore digital services of the mentioned platform in real time for the first time.

Keywords: cloud platforms, cybersecurity, cyber resilience, information security threats, cloud computing vulnerabilities, cyber attacks by intruders, residual security risks, risk management, counteracting cyber attacks by intruders, cyber immune defense system, cyber immunity.

[13] Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, A.A.Balyabin@yandex.ru

[14] Sergei Petrenko, PhD (Eng., Grand Doctor), Full Professor, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Petrenko.SA@talantiuspeh.ru

УДК 004.056

Модель облачной платформы «ГосТех» с кибериммунитетом

Балябин А.А.[15], **Петренко С.А.**[16]

В настоящей работе представлена и обоснована авторская математическая модель платформы «ГосТех» с кибериммунитетом, инженерная реализация которой позволяет впервые обнаруживать и нейтрализовать ранее неизвестные компьютерные атаки злоумышленников в нотации MITRE ATT&CK на цифровые сервисы упомянутой платформы. Представлены результаты экспериментальных исследований устойчивости функционирования платформы «ГосТех» с кибериммунитетом, которые свидетельствуют об эффективности предлагаемого подхода.

Ключевые слова: облачные платформы, кибербезопасность, киберустойчивость угрозы безопасности информации, уязвимости облачных вычислений, компьютерные атаки злоумышленников, остаточные риски безопасности, управление рисками, противодействие кибератакам злоумышленников, кибериммунная система защиты, кибериммунитет.

Введение

Рост киберугроз в мире достигает беспрецедентных масштабов и является одним из значимых вызовов для современной экономики данных. Современные информационно-технические воздействия (ИТВ) все чаще носят организованный и целенаправленный характер (*Advanced Persistent Threats, APT*), отличаются высокой интенсивностью и большим количеством задействованных ресурсов [1, 2]. Наибольшую опасность среди них представляют воздействия, включающие эксплуатацию уязвимостей «нулевого дня» (0-day) в качестве начального вектора, поскольку они не могут быть своевременно обнаружены и предотвращены существующими классическими средствами защиты [3-5].

Количество инцидентов информационной безопасности (ИБ), связанных с данным типом воздействий, в 2024 году практически утроилось по сравнению с аналогичным показателем предыдущего года, составив 14% от общего количества зарегистрированных инцидентов [6].

Особое беспокойство вызывают сочетанные или массово-групповые кибератаки злоумышленников на объекты критической информационной инфраструктуры (КИИ) Российской Федерации (РФ), относящиеся к сфере государственного управления, оборонно-промышленного комплекса, энергетической отрасли, транспорта и здравохранения. При этом государственные информационные системы (ГИС) и/или цифровые (облачные) сервисы КИИ РФ, как правило, создаются на основе Единой цифровой платформы (ЕЦП) «ГосТех». Нарушение функционирования упомянутых объектов КИИ РФ вследствие компьютерных атак злоумышленников могут привести к катастрофическим последствиям [7-10].

Следует констатировать, что известные методы и средства обеспечения кибербезопасности и киберустойчивости, не обладающие адаптивностью и интеллектуальными механизмами самообучения, не способны в полной мере предотвратить реализацию новых, ранее неизвестных угроз.

[15] Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», A.A.Balyabin@yandex.ru

[16] Петренко Сергей Анатольевич, руководитель группы, доктор технических наук, профессор, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Petrenko.SA@talantiuspeh.ru

Для решения этой научной задачи необходимо использовать, так называемые, проактивные подходы [8-10], одним из которых является подход на основе кибериммунитета [5-14].

Постановка задачи

Дано. Представим вычислительную программу цифрового сервиса ЕЦП «ГосТех» в виде модели машины Тьюринга (МТ) T :

$$T = \langle Q, \Sigma, \Gamma, \delta, q_0, q_F \rangle, \quad (1)$$

где Q – конечное множество состояний МТ; Γ – множество допустимых символов ленты; $\Sigma \subseteq \Gamma$ – множество входных символов МТ; δ – функция переходов МТ; q_0 – начальное состояние МТ; q_F – конечное состояние МТ.

Единая цифровая платформа «ГосТех» характеризуется как многоуровневая иерархическая система [14], а значит ее можно представить в виде универсальной МТ (УМТ) большой вложенности [12]:

$$U_i = \left(\left\{ U_{i-1,j} \right\}, \left\{ L_{вх_{i-1,j}} \right\}, \left\{ L_{вых_{i-1,j}} \right\} \right), \ j = \overline{1..n}, \quad (2)$$

где $\left\{ U_{i-1,j} \right\}$ – множество машин $(i-1)$-го уровня; $\left\{ L_{вх_{i-1,j}} \right\}$ – множество языков входных данных машин $(i-1)$-го уровня; $\left\{ L_{вых_{i-1,j}} \right\}$ – множество языков выходных данных машин $(i-1)$-го уровня. Таким образом, УМТ i-го уровня принимает на вход n УМТ $(i-1)$-го уровня с их входными данными и возвращает выходные данные машин.

Требуется. Разработать модель Ω устойчивого цифрового сервиса платформы «ГосТех» с кибериммунитетом в условиях ИТВ:

$$\Omega = \{ U, M, D, R, K, L_{вх}, L_{вых} \}, \quad (3)$$

где M – эталонная семантическая модель цифрового сервиса; D – обнаружитель нарушений семантики вычислений; R – генератор микропрограмм восстановления; K – восстановитель штатного функционирования цифрового сервиса.

Модель сервиса с кибериммунитетом

Машина Тьюринга реализует алгоритм и обладает свойством детерминированности. В соответствии с теоремой Бёма-Якопини любой алгоритм программы можно представить тремя примитивами: последовательностью, ветвлением, циклом, как показано на рис. 1.

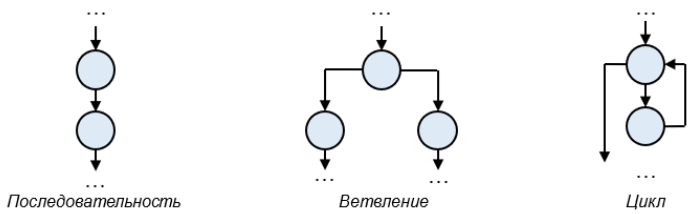


Рис. 1. Разновидности примитивов алгоритмов программ

Для описания алгоритма с помощью данных примитивов применяется граф потока управления (ГПУ):

$$\Gamma(B, D), \quad (4)$$

где $B = \{ B_i \}$ – множество линейных участков программы; $D = \{ B \times B \}$ – множество связей по управлению.

Таким образом, существует связь между машиной Тьюринга и графом потока управления, как показано на рис. 2.

Рис. 2. Связь между МТ и ГПУ

Каждый линейный участок графа в свою очередь представляет собой последовательность инструкций $B_i = \{b_{i1}, b_{i2}, ..., b_{im_i}\}$, где b_{im_i} – инструкция, m_i – количество инструкций в линейном блоке B_i. Инструкции декомпозируются в последовательности атомарных операций, состоящих из бинарного оператора и двух операндов.

Определим отображения, необходимые для построения модели:

$\alpha : \Gamma \to \Gamma'$ – отображение трансляции с кибериммунитетом, вносящее структурно-функциональную избыточность в исходный ГПУ программы;

$\beta : \Gamma \to M$ – отображение синтеза эталонной семантической модели программы;

$\gamma : X \to \{0,1\}$ – отображение проверки входных данных;

$\delta : \Gamma \times X \to P$ – отображение запуска программы цифрового сервиса с некоторыми входными данными;

$\psi : M \times S \to \{0,1\}$ – отображение обнаружения нарушений семантики вычислений;

$\xi : M \times S \to A$ – отображение синтеза сценария восстановления штатного функционирования цифрового сервиса;

$\eta : S \times A \to S$ – отображение восстановления штатного функционирования цифрового сервиса.

Тогда схему модели цифрового сервиса платформы «ГосТех» с кибериммунитетом можно представить с помощью отображений вида (см. рис. 3).

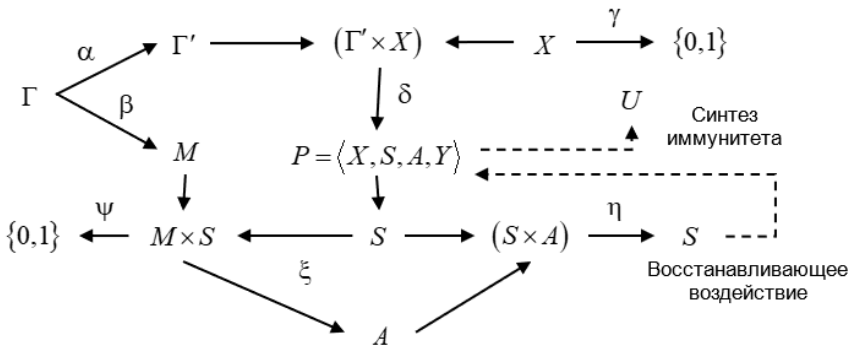


Рис. 3. Схема модели цифрового сервиса ЕЦП «ГосТех» с кибериммунитетом

Оценка результативности работы

ЕЦП «ГосТех» является динамической системой, сформируем показатель устойчивости следующим образом. Будем оценивать устойчивость функционирования цифрового сервиса по показателю вероятности P нахождения восстанавливаемой системы в работоспособном состоянии в зависимости от времени t [12]:

$$P(t) = \frac{\mu(t)}{\lambda(t)+\mu(t)}\left(1+\frac{\lambda(t)}{\mu(t)}e^{-(\lambda(t)+\mu(t))t}\right), \quad (5)$$

где $\lambda(t)$ – функция интенсивности нарушений от времени; $\mu(t)$ – функция интенсивности восстановлений от времени.

При этом, интенсивность нарушений прямо пропорциональна вероятности искажения, которая в свою очередь, прямо пропорциональна (~) количеству входных данных, приводящих к нарушениям и обратно пропорциональна коэффициенту покрытия кибериммунитета [6, 12]:

$$\lambda \sim P_{иск},\ P_{иск} \sim \frac{\left|L_{вх}^{-}\right|}{\left|L_{вх}\right|},\ P_{иск} \sim \frac{1}{k_{покр}}, \tag{6}$$

где $L_{вх}^{-}$ – подъязык входных данных, приводящих к нарушениям, $L_{вх}$ – язык входных данных программы цифрового сервиса платформы «ГосТех», $k_{покр}$ – коэффициент покрытия кибериммунитета.

Результаты экспериментальных исследований устойчивости типового цифрового сервиса платформы «ГосТех» с кибериммунитетом приведены на рис. 4.

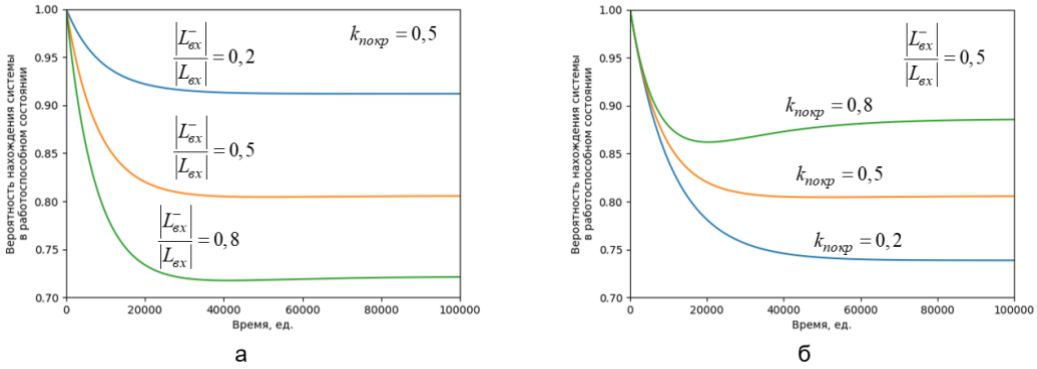


Рис. 4. Вероятность нахождения цифрового сервиса в работоспособном состоянии: *а* – при различных коэффициентах интенсивности нарушений; *б* – при различных значениях коэффициента покрытия кибериммунитета

Как видно, учет свойства самовосстановления позволяет обеспечить устойчивость функционирования цифрового сервиса на уровне $\lim_{t\to\infty} P(t)$. При этом, предельная вероятность устойчивого функционирования цифрового сервиса тем выше, чем больше коэффициент покрытия кибериммунитета $k_{покр}$.

Заключение

В работе была рассмотрена и обоснована авторская математическая модель платформы «ГосТех» с кибериммунитетом на основе аппарата универсальных машин Тьюринга. Это позволило количественно исследовать поведение цифровых сервисов упомянутой платформы в условиях роста угроз безопасности. Предложить возможные программные архитектуры трех основных механизмов противодействия компьютерным атакам злоумышленников в нотации MITRE ATT&CK, а именно: обнаружителя, нейтрализатора и восстановителя цифровых сервисов платформы «ГосТех».

Результаты экспериментальных исследований позволили подтвердить эффективность предлагаемого подхода для обеспечения киберустойчивости платформы «ГосТех» в условиях роста угроз безопасности.

К дальнейшим направлениям исследований можно отнести исследование возможности интеллектуального управления коэффициентом покрытия кибериммунитета $k_{покр}$, а также разработки многоуровневой модели цифрового сервиса платформы «ГосТех».

Статья подготовлена по результатам Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус».

Литература

1. *Балябин, А. А. Угрозы устойчивости функционирования облачных платформ / А. А. Балябин // Международная конференция по мягким вычислениям и измерениям. – 2024. – Т. 1. – С. 308-312.*

2. *Балябин, А. А. Обеспечение устойчивости функционирования облачных платформ на основе кибериммунитета / А. А. Балябин // Международная конференция по мягким вычислениям и измерениям. – 2024. – Т. 1. – С. 291-295.*

3. *Балябин, А. А. Метод иммунного ответа на ранее неизвестные вредоносные воздействия / А. А. Балябин, В. А. Новиков, С. А. Петренко // Методы и технические средства обеспечения безопасности информации. – 2022. – № 31. – С. 11-13.*

4. *Бирюков, Д. Н. Порождение сценариев предупреждения компьютерных атак / Д.Н.Бирюков, А. Г. Ломако, С. А. Петренко // Защита информации. Инсайд. – 2017. – № 4(76). – С. 70-79.*

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

6. *Корниенко, А. А. Модели и методы риск-ориентированного проактивного управления информационной безопасностью железнодорожной транспортной системы / А. А. Корниенко, А.П.Глухов // Бюллетень Объединенного ученого совета ОАО РЖД. – 2018. – № 3. – С. 42-54.*

7. *Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.*

8. *Месарович М., Мако Д., Такахара И. Теория многоуровневых иерархических систем. – М.: Мир – 1973. – 344 с.*

9. *Петренко, С. А. Киберустойчивость индустрии 4.0/ С. А. Петренко. – Санкт-Петербург: Издательский Дом "Афина", 2020. – 256 с.*

10. *Петренко, С. А. Кибериммунология / С. А. Петренко. – Санкт-Петербург: Афина, 2021. – 239 с.*

11. *Петренко, С. А. Национальная система раннего предупреждения о компьютерном нападении / С. А. Петренко, Д. Д. Ступин; – Санкт-Петербург: Издательский Дом "Афина", 2017. – 440 с.*

12. *L. Caviglione et al., "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in IEEE Access, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.*

13. *S. Petrenko, E. Khismatullina. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats. Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.). 420 p. DOI: 10.1007/978-3-030-29852-4.*

14. *Y. Li, Q. Liu. «A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments», Energy Reports, vol. 7, pp. 8176-8186, 2021, DOI 10.1016/j.egyr.2021.08.126.B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, doi:10.1109/ACCESS.2021.3073203.*

Model of the Cloud Platform "GosTech" with Cyber Immunity

Balyabin A.A.[17], **Petrenko S.A.** [18]

This paper presents and substantiates the author's mathematical model of the GosTech platform with cyber immunity, the engineering implementation of which allows for the first time to detect and neutralize previously unknown computer attacks of intruders in the MITRE ATT&CK notation on the digital services of the said platform. The results of experimental studies of the stability of the GosTech platform with cyber immunity are presented, which indicate the effectiveness of the proposed approach.

Keywords: cloud platforms, cybersecurity, cyber resilience, information security threats, cloud computing vulnerabilities, cyber attacks by intruders, residual security risks, risk management, counteracting cyber attacks by intruders, cyber immune defense system, cyber immunity.

[17] Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, A.A.Balyabin@yandex.ru
[18] Sergei Petrenko, PhD (Eng., Grand Doctor), Full Professor, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Petrenko.SA@talantiuspeh.ru

УДК 004.056

Мутационное фаззинг тестирование

Богословский Ф.И.[19]

В данной статье описывается исследование мутационного фаззинг тестирования применительно к требованиям безопасной разработки ПО. Проанализирован текущий этап развития фаззинга и векторы оптимизаций данного процесса как одного из этапов непрерывного цикла разработки ПО. В процессе работы были изучены существующие оптимизации и подходы к размытию исходного кода используя анализ и сравнение разных подходов к поиску уязвимостей в исходном коде с помощью фаззинг тестирования. Итогом исследования стало формальное описание метода анализа покрытия кода тестовым примером и предложен оптимальный метод мутации данных на основе алгоритма Фишера-Йетса.

Ключевые слова: фаззинг, уязвимости, разработка, мутация данных

Введение

Поиск уязвимостей в программном обеспечении является обязательной частью практики безопасной разработки [1]. На текущий момент существуют различные подходы к решению этой задачи. Последние 3-4 года активно внедряется требование о проведении фаззинг тестирования при разработке ПО [2]. По причине того, что корнем каждой уязвимости является дефект или неправильное, не заложенное разработчиком поведение, стоит отметить, что исправление найденных дефектов (в последствии уязвимостей) в процессе разработки стоит компании в десятки раз дешевле чем исправление дефекта после выпуска релиза ПО. Стоит понимать, что не все дефекты могут быть критичны и опасны, например, орфографические ошибки в выводе на экран вряд ли впоследствии смогут стать уязвимостью. Однако дефекты связанные с утечкой памяти или переполнением буфера памяти могут сильно повлиять на качество и безопасность программного обеспечения. Одним из методов поиска данного вида уязвимостей является фаззинг-тестирование[20] [3-10].

Предположим, что после предоставления фаззеру начального ввода t_0, который выполняет путь 0, фаззер сразу исследует путь i+1. Предыдущий ввод t_i изменяется случайным образом, который реализует путь i. Каждый сгенерированный входной сигнал напрямую выбирается в качестве следующего начального значения, а переходы между состояниями описывается цепью Маркова. Вероятностные переходы p_{ij} определяются как вероятность сгенерировать данные, которые реализуют путь j. Достигается это через случайное изменение предыдущего значения t_i. Такая цепь Маркова неоднородна по времени. Анализ сложен, а существование стационарного распределения не гарантируется. Для получения стационарного распределения стоит рассмотреть фаззинг тестирование как однородную по времени модель: стационарное распределение существует для модели фаззинга на основе покрытия. Пространство состояний цепи Маркова определяется обнаруженными путями и их непосредственными соседями. Учитывая множество входных данных T, пусть S + будет набором (обнаруженных) путей, который реализуется через T, а S− будет набором (неоткрытых) путей, которые реализуются входными данными, сгенерированными случайным изменением любого t ∈ T. Тогда множество состояний S цепи Маркова задаются в виде[21]:

$$S = S^+ \cup S^- \quad (1)$$

[19] Богословский Федор Игоревич, МГТУ им. Н.Э.Баумана, bogoslovskiyfi@student.bmstu.ru
[20] https://bdu.fstec.ru/education/videos/2/
[21] https://mboehme.github.io/paper/CCS16.pdf

Опишем предметную область математической моделью вероятности того, что фаззинг начального значения, которое реализует программный путь i, генерирует начальное значение, которое реализует путь j как вероятность перехода pij в цепи Маркова. Это позволяет нам описать цель фаззинга как эффективного исследования пространства состояний цепочки и объяснить проблемы и возможности. Можно смело утверждать, что фаззер AFL, основанный на покрытии использует более четкие пути в единицу времени, если он фокусируется на входных данных в областях с низкой плотностью Марковской цепи.

К примеру, если текущими входными данными является слово “fun!”, цепь Маркова находится в состоянии f***. Вероятность перехода в состояние fu** равна 2^{-10}. В среднем требуется 2^{10} = 1024 выполнения MI на слове “fun!”, чтобы выполнить путь 3 и достичь состояния fu**. Учитывая слово “fun!”, вероятность перехода в то же состояние f*** равна 0,75, потому что MI может выбрать первую букву и "f" в качестве замены или вторую букву и любую букву, кроме "u", в качестве замены с общей вероятностью 0,25, и он может выбрать третью или четвертое 23 письмо с общая вероятность равна 0,5. Вероятность перехода в состояние **** равна 1/4 – 2^{-10}, потому что MI может выбрать первую из четырех букв и заменить ее любой буквой, кроме ’f’. Фаззер на основе покрытия представляет собой совокупность случайных проходов в цепи Маркова. Для каждого начального значения t ∈ T есть один проход. Цель состоит в том, чтобы найти интересный путь s ∈ S −. Это не выполнится никаким t ∈ T при генерации минимального количества входных условий.

Концептуально все прогоны могут двигаться одновременно. Технически ресурсы ограничены и нам нужно выбрать какие прогоны могут двигаться и с какой частотой. Состоянию i присваивается p(i) = 2^{16} = 64k каждый раз, когда выбирается t_i. Поскольку большинство 4-символьных слов не начинаются с "f", то первый ввод t_0, вероятно, использует путь 0. После того как 2^{16} входных данных были сгенерированы с помощью фаззинга t_0, ожидается, что несколько входных данных будут начинаться с буквы 'f'. Один вход, который использует путь 1 сохраняется в качестве начального значения t_1. После того как еще 2^{16} входных данных были сгенерированы с помощью фаззинга t_1, ожидается, что по крайней мере один вход будет использовать путь 2 и сохраняется как t_2. В таблице 1 показано как продолжается процедура. После того как из четырех начальных значений которые были сохранены для каждого пути, было сгенерировано в общей сложности 256 тыс. входных данных, обнаружен сбой в СБФ. Более эффективному фаззеру потребовалось бы сгенерировать не более E[X01]+E[X12]+E[X 23]+ E[X 34] = $4 \cdot 2^{10}$ = 4k входных данных, чтобы выявить ту же уязвимость.

Таблица 1

Состояния и кол-во тестов для нахождения всех путей

Кол-во тестов	Состояния	Найденные состояния
1	****	****
2^{16} + 1	F***	****, F***
$2*2^{16}$ + 1	FU**	****, F***, FU**,
$3*2^{16}$ + 1	FUZ*	****, F***, FU**, FUZ*
$4*2^{16}$ + 1	FUZZ	****, F***, FU**, FUZ*,FUZZ

Фаззер greybox, основанный на покрытии, представляет собой набор случайных агентов в цепи Маркова. Для каждого начального значения t ∈ T есть один агент. Цель состоит в том, чтобы найти интересный путь s ∈ S − который не используется никаким t ∈ T при создании минимального количества входных данных. Концептуально, что все агенты могут двигаться одновременно. Вычислительные ресурсы ограничены, и нам нужно выбрать, какие ходунки могут двигаться и как часто. При последовательной настройке

фаззер выбирает следующий вход для фаззинга t ∈ T в соответствии с chooseNext и генерирует столько входных сигналов, сколько определено p = PowerEnergy(t). Обычно значение p < M, где M ∈ N определяет верхнюю границу количества генерируемых входных данных. В AFL M равно 160 тыс.

Энергии больше, чем требуется. AFL реализует расписание, которое назначает постоянную энергию в зависимости от количества раз, когда соответствующее начальное значение было выбрано из очереди.

Пусть Xij - случайная величина, описывающая минимальную энергию, которая должна быть присвоена состоянию i ∈ S + таким образом, фаззер обнаруживает новое состояние j ∈ S−, где $p_{ij} > 0$

$$\mathbb{E}[X_{ij}] = \frac{1}{p_{ij}} \qquad (2)$$

входных данных, чтобы выявить ту же уязвимость.

Мутации в AFL++ также предусматривают постоянное потребление высокой энергии: перемешивание исходных значений, или, другими словами, затравки для фаззинга в нашей машине, часто занимает около минуты. Это создаёт проблему быстрого перемешивания. Исходные значения выбираются из десяти, так что они проходят интересные траектории в области с низкой плотностью в стационарном распределении цепи Маркова. Присвоение высокой энергии исходным значением и значения, находящимся в непосредственной близости, позволяет обнаружить гораздо больше соседей в той же области с низкой плотностью. Однако по мере того, как сохраненные входные данные прокладывают пути с высокой плотностью регионы, существует естественная тенденция – слишком много энергии отводится этим входным данным. По определению, чем выше плотность стационарного распределения цепи Маркова для данного состояния i, тем выше доля входных данных, генерируемых путем фаззинга t_i, которые будут использовать высокочастотные пути.

Пример. Пусть начальным значением будет слово fun!, а графику мощности AFL присвоено значение энергии $p(i) = 2^{16} = 65536$ до состояния i при каждом выборе ti. Это позволяет нам обсудить случай, когда следующее состояние не найдено за одну итерацию фаззинга и может потребоваться несколько циклов по циклической очереди. Напомним, что AFL выбирает исходные данные в порядке их добавления, как после 2^{16} -кратного перемешивания исходного количества семян обнаруживаются два новых семени. Примерно четверть количества исходных значений использует пути **** и f*** соответственно. При растушевке первого обнаруженного исходного значении все растушевки выполняются по одному и тому же пути. Добавляем второе обнаруженное значение и выполняем четверть движения по траектории **** и три четверти движения по траектории f***.

Поскольку новых исходных значений обнаружено не было, то новый цикл начинается с начального зернышка. Эта процедура продолжается до тех пор, пока уязвимость не будет обнаружена. В каждой строке мы видим, что большинство запусков использует путь ****. Очевидно, что фаззер тратит слишком много времени на использование этого высокочастотного пути. Это же время приоритетней потратить на фаззинг затравки, используя низкочастотный канал fun*.

Подводя итог, можно сказать, что у существующих фаззеров greybox на основе покрытия есть две проблемы:

1. Может выделять больше энергии, чем требуется и тратится большое количествово времени на обработку высокочастотных соседей.

2. Может выделять слишком много энергии состояниям в областях с высокой плотностью стационарного распределения цепи и недостаточно энергии состояниям в областях с низкой плотностью.

```
      void UpdateEnergy(size_t GlobalNumberOfFeatures, bool ScalePerExecTime,
std::chrono::microseconds AverageUnitExecutionTime) {
    Energy = 0.0;
    SumIncidence = 0;
    // Apply add-one smoothing to locally discovered features.
    for (auto F : FeatureFreqs) {
      size_t LocalIncidence = F.second + 1;
      Energy -= LocalIncidence * logl(LocalIncidence);
      SumIncidence += LocalIncidence;
    }    // Apply add-one smoothing to locally undiscovered features.
    //   PreciseEnergy -= 0; // since logl(1.0) == 0)
    SumIncidence += (GlobalNumberOfFeatures - FeatureFreqs.size());
    // Add a single locally abundant feature apply add-one smoothing.
    size_t AbdIncidence = NumExecutedMutations + 1;
    Energy -= AbdIncidence * logl(AbdIncidence);
    SumIncidence += AbdIncidence; // Normalize.
    if (SumIncidence != 0)
      Energy = (Energy / SumIncidence) + logl(SumIncidence);
    if (ScalePerExecTime) { // Scaling to favor inputs with lower execution
time.
      uint32_t PerfScore = 100;
      if (TimeOfUnit.count() > AverageUnitExecutionTime.count() * 10)
        PerfScore = 10;
      else if (TimeOfUnit.count() > AverageUnitExecutionTime.count() * 4)
        PerfScore = 25;
      else if (TimeOfUnit.count() > AverageUnitExecutionTime.count() * 2)
        PerfScore = 50;
      else if (TimeOfUnit.count() * 3 > AverageUnitExecutionTime.count() * 4)
        PerfScore = 75;
      else if (TimeOfUnit.count() * 4 < AverageUnitExecutionTime.count())
        PerfScore = 300;
      else if (TimeOfUnit.count() * 3 < AverageUnitExecutionTime.count())
        PerfScore = 200;
      else if (TimeOfUnit.count() * 2 < AverageUnitExecutionTime.count())
        PerfScore = 150;
      Energy *= PerfScore;
   }
}
```

Code Block 1 – Пример обновления энергии для исходных данных

Выделите больше энергии затравке с высокой энтропией и это позволит получить больше информации о глобально редких объектах, находящихся поблизости от затравки. Поскольку мы не знаем энтропию семени, которое никогда не запускалось, мы присваиваем свежим семенам максимальную энтропию и позволяем II->Energy приблизиться к истинной энтропии сверху. Если значение ScalePerExecTime равно true, вычисленная энтропия масштабируется в зависимости от того, насколько быстро выполняется этот ввод по сравнению со средним временем выполнения входных данных. Чем быстрее выполняется ввод, тем больше энергии выделяется на вход.

Этот код реализует метод UpdateEnergy, который обновляет значение переменной Energy на основе нескольких факторов, включая количество обнаруженных и не обнаруженных локальных признаков (features), обилие мутаций, а также время выполнения. Далее объясню алгоритм работы этого метода по шагам:

Входные параметры

GlobalNumberOfFeatures: количество глобальных признаков (features), известных в системе.

ScalePerExecTime: логическое значение, указывающее, нужно ли масштабировать энергию в зависимости от времени выполнения.

AverageUnitExecutionTime: среднее время выполнения единицы работы (или задачи) в микросекундах.

Локальные переменные

Energy: переменная, которая хранит итоговую энергию. Инициализируется как 0.

SumIncidence: переменная для хранения суммы встречаемости признаков. Инициализируется как 0.

Алгоритм работы:

1. Инициализация переменных

Energy сбрасывается до 0.0.

SumIncidence сбрасывается до 0.

2. Обработка обнаруженных признаков (features)

Цикл проходит по каждому обнаруженному локально признаку из контейнера FeatureFreqs.

Для каждого признака значение его частоты встречаемости увеличивается на 1 (add-one smoothing — это метод сглаживания, чтобы избежать проблемы с нулевой частотой).

Рассчитывается вклад этого признака в энергию по формуле: Energy -= LocalIncidence * logl(LocalIncidence), где LocalIncidence — это частота встречаемости признака с добавлением единицы.

Значение частоты встречаемости добавляется в SumIncidence.

3. Обработка не обнаруженных признаков

Количество не обнаруженных признаков вычисляется как разница между общим количеством глобальных признаков (GlobalNumberOfFeatures) и количеством обнаруженных локально признаков (размер контейнера FeatureFreqs).

Эта величина добавляется в SumIncidence. Вклад в энергию от этих признаков не учитывается, так как логарифм от 1 равен 0.

4. Обработка обильных мутаций

Рассчитывается частота мутаций с добавлением единицы (AbdIncidence = NumExecutedMutations + 1).

Этот вклад также учитывается в общей энергии по формуле: Energy -= AbdIncidence * logl(AbdIncidence).

AbdIncidence добавляется к SumIncidence.

5. Нормализация энергии

Если сумма всех встречаемостей (SumIncidence) не равна нулю, энергия нормализуется по формуле:

Energy = (Energy / SumIncidence) + logl(SumIncidence)

Это шаг нормализации, где энергия делится на сумму

встречаемостей, и к результату прибавляется логарифм суммы встречаемостей.

Energy *= PerfScore;

Резюме алгоритма:

Сначала вычисляется энергия на основе частоты встречаемости признаков и мутаций с добавлением единицы.

Энергия нормализуется на основе суммы всех встречаемостей.

Если необходимо, энергия масштабируется по времени выполнения задачи, чтобы задачи с меньшим временем выполнения получали больше энергии.

Этот алгоритм использует логарифмическую функцию для вычисления энергии, где более частые события (например, признаки или мутации) имеют больший вклад в итоговое значение энергии.

6. Масштабирование энергии по времени выполнения (если нужно)

Если ScalePerExecTime равно true, энергия масштабируется в зависимости от времени выполнения относительно среднего времени выполнения (AverageUnitExecutionTime).

Рассчитывается PerfScore (оценка производительности) на основе нескольких условий:

Чем дольше время выполнения, тем меньше балл PerfScore (от 10 до 300).

В зависимости от того, насколько время выполнения текущей задачи (TimeOfUnit) превышает или меньше среднего времени выполнения, балл варьируется по условиям:

Если время выполнения более чем в 10 раз превышает среднее, PerfScore равен 10.

Если время выполнения составляет менее четверти среднего времени, PerfScore может быть равен 300.

Наконец, энергия масштабируется на этот PerfScore.

Для того что бы снизить большое выделение энергии соседним значения при мутациях входных значений, предлагается использовать алгоритм перетасовки Фишера – Йетса. Это должно позволить снизить выделение энергии исходным данных приблизительно схожими между собой и увеличить охват. Имея массив, реализуем алгоритм для генерации случайной перестановки элементов массива. Здесь перетасовка означает, что каждая перестановка элемента массива должна быть одинаково вероятной.

Пусть заданный массив будет arr[]. Простым решением является создание вспомогательного массива temp[], который изначально является копией arr[]. Случайным образом выберите элемент из temp[], скопируйте случайно выбранный элемент в arr[0] и удалите выбранный элемент из temp[]. Повторите тот же процесс n раз и продолжайте копировать элементы в arr[1], arr[2], ... Временная сложность этого решения будет равна $O(n^2)$.

Алгоритм перетасовки Фишера–Йейтса работает в O(n) временной сложности. Предполагается, что нам дана функция rand(), которая генерирует случайное число за O(1) времени. Идея состоит в том, чтобы начать с последнего элемента и поменять его местами со случайно выбранным элементом из всего массива (включая последний). Теперь рассмотрим массив от 0 до n-2 (размер, уменьшенный на 1), и повторяем процесс, пока не дойдем до первого элемента.

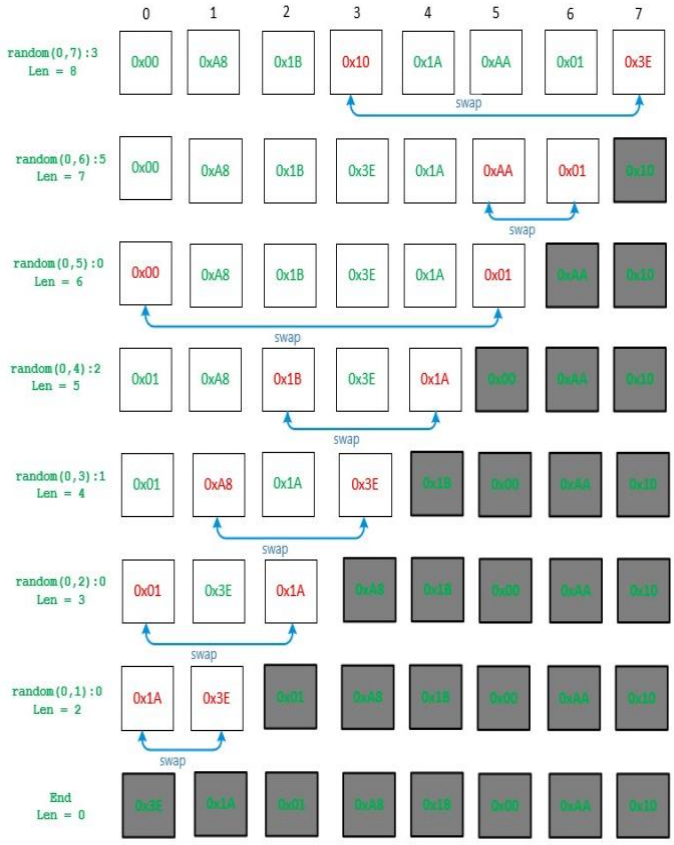


Рисунок 1 – Алгоритм перетасовки Фишера–Йейтса

Вывод

В ходе работы было предложено использование алгоритма Фишера-Йетса для оптимизации подхода к мутационному фаззингу, что позволит сократить время перебора исходных данных (тестовых примеров). Исследование показало, что использование степени мутации как параметра позволяет эффективно управлять процессом генерации и мутации входных данных. Значение этого параметра может быть настроено в зависимости от конкретных требований и особенностей тестируемого кода. В ходе работы выявлено положительное влияние алгоритма Фишера-Йетса на степень мутации и обеспечения наиболее точных и разнообразных тестовых данных.

Литература

1. *Барабанов А.В., Вареница В.В., Марков А.С. Аудит безопасности программ. Учебно-методическое пособие / Москва, МГТУ им. Н.Э.Баумана, 2021. 56 с.*

2. *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.*

3. *Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ / Арустамян С.С., Антипов И.С. В сборнике: Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. С. 11-15.*

4. *Интеллектуальный метод мутации входных корпусов с обратной связью / Самарин Н.Н., Тулинова А.В. // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 142-148.*

5. *Козачок А.В., Ерохина Н.С., Николаев Д.А. Способ обнаружения программных дефектов в Javascript-интерпретаторах методом фаззинг-тестирования // Вопросы кибербезопасности. 2024. № 2 (60). С. 74-80.*

6. *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.*

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

8. *Модели и подходы к анализу поверхности атаки для фаззинг-тестирования ядра Linux / Теплюк П.А., Якунин А.Г. // Безопасность информационных технологий. 2024. Т. 31. № 1. С. 135-145.*

9. *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.*

10. *Шелухин О.И., Раковский Д.И. Разработка программно-аппаратного комплекса моделирования многозначных компьютерных атак // Вопросы кибербезопасности. 2024. № 4 (62). С. 116-130.*

Mutation fuzzing testing

Bogoslovsky F.I.[22]

In the article mutational fuzz testing as applied to secure software development requirements is explored. The current stage of fuzzing development and optimization vectors of this process as one of the stages of the Continuous Integration/Continuous Delivery are analyzed. In the process of working towards existing optimizations and approaches to source code fuzzing were studied using analysis and comparison of different approaches to finding vulnerabilities in source code using fuzz testing. The result of the study was a formal description of the method for analyzing code coverage by a test example and proposed an optimal method for data mutation based on the Fisher-Yates algorithm.

Keywords: fuzzing, vulnerability, develop, mutation data

[22] Bogoslovsky Fedor Igorevich, Bauman Moscow State Technical University, bogoslovskiyfi@student.bmstu.ru

УДК 004.056

Актуальность проблемы выявления сгенерированного видео с использованием технологий искусственного интеллекта в социальных сетях и цифровых медиа

Борисов С.В.[23]

Ввиду постоянного роста количества видеоматериала в социальных сетях и цифровых медиа, конкуренция между авторами за внимание аудитории увеличивается. Широкое распространение видеоматериала становится важнейшей частью развития социальных сетей. Вместе с развитием технологий искусственного интеллекта, число сгенерированных ими видео постоянно растет. Было проведено исследование вопроса актуальности проблемы необходимости выявления такого видеоматериала с целью минимизации негативного воздействия на пользователей социальных сетей. Результатом рассмотрения проблематики выявления видео, созданного с применением технологий искусственного интеллекта, стало подтверждение ее актуальности в области не только социальных наук, но и в информационной безопасности, определена потребность в ее дальнейшем исследовании, а также изложены перспективные направления дальнейших работ.

Ключевые слова: видео, распространение информации, безопасность пользователей, социальные сети, противоправный контент.

Введение

По данным российской аналитической системы Brand Analytics, в марте 2023 года число активных авторов в социальных медиа в России составило 63 млн. Авторы написали 1,44 млрд публичных сообщений. Очевидной проблемой безопасности современного общества стало распространение вредоносной и недостоверной информации [1, 2]. Видео – информация в мультимедийном формате. К видеоконтенту можно отнести не только само видео, но и его описание, теги и хештеги, ссылки, комментарии.

Обилие разножанрового видео на сегодняшний день является следствием развития площадок видеохостингов и социальных сетей. Современные социальные сети практически не обходятся без возможности размещения видеоматериалов: коротких видеороликов с бесконечной лентой, видеосообщений, gif-анимаций и др.

Можно выделить следующие функции видео:

1. Информационная – обеспечивает освещение различных событий и новостных сообщений;
2. Познавательная – представляет собой распространение научных, поп-научных и иных материалов с целью образования;
3. Коммуникативная – общение между автором контента и его аудиторией, сбор мнений, формирование статистик, мониторинг настроения аудитории;
4. Интегративная – создание эффекта сопричастности отдельного человека к некоему единому целому;
5. Манипулятивная – негативное воздействие на сознание людей с целью извлечения собственной выгоды, дестабилизации ситуации, использования в сфере мошенничества и др.

[23] Борисов Сергей Валерьевич, аспирант кафедры Защищенных систем связи, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», Санкт-Петербург, serbor2016@yandex.ru

Развитие социоинженерных атак

Особое внимание в вопросе защиты пользователей представляет манипулятивная функция видео. Крайне острая проблема манипуляции посредством использования авторитетов [3, С. 68]. Вредоносная информация – это отдельный информационный объект и/или совокупность объектов в сети Интернет, содержащий запрещенную или ограниченную к распространению информацию [4]. Например, к ней можно отнести рекламу схем обогащения, предложение о работе, предложений субсидий, грантов, других выплат, имеющих признаки противоправного контента.

Вместе с тем возрастает и количество видеоматериалов, содержащую такую рекламу, а также другие способы распространения, например, содержание qr-кодов, ведущих на противоправные сайты, ссылки в подписях к видео и другие формы.

Любое значимое событие вызывает общественную реакцию и резонанс [5]. Распространение вредоносной информации в социальных сетях представляет угрозу информационной безопасности и является проблемой национального значения [6].

В связи с этим вырастают и риски использования социальных сетей.

Развитие искусственного интеллекта

Благодаря развитию искусственного интеллекта и доступности его инструментов, распространение противоправной информации растет. Возможность генерации материалов с помощью технологий искусственного интеллекта, упрощения его создания, простота его графической модификаций, использование неэтических средств продвижения, таких как содержание противоправной рекламы, описания, несоответствующей тематике видео, тиражирования таких материалов с использованием специального программного обеспечения, делает проблему особенно острой.

Необходимо искать новые пути регулирования данного вопроса, совершенствовать технические средства анализа, определения незаконных видеоматериалов в социальных сетях для защиты их пользователей.

Определение актуальности проблемы

Как следствие, основная сложность выявления и противодействия распространению вредоносной видеоинформации в социальных сетях следует из постоянного развития площадок социальных сетей и информационных технологий, а именно:

1. Лавинообразного роста и информации, циркулирующей в социальных сетях [7] и её разнородность;
2. Широкого распространения видеоматериалов, в том числе с использованием специализированного автоматизированные программные комплексы, которые автоматически создают контент в социальных сетях и взаимодействуют с другими пользователями – ботов [8, с. 100];
3. Генерация видеоконтента посредством генеративных моделей нейронных сетей;
4. Продолжением увеличения числа проводимых социоинженерных атак на пользователей.

Современные исследования направлены преимущественно на анализ текстовой информации [4, 8-12]. Для определения безопасности видеоматериала необходимо проанализировать инструменты для генерации видео, установить их характерные признаки и черты, определить модель безопасности видеоинформации, включающей возможное

создание видеоматериалов с помощью генеративных моделей искусственного интеллекта, их особенности и характерные черты, а также предложить способы их определения.

Учитывая постоянно изменяющиеся социальные, политические, экономические составляющие жизни общества и рост количества контента в сети Интернет, необходимо вести работу по недопущению распространения вредоносной информации, в том числе в социальных сетях.

Выводы

Практическим результатом работы является определение необходимости дальнейшего исследования проблемы распространения опасных видеоматериалов на площадках социальных сетей и видеохостингов.

В качестве дальнейшего исследования предлагается определить улучшенную модель вредоносной информации, которая, в отличие от существующих аналогов, будет включать видеоинформацию, ее возможную причастность к генерации с помощью искусственного интеллекта. Также, для минимизации негативных последствий на пользователей платформы необходимо предложить архитектуру системы выявления видеоматериала, созданного с помощью искусственного интеллекта, на платформах социальных сетей и видеохостингах.

Литература

1. *Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Модель вредоносной информации и ее распространителя в социальных сетях. // Защита информации. Инсайд. 2020. № 3 (93). С. 66–72.*
2. *Басараб М.А., Иванов И.П., Колесников А.В., Матвеев В.А. Обнаружение противоправной деятельности в киберпространстве на основе анализа социальных сетей: алгоритмы, методы и средства (обзор) // Вопросы кибербезопасности. 2016. № 4 (17). С. 11-19.*
3. *Гагиев Т.А., Гогаев Г.П., Кокаева И.Ю. О манипулятивном влиянии медийной информации на современную молодежь. // Вестник Северо-Осетинского государственного университета имени К. Л. Хетагурова. 2023. № 4. С. 66-71.*
4. *Виткова Л.А. Модели, алгоритмы и методика противодействия вредоносной информации в социальных сетях: диссертация на соискание ученой степени кандидата технических наук / Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский федеральный исследовательский центр российской академии наук». 2021. – С. 19.*
5. *Сахаров Д. В., Шашкин В. С. Система противодействия распространению вредоносной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 783–787.*
6. *Виткова Л. А., Чечулин А. А., Сахаров Д. В. Выбор мер противодействия вредоносной информации в социальных сетях // Вестник Воронежского института ФСИН России, 2020. № 3. С. 20–29.*
7. *Василькова В.В., Легостаева Н.И. Боты на публичных аренах социальных сетей. // Социологический журнал. 2021. Т. 27. № 4. С. 99-117.*
8. *Абрамов М.В. Методы и алгоритмы анализа защищенности пользователей информационных систем от социоинженерных атак: оценка параметров моделей: диссертация на соискание ученой степени кандидата технических наук / Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский федеральный исследовательский центр российской академии наук», 2018. – С. 46.*

9. Полетаев В.С. Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет-ресурсов: диссертация на соискание ученой степени кандидата технических наук / Федеральное государственное бюджетное образовательное учреждение «Ульяновский государственный университет», 2020. – С. 4.

10. Проноза А.А., Виткова Л.А., Чечулин А.А., Котенко И.В., Сахаров Д.В. Методика выявления каналов распространения информации в социальных сетях. // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. Т. 14. № 4. С. 362-377.

11. Шварцкопф Е.А. Риск-модели социальных информационных сетей для общения в динамике их роста и межсетевой диффузии деструктивного контента: диссертация на соискание ученой степени кандидата технических наук / Федеральное государственное бюджетное образовательное учреждение высшего образования "Воронежский государственный технический университет". 2018. С. – 16.

12. Нечипуровский Д.И. Роль искусственного интеллекта в операциях по кибербезопасности в 2024 году // Научный аспект. 2024. Т. 11. № 5. С. 1384-1388.

Научный руководитель: Сахаров Дмитрий Владимирович, доцент, кандидат технических наук, доцент кафедры Защищенных систем связи, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», sguard7@mail.ru .

The relevance of the problem of identifying generated video using artifical intelligence technologies in socail networks and digital area

Borisov S.V.[24]

Due to the constant growth in the number of videos on social networks and digital media, competition between authors for the attention of the audience is increasing. The widespread distribution of video material is becoming an essential part of the development of social networks. Along with the development of artificial intelligence technologies, the number of videos generated by them is constantly growing. A study was conducted on the relevance of the problem of the need to identify such video material in order to minimize the negative impact on users of social networks. The result of the consideration of the problem of identifying videos created using artificial intelligence technologies was the confirmation of its relevance in the field of not only social sciences, but also in information security, the need for further research was identified, and promising areas for further work were outlined.

Keywords: video, information dissemination, user safety, generative model.

[24] Sergei Borisov, postgraduate MSC, Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruevich St Petersburg State University of Telecommunications, Saint-Petersburg, serbor2016@yandex.ru

УДК 004.056

Определение доверительных интервалов для показателей результативности функционирования средств обнаружения веб-бэкдоров

Боровков В.Е.[25], Ключарев П.Г.[26]

В статье рассматривается проблема оценивания результативности функционирования средств обнаружения веб-бэкдоров (СОВБ). В современных работах исследователи часто используют собственные наборы данных для тестирования результативности СОВБ, что может привести к необъективности полученных результатов. Для решения данной проблемы предложен метод, основанный на формировании тестовых наборов данных с учетом специальной выборки, а также на применении статистической теории для расчета доверительных интервалов показателей результативности СОВБ. Формирование тестовых наборов осуществляется на основе анализа различных типов веб-бэкдоров, которые должны быть выявлены средствами обнаружения. Объективность результатов обеспечивается тем, что вместо «точечных» значений предоставляются доверительные интервалы, зависящие от объемов тестовых наборов данных. Данная работа может быть полезной для специалистов и исследователей в области информационной безопасности, которые хотят проводить более объективную оценку своих СОВБ.

Ключевые слова: веб-бэкдоры, веб-шеллы, методы и средства тестирования, показатели результативности, средства обнаружения, средства защиты.

Введение

Веб-бэкдор представляет собой скрытый механизм, позволяющий злоумышленнику получать несанкционированный удаленный доступ к веб-серверу. К таким веб-бэкдорам могут относиться веб-шеллы, веб-загрузчики и другие инструменты [1,2]. Это может привести к сбоям в работе сервера и утечке чувствительной информации. Кроме того, через веб-бэкдоры злоумышленники могут получить доступ к внутренней инфраструктуре организации, что в итоге может привести к полной компрометации сети. Поэтому актуальным направлением является разработка средств обнаружения веб-бэкдоров [3]. В работах [1,4] было выявлено, что многие исследователи при разработке различных методов обнаружения веб-бэкдоров, не проводили проверку своих результатов в реальных условиях и использовали собственные наборы данных для оценки эффективности своих инструментов. Это может привести к необъективности их тестирования.

Для тестирования СОВБ необходимо использовать набор объектов, который включает как легитимные элементы (без признаков веб-бэкдоров), так и сами веб-бэкдоры. В зависимости от принципов работы СОВБ эти объекты могут быть представлены в различных форматах, например, в виде файлов или HTTP-пакетов. Система анализирует каждый объект, определяя, заражен он или нет. Для этого применяются следующие обозначения: TP — число истинно положительных классификаций, TN — число истинно отрицательных классификаций, FP — число ложноположительных классификаций, FN — число ложноотрицательных классификаций. На основе этих данных можно рассчитать

[25] Боровков Владислав Евгеньевич, аспирант кафедры ИУ-8 МГТУ им Н.Э. Баумана, Москва, Россия, vbscience@yandex.ru.
[26] Ключарёв Петр Георгиевич, доктор технических наук, профессор кафедры ИУ-8 МГТУ им. Н.Э. Баумана, г. Москва, pk.iu8@yandex.ru

показатели результативности СОВБ. В качестве таких показателей могут быть использованы следующие метрики, присущие бинарному классификатору [5]:

$$Re = \frac{TP}{TP + FN};\ Pr = \frac{TP}{TP + FP};\ Ac = \frac{TP + TN}{TP + TN + FP + FN}. \quad (1)$$

Формирование тестового набора данных

В данной работе необходимо определить доверительные интервалы для показателей результативности СОВБ (1). Значения этих показателей зависят от качества тестового набора.

Для СОВБ, работающих по принципу анализа содержимого файлов, можно использовать исследования [6-9] для формирования тестовых наборов данных.

Для подготовки тестового набора необходимо сначала классифицировать виды веб-бэкдоров, которые должен обнаруживать СОВБ, а затем создать набор в соотношении один к одному: один веб-бэкдор на один легитимный объект, поскольку показатель Ac не является информативным в задачах с неравными классами. Таким образом, в наборе будет $N_{\text{вб}}$ веб-бэкдоров и $N_{\text{л}}$ легитимных объектов, при этом $N_{\text{вб}} = N_{\text{л}} = N$. Веб-бэкдоры могут быть разделены на k групп, и набор будет формироваться пропорционально объему этих групп в предположении, что веб-бэкдоры равномерно распределены по этим группам (считаем, что злоумышленник может использовать любой вид веб-бэкдора с равной вероятностью).

Например, если СОВБ должно обнаруживать 64 вида веб-бэкдоров, минимальный пакет тестового набора данных будет состоять из 128 объектов: $N_{\text{л}}$ =64 легитимных и $N_{\text{вб}} =$ 64 веб-бэкдора, по одному экземпляру каждого вида.

Вычисление доверительных интервалов для показателей результативности

Согласно выборке, которая была предложена в предыдущем разделе, а также по определению переменных TP, TN, FP, FN следует, что:

$$TP + FN = N_{\text{вб}} = N, \quad (2)$$
$$TN + FP = N_{\text{л}} = N \quad (3)$$

Отсюда следует, что результат анализа легитимных объектов не влияет на значения TP и FN. Пусть $w_{TP} = \frac{TP}{N_{\text{вб}}} = \frac{TP}{N}$, $w_{FN} = \frac{FN}{N_{\text{вб}}} = \frac{FN}{N}$ – соответственно доля TP и FN относительно общего числа веб-бэкдоров в выборке. Аналогично результат анализа веб-бэкдоров не влияет на значения TN и FP. $w_{TN} = \frac{TN}{N_{\text{л}}} = \frac{TN}{N}$, $w_{FP} = \frac{FP}{N_{\text{л}}} = \frac{FP}{N}$ – соответственно доля TN и FP относительно общего числа легитимных объектов в выборке.

При проведении статистических исследований используем выборочные доли для оценки истинных долей TP, TN, FP, FN – $w^*_{TP}, w^*_{TN}, w^*_{FP}, w^*_{FN}$, соответственно, с требуемой вероятностью P.

Набор легитимных объектов формируется за счет собственно-случайного отбора [10]. Предельная ошибка выборки для доли в таком случае будет вычисляться по формуле:

$$\Delta_{w_{TN}} = \Delta_{w_{FP}} = z\sqrt{\frac{\sigma_w^2}{N_{\text{л}}}}, \quad (4)$$

где $\Delta_{w_{TN}}$, $\Delta_{w_{FP}}$ - предельные ошибки для доли TN и FP соответственно, z – коэффициент доверия, который определяется на основе табличных значений в зависимости от вероятности P, σ_w^2 – дисперсия доли TN (FP) в выборке:

$$\sigma_w^2 = w(1-w), \tag{5}$$

где w – доля TN (FP) в выборке легитимных объектов.

Набор веб-бэкдоров формируется за счет типической выборки, пропорциональной объему групп [11].

Предельная ошибка выборки для доли в таком случае будет вычисляться по формуле:

$$\Delta_{w_{TP}} = \Delta_{w_{FN}} = z\sqrt{\frac{\overline{\sigma_w^2}}{N_{\text{вб}}}}, \tag{6}$$

где $\Delta_{w_{TP}}$, $\Delta_{w_{FN}}$ - предельные ошибки для доли TP и FN соответственно, $\overline{\sigma_w^2}$ – средняя из групповых дисперсий типических групп для w_{TP} (w_{FN}).

Средняя из групповых дисперсий $\overline{\sigma_w^2}$ вычисляется по формуле:

$$\overline{\sigma_w^2} = \frac{\sum_{j=1}^{k} \sigma_j^2 N_j}{\sum_{j=1}^{k} N_j} \tag{7}$$

где N_j – количество элементов в j-й типической группе, k – количество типических групп (или видов веб-бкэдоров, которые должен выявлять СОВБ), σ_j^2 – дисперсия выборочной доли в j-й типической группе. Дисперсия выборочной доли в j-й типической группе определяется по формуле:

$$\sigma_j^2 = w_j(1-w_j), \tag{8}$$

где w_j – выборочная доля TP (FN) в j-й типической группе.

Вычислив предельные ошибки можно представить доверительные интервалы для значений $w_{TP}^*, w_{TN}^*, w_{FP}^*, w_{FN}^*$:

$$\begin{gathered} w_{TP} - \Delta_{w_{TP}} \le w_{TP}^* \le w_{TP} + \Delta_{w_{TP}}, \\ w_{TN} - \Delta_{w_{TN}} \le w_{TN}^* \le w_{TN} + \Delta_{w_{TN}}, \\ w_{FP} - \Delta_{w_{FP}} \le w_{FP}^* \le w_{FP} + \Delta_{w_{FP}}, \\ w_{FN} - \Delta_{w_{FN}} \le w_{FN}^* \le w_{FN} + \Delta_{w_{FN}}, \end{gathered} \tag{9}$$

Для малых объемов выборок, при невозможности вычислить $\overline{\sigma_w^2}$, можно ограничить это значение. Пусть в наборе есть k видов веб-бэкдоров, тем самым в каждой подгруппе будет $\frac{N_{\text{вб}}}{k} = m$ веб-бэкдоров (согласно выборке, предложенной в предыдущем разделе, количество элементов в каждой j-й типической группе будут равны).

Средняя выборочная доля TP (для FN проводятся аналогичные вычисления) равна:

$$\overline{w}_{TP} = \frac{\sum_{j=1}^{k} w_{TPj} N_j}{\sum_{j=1}^{k} N_j} = \frac{\sum_{j=1}^{k} w_{TPj}}{k}, \tag{10}$$

где w_{TPj} – доля TP в $j-$ й подгруппе, N_j – количество веб-бэкдоров в каждой подгруппе (равно m).

Согласно формулам (7) и (10) получаем:

$$\overline{\sigma_w^2} = \overline{w}_{TP} - \frac{\sum_{j=1}^{k} {w_{TP}}_j^2}{k} \tag{11}$$

С другой стороны:

$$\overline{w}_{TP} = \frac{TP}{N} = \frac{\sum_{j=1}^{k} TP_j}{N}, \tag{12}$$

$$\sigma_{\overline{w}}^2 = \overline{w}_{TP}(1 - \overline{w}_{TP}) = \overline{w}_{TP} - {\overline{w}_{TP}}^2, \tag{13}$$

где $\sigma_{\overline{w}}^2$ – дисперсия средней выборочной доли, $TP_j -$ количество TP соответственно в j-й типической группе.

Из неравенства Коши-Буняковского [12] получаем, что:

$${\overline{w}_{TP}}^2 = (\frac{\sum_{j=1}^{k} {w_{TP}}_j}{k})^2 \leq \frac{\sum_{j=1}^{k} {w_{TP}}_j^2}{k} => \ \sigma_{\overline{w}}^2 \geq \overline{\sigma_w^2} \tag{14}$$

Тем самым вычислив $\sigma_{\overline{w}}^2$, можно использовать его вместо $\overline{\sigma_w^2}$, однако это приведет к увеличению предельной ошибки.

Зная доверительные интервалы для $w_{TP}^*, w_{TN}^*, w_{FP}^*, w_{FN}^*$, можно также ограничить значения Re^*, Ac^*, Pr^* (истинные значения Re, Ac, Pr соответственно).

1) Оценка Re^*

$$Re = \frac{TP}{TP+FN} = \frac{TP}{N_{\text{вб}}} = w_{TP}.$$

Из неравенств (9) следует:

$$Re - \Delta_{w_{TP}} \leq \ Re^* \leq \ Re + \Delta_{w_{TP}} \tag{15}$$

2) Оценка Ac^*

$$Ac = \frac{TP + TN}{TP + TN + FP + FN} = \frac{TP + TN}{2N} = \frac{1}{2}w_{TP} + \frac{1}{2}w_{TN}$$

Согласно неравенствам (9):

$$Ac^* = \frac{1}{2}w_{TP}^* + \frac{1}{2}w_{TN}^* \leq \frac{1}{2}\left(w_{TP} + \Delta_{w_{TP}}\right) + \frac{1}{2}\left(w_{TN} + \Delta_{w_{TN}}\right) = Ac + \frac{\Delta_{w_{TP}} + \Delta_{w_{TN}}}{2}.$$

Аналогично доказывается с другой стороны.

Отсюда получается:

$$Ac - \frac{\Delta_{w_{TP}} + \Delta_{w_{TN}}}{2} \ \leq \ Ac^* \leq \ Ac + \frac{\Delta_{w_{TP}} + \Delta_{w_{TN}}}{2} \tag{16}$$

3) *Оценка* Pr^*.

Pr через w_{FP} и w_{TP} выражается так ($w_{TP} > 0$):

$$Pr = \frac{TP}{TP + FP} = \frac{\frac{TP}{N}}{\frac{TP}{N} + \frac{FP}{N}} = \frac{1}{1 + \frac{w_{FP}}{w_{TP}}}$$

Согласно неравенствам (9):

$$Pr^* = \frac{1}{1 + \frac{w^*_{FP}}{w^*_{TP}}} \leq \frac{1}{1 + \frac{w_{FP} - \Delta_{w_{FP}}}{w_{TP} + \Delta_{w_{TP}}}} = \frac{w_{TP} + \Delta_{w_{TP}}}{w_{TP} + w_{FP} + \Delta_{w_{TP}} - \Delta_{w_{FP}}} \quad (17)$$

$$Pr^* = \frac{1}{1 + \frac{w^*_{FP}}{w^*_{TP}}} \geq \frac{1}{1 + \frac{w_{FP} + \Delta_{w_{FP}}}{w_{TP} - \Delta_{w_{TP}}}} = \frac{w_{TP} - \Delta_{w_{TP}}}{w_{TP} + w_{FP} + \Delta_{w_{FP}} - \Delta_{w_{TP}}}, \text{при } w_{TP} > \Delta_{w_{TP}} \quad (18)$$

Таким образом, исходя из того, какой по объему набор тестовых данных, можно с вероятностью P найти доверительные интервалы, в которых находятся истинные значения показателей результативности Re^*(15), Ac^*(16), Pr^* (17-18).

Пример

Пусть СОВБ должно обнаруживать 64 вида веб-бэкдоров. Сформированный минимальный тестовый набор состоит из 64 легитимных объектов и 64 веб-бкэдоров по одной реализации на каждый вид веб-бэкдора. При проведении тестирования данной средство выдало следующие результаты: TP – 27, $TN - 62$, $FP - 2$, $FN - 37$. Определим доверительные интервалы для показателей результативности Re, Ac, Pr. Коэффициент доверия z будем вычислять для $P = 0.997$.

Согласно (6), (14):

$$\Delta_{w_{TP}} = \Delta_{w_{FN}} = z\sqrt{\frac{\overline{\sigma^2_w}}{64}} \leq z\sqrt{\frac{\sigma^2_{\overline{w}}}{64}} = z\sqrt{\frac{\overline{w}(1-\overline{w})}{64}} = 3\sqrt{\frac{\frac{27}{64}\cdot\frac{37}{64}}{64}} \approx 0.185$$

Согласно (4):

$$\Delta_{w_{FP}} = \Delta_{w_{TN}} = z\sqrt{\frac{w(1-w)}{64}} = 3\sqrt{\frac{\frac{62}{64}\cdot\frac{2}{64}}{64}} \approx 0.065$$

Тогда:

$$0.422 - 0.185 \leq w^*_{TP} \leq 0.422 + 0.185$$
$$0.578 - 0.185 \leq w^*_{FN} \leq 0.578 + 0.185$$
$$0.031 - 0.065 \leq w^*_{FP} \leq 0.031 + 0.065$$
$$0.969 - 0.065 \leq w^*_{TN} \leq 0.969 + 0.065$$

Отсюда, согласно (15-18):

$$0.422 - 0.185 \leq Re^* \leq 0.422 + 0.185$$
$$0.711 \leq Pr^* \leq 1$$
$$0.695 - 0.125 \leq Ac^* \leq 0.695 + 0.125$$

Как следует из последних расчетов, доверительные интервалы для показателей результативности достаточно широкие, что указывает на необходимость увеличения объема выборки с целью их сужения.

Выводы

Многие исследователи производят оценку показателей результативности функционирования СОВБ исключительно на основе собственных наборов данных, что делает эту оценку не полностью объективной.

В настоящей статье предложен метод, позволяющий вычислить показатели результативности функционирования СОВБ с использованием статистической теории. Вместо получения «точечных» значений, предлагается формирование доверительных интервалов, которые обеспечивают более полное представление о полученных результатах.

К факторам, влияющим на ширину доверительного интервала, относятся размер выборки, изменчивость выборки и доверительная вероятность нахождения показателя в данном интервале.

Существенным аспектом является также качество формирования тестового набора данных для проведения испытаний.

Для этого необходимо произвести всесторонний анализ всех возможных типов веб-бэкдоров, которые должны быть обнаружены СОВБ, и создать набор данных с учетом равновероятного использования злоумышленником различных видов веб-бэкдоров.

Литература

1. Боровков В.Е., Ключарёв П.Г. Методы защиты веб-приложений от злоумышленников // Вопросы кибербезопасности. 2023. № 5(57). С. 89-99.

2. Wu Y., Sun Y., Huang C., Jia P., Liu L. Session-Based Webshell Detection Using Machine Learning in Web Logs // Security and Communication Networks. 2019. Vol. 2019. P. 1-11.

3. Ma M., Han L., Zhou C. Research and application of artificial intelligence based webshell detection model: A literature review // Cryptography and Security. 2024. Pp. 1-21.

4. Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 // Труды Института системного программирования РАН. 2020. № 32(5). С. 81-94.

5. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn, Keras и Tensorflow: концепции, инструменты и техники для создания интелектуальных систем, 2-е изд.: Пер. с англ. –СПб.: ООО «Диалектика». 2020. 1040 с.

6. Zhu T., Weng Z., Fu L., Ruan L. A Web Shell Detection Method Based on Multiview Feature Fusion // Applied Sciences. 2020. Vol. 10(18). Pp. 1-16.

7. Pu A., Feng X.., Zhang Y., Wan X., Han J., Huang C. BERT-Embedding-Based JSP Webshell Detection on Bytecode Level Using XGBoost. // Security and Communication Networks. 2022. Pp. 1-11.

8. Nguyen N., Le V., Phung V., Du P. Toward a Deep Learning Approach for Detecting PHP Webshell // SoICT 2019: Proceedings of the Tenth International Symposium on Information and Communication Technology. 2019. Pp. 514-521.

9. Zhang H., Liu M., Yue Z., Xue Z., Shi Y., He X. A PHP and JSP Web Shell Detection System with Text Processing Based on Machine Learning // 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2020. Pp 1584-1591.

10. Илышев А.М. Общая теория статистики. Учебник для студентов вузов, обучающихся по специальностям экономики и управления. М.: ЮНИТИ. 2012. 535 с.

11. Статистические методы анализа данных / Ниворожкина Л.И. [и др.]. М.: РИОР. 2016. 333 с.

12. Соловьев Ю.П. Неравенства. М.: МЦНМО, 2005. 16 с.

Determination of Confidence Intervals for Performance Indicators of Web Backdoor Detection Tools

Borovkov V.E.[27], Klyucharev P.G.[28]

Abstract. The article considers the problem of assessing the effectiveness of the functioning of web backdoor detection tools (WBDT). In modern works, researchers often use their own data sets to test the effectiveness of the WBDT, which can lead to bias in the results obtained. To solve this problem, a method is proposed based on the formation of test datasets taking into account a special sample, as well as on the application of statistical theory to calculate confidence intervals for WBDT performance indicators. The formation of test suites is based on the analysis of various types of web backdoors that must be identified by detection tools. The objectivity of the results is ensured by the fact that instead of "point" values, confidence intervals are provided, depending on the volume of test datasets. This work may be useful for specialists and researchers in the field of information security who want to conduct a more objective assessment of their WBDT.

Keywords: web backdoors, web shells, testing methods and tools, performance indicators, detection tools, security tools.

[27] Vladislav Borovkov, doctoral student of Information Security department, Bauman Moscow State Technical University, Moscow, Russia, vbscience@yandex.ru

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

УДК 004.043 : 378.146

О результатах автоматизированной проверки на плагиат исходного кода на языке Си++ у студентов, обучающихся по специальностям, связанных с информационной безопасностью

Быков А.Ю.[29]

В статье представлены результаты проверки на плагиат при выполнении контрольных работ по написанию программ на языке Си++, проверяемых в автоматическом режиме. Для сравнения программ использовался метод, заключающийся в сравнении текстовых представлений программ на основе различных метрик. В частности, использовались метрики: Дамерау-Левенштейна и метрика на основе вычисления m-грамм. Представлены результаты сравнения программ на сходство при выполнении контрольной работы в одной из групп студентов. Сделаны выводы о параметрах проверки на плагиат по представленным метрикам.

Ключевые слова: язык программирования, автоматизированная проверка исходного кода, мера сходства, сравнение строк, метрика

Введение

При обучении языкам программирования, а также для защиты авторских прав разработчиков программных продуктов возникает задача выявления плагиата в исходных кодах программ. По некоторым источникам, больше половины студентов технических специальностей хотя бы раз нечестно сдавали задания по программированию [1-3].

Существует множество открытых и проприетарных решений [4], так или иначе решающих данную задачу: из открытых, например, популярны MOSS и JPlag. Многие из этих систем сканируют интернет на поиск похожих программ и (или) являются отдельными программными средствами, плохо сопрягаемыми с другими программными продуктами.

В статье рассматривается решение частной задачи. Есть готовое учебное интернет-приложение, аналогичное [5], но которое используется для обучения студентов языку Си++. Одна из реализуемых функций приложения является разгрузка студентами исходного кода программы, реализующей заданное задание, например, при выполнении контрольной работы. Код компилируется на сервере, запускается приложение с тестовыми данными, выходные результаты тестов сравниваются с правильными заранее заданными данными. Процесс проверки выполняется автоматически. При выполнении контрольной работы, в случае если вариантов заданий не много, возникает проблема плагиата. Ниже представлены используемые методы проверки, встроенные в учебное интернет-приложение и полученные результаты проверки работ студентов, обучающихся по специальностям, связанными с информационной безопасностью (ИБ). Различные аспекты подготовки специалистов в области ИБ рассмотрены в [6-9].

1. Описание используемых методов проверки на плагиат

В соответствии с [1-4] выделяют четыре основных типа заимствования исходного кода:

[29]Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

1. Программный код скопирован без каких-либо изменений (идентичен оригиналу с точностью до комментариев).

2. Код скопирован с простыми заменами идентификаторов (имен функций, переменных, классов и т.п.).

3. Код может включать заимствования второго типа, а также модификации скопированного оригинала путем добавления, редактирования или удаления его фрагментов или изменение порядка их исполнения, не влияющие на логику самой программы.

4. Программа некоторым образом переписана с общим сохранением логики работы и функциональности, однако синтаксически она может абсолютно отличаться от оригинала.

Учитывая, что студенты впервые изучают язык программирования и пишут относительно простые программы, важно выявлять плагиат 1-го и 2-го типов, плагиат 3-го и 4-го касается более-менее тех, кто уже умеет программировать.

По анализу литературы [1-4] можно выделить 5 основных подходов к выявлению плагиата в программах:

1. Text-based метод заключается в сравнении текстовых представлений программ на основе некоторой метрики, например расстояния Левенштейна и (или) других метрик.

2. Token-based метод основан на преобразовании ключевых слов программы в последовательность лексем языка программирования (далее просто токенов). Полученные токены сравниваются любым доступным способом.

3. Metric-based метод определяет на полученных в предыдущем методе токенах некоторые метрики (например, кол-во используемых циклов и условных конструкций), а далее считает схожесть программ на основе количества совпадающих метрик.

4. Tree-based подход требует представления кода в виде абстрактного синтаксического дерева (Abstract Syntax Tree). Далее требуется алгоритм сравнения деревьев.

5. Binary-based метод требует прохождения кодом этапа компиляции. Полученное бинарное представление (ассемблерный листинг или байт-код) служит основой для дальнейшего сравнения программ.

Все перечисленные подходы имеет свои достоинства и недостатки. Остановимся более подробно на первом подходе. Данный способ отличается своей скоростью и простотой, недостатком считается, что результативность быстро снижается даже на простейших модификациях программы.

Будем рассматривать исходный код как строку символов. Для этого выполняется предварительныя обработка. Содержимое каждого файла исходного кода (файлы с расширениями cpp, h, hpp и другие) записывается в строку, при этом удаляются комментарии и все символы-разделители. Все строки, соответствующие файлам с расширением cpp, соединяются в одну строку, при этом вместо директивы #include включения заголовочного файла, входящего в проект, вставляется строка, задающая этот заголовочный файл. Вставка производится один раз, при повторном включении этого файла директивой include вставка не производится. Д

ля сравнения строк были выбраны две метрики: Дамерау-Левенштейна и метрика на основе вычисления m-грамм. Эти метрики также часто используются в задачах, связанных с проблемами ИБ [10, 11]. Расстояние Дамерау-Левенштейна – это мера разницы двух строк символов, определяемая как минимальное количество операций вставки, удаления, замены и транспозиции (перестановки двух соседних символов), необходимых для перевода одной строки в другую. Является модификацией расстояния Левенштейна: к операциям вставки, удаления и замены символов, определённых в расстоянии Левенштейна добавлена операция транспозиции (перестановки) символов. Расстояние может быть переведено в меру близости или сходства по формуле:

$$\mu = \frac{r_{max} - r}{r_{max}}, \quad (1)$$

где r – расстояние, вычисленное по некоторой метрике, r_{max} – максимальное расстояние возможное между объектами, в решаемой задаче, $\mu \in [0,1]$ – мера близости. Для расстояния Дамерау-Левенштейна r_{max} равно максимальной длине строки из двух сравниваемых.

Мера сходства на основе m-грамм [12] между двумя строками X и Y вычисляется по формуле:

$$\mu_m = \frac{2m(X,Y)}{m(X)+m(Y)}, \quad (2)$$

где $m(X)$ и $m(Y)$ число m-грамм в строках X и Y, соответственно, $m(X,Y)$ – число m-грамм, входящих в строку X и в строку Y, независимо от позиции расположения. m-граммами называются сочетаний из m смежных символов.

Алгоритм вычисления параметров для m-грамм работает следующим образом. Задается значение m, для каждой строки выбирается m-грамма в начале начиная с 1-го символа, далее со 2-го символа и т.д. пока правая граница m-граммы не дойдет для конца строки. Эти m-граммы сохраняются в словаре (карте), ключом является m-грамма (дублирование ключей запрещено), значением – целое-счетчик повторения m-граммы в строке. Далее перебираем m-граммы (ключи) во второй строке и строим для нее второй словарь по такому же алгоритму.

На следующем шаге сравниваем два словаря на повторение m-грамм и считаем сумму повторений, начальное значение суммы равно 0. Если есть m-грамма в двух словарях, то к сумме прибавляем минимальное значение для этого ключа из двух словарей. Это сумма представляет значение $m(X,Y)$ из формулы (2). Знаменатель в (2) вычисляется как сумма значений всех ключей в двух словарях.

2. Результаты проверки на плагиат в одной учебной группе

В любом случае данные методы проверки на плагиат будут давать меру сходства даже для разных программ, так как в них используются ключевые слова из одного множества этих слов. Тестирование в учебной группе выполнялось на задании, в котором требовалось создать один класс, например, класс для хранения данных о студенте, содержащий следующие данные: фамилия, имя, отчество, оценки, полученные за период обучения (возможные значения оценки 3, 4 или 5). Методы и конструкторы определить самому. На вход программы поступают данные: число объектов и данные каждого объекта, на выходе программа должны вывести данные в определенном формате после сортировки объектов.

Предварительно тестирование сравнения совершенно разных программ на основе m-грамм с разными значениями m показало, что при m=1 или m=2, результаты сходства могут быть достаточное большими, начиная с m=3, они падают. Например, 0.66 при m=1, 0.45 при m=2, 0.33 при m=3, далее сходство уменьшается, на разных примерах порядок цифр был похожий. Поэтому решено при реальной проверке работ студентов использовать пять значений m: 3, 4, 5, 6, 7. Алгоритм сравнения разных работ работал так: первая работа не сравнивалась ни с чем при загрузке ее на сервер, каждая следующая сравнивалась со всеми загруженными ранее, выявлялись наиболее близкие работы по средним значениям разных измерений.

Результаты сравнений разных работ, которые выполнялись без списывания студентами, обучающимися на оценки отлично и хорошо представлены (табл. 1). В последнем столбце таблицы приведено среднее значение меры сходства по всем проведенным измерениям. При этом, как показал анализ при просмотре программы преподавателем, студент под № 6 в этой таблице со средним значением сходства 0,46 использовал одинаковую функцию с другой работой.

Таблица 1.

Результаты сравнения работ без плагиата

№ п/п	Сходство по Дамерау-Левенштейна	Сходство на основе m-грамм					Среднее значение сходства
		m=3	*m*=4	*m*=5	*m*=6	*m*=7	
1.	0,23	0,39	0,32	0,29	0,25	0,23	0,29
2.	0,37	0,37	0,30	0,25	0,22	0,18	0,28
3.	0,38	0,46	0,37	0,30	0,25	0,21	0,33
4.	0,33	0,37	0,30	0,25	0,22	0,18	0,28
5.	0,30	0,40	0,29	0,22	0,17	0,14	0,25
6.	0,48	0,56	0,51	0,45	0,41	0,37	0,46

Студенты не были заранее предупреждены о проверке на наличие плагиата, поэтому первые списывающие получили меру схожести по всем параметрам с одной из программ, уже загруженных на сервер равную 1, об этом студенты получили сообщение. Для повторной сдачи началась модификации программ, в основном заменой идентификатор. Результаты второго этапа сдачи, тех кто заимствовал чужую программу, представлены (табл. 2).

Таблица 2.

Результаты сравнения работ с плагиатом при замене идентификаторов

№ п/п	Сходство по Дамерау-Левенштейна	Сходство на основе m-грамм					Среднее значение сходства
		m=3	m=4	m=5	m=6	m=7	
1.	0,74	0,80	0,76	0,72	0,68	0,65	0,73
2.	0,75	0,75	0,70	0,66	0,62	0,58	0,68
3.	0,74	0,73	0,68	0,63	0,59	0,55	0,65
4.	0,95	0,90	0,86	0,83	0,80	0,77	0,85
5.	0,57	0,60	0,54	0,49	0,44	0,40	0,51
6.	0,88	0,86	0,83	0,80	0,77	0,74	0,81

Выводы

Приведены результаты проверки на плагиат студенческих программ на языке Си++ с использованием различных метрик и их параметров. Сравнительный анализ метрик на основе расстояния Дамерау-Левенштейна и на основе *m*-грамм показал относительно близкие результаты, мера сходства при увеличении значения *m* уменьшалась. При принятии решения о наличии плагиата в программе условно рекомендуется ввести границу по среднему значению меры сходства на уровне 0,4-0,5. Граница в интервале 0,7-0,8 может быть использована для приема контрольных работ со снижением оценки, в этом случае можно считать, что студент частично разобрался в работе во время правки исходного кода в основном путем замены идентификаторов и других косметических изменений.

Литература

1. Огнева Т.А., Лапшева Е.Е. Применение кластеризации в задаче поиска плагиата в программном коде // Информационные технологии в образовании. 2023. № 6. С. 254-259.

2. Гусев С.С. Методы анализа произвольных текстов и исходных кодов программ с точки зрения наличия идентичных фрагментов // В сборнике: Анализ, моделирование, управление, развитие социально-экономических систем (АМУР-2022). сборник научных трудов XVI Международной школы-симпозиума АМУР-2022. Симферополь, 2022. С. 124-132.

3. Егоров А.Н., Леверьев В.С. Поиск заимствований в текстах исходных кодов на примере олимпиадного программирования // В сборнике: Современные информационные технологии, инновации и молодежь - "СИТИМ-2023". Материалы Всероссийской студенческой научно-практической конференции с международным участием. Ульяновск, 2023. С. 78-82.

4. Тихов Д.С., Абрамова О.Ф. Обзор программных средств автоматизации определения уникальности текста с целью выявления плагиата // Научно-практические исследования. 2020. № 1-4 (24). С. 106-111.

5. Быков А.Ю., Глинская Е.В. Образовательный ресурс для дисциплины "Математическое моделирование" с использованием средств имитационного моделирования на основе технологии облачных вычислений // Свидетельство о регистрации программы для ЭВМ RU 2017616539, 08.06.2017. Заявка № 2017611815 от 02.03.2017.

6. Кузнецова В.Ю. Аспекты оценки эффективности подготовки специалистов в области информационной безопасности // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2019. С. 230-232.

7. Басараб М.А., Бельфер Р.А., Кравцов А.В. Учебный имитатор объединенной отечественной сети ПД специального назначения (структура, функции) // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2019. С. 12-18.

8. Дорофеев А.В., Марков А.С. Обучение специалистов в области кибербезопасности в стиле Purple Team // Защита информации. Инсайд. 2023. № 6 (114). С. 66-71.

9. Царегородцев А.В. Кадры решают всё: назад в будущее // Безопасные информационные технологии. Сборник трудов XII международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2023. С. 146-149.

10. Бутусов И.В., Романов А.А. Предупреждение инцидентов информационной безопасности в автоматизированных информационных системах // Вопросы кибербезопасности. 2020. № 5 (39). С. 45-51. DOI:10.21681/2311-3456-2020-05-45-51

11. Соколова Т.В., Чеповский А.М. Проблема восстановления профилей пользователей социальных сетей // Вопросы кибербезопасности. 2019. № 4 (32). С. 88-93. DOI: 10.21681/2311-3456-2019-4-88-93

12. Гайдамакин Н.А. Мера сходства последовательностей одинаковой размерности // Математические структуры и моделирование. 2016. № 4 (40) . С. 5–16

On the results of automated plagiarism testing of C++ source code for students studying in information security-related specialties

Bykov A.Yu. [30]

The article presents the results of plagiarism checks during the execution of tests on writing programs in C++, checked in automatic mode. To compare the programs, a method was used consisting of comparing text representations of programs based on various metrics. In particular, the following metrics were used: Damerau-Levenshtein and a metric based on calculating m-grams. The results of comparing programs for similarity during the execution of a test in one of the student groups are presented. Conclusions are made about the parameters of plagiarism checks based on the presented metrics.

Keywords: programming language, automated source code verification, similarity measure, string comparison, metric.

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

УДК 004.056

О схемах и протоколах выполнения криптосистем по доверенности на основе симметричных криптоалгоритмов

Варфоломеев А.А.[31]

Аннотация. Рассмотрены и проанализированы основные схемы и протоколы криптосистем по доверенности (Proxy Cryptosystems), использующие только симметричные алгоритмы для обеспечения секретности и/или аутентичности передаваемых или хранимых больших объемов данных. Данное ограничение связано с большой вычислительной сложностью асимметричных алгоритмов. Наряду с перешифрованием по доверенности (Proxy Re-Encryption) и цифровой подписью по доверенности (Proxy Signature) выделяется цифровая имитовставка по доверенности (Proxy Re-Authentication). Приведены рекомендации по улучшению разработанных схем и протоколов для их более эффективного использования.

Ключевые слова: криптография, доверие, секретность, аутентификация

Введение,

Впервые понятие выполняемых по доверенности криптосистем появилось в работах [1] применительно к асимметричным шифрам (Proxy Re – encryption, PRE, для краткости - прокси перешифрование). Далее это понятие было перенесено на выполняемые по доверенности цифровые подписи (Proxy Signature, PS, для краткости – прокси подпись), которые являлись тоже реализацией асимметричных алгоритмов. Прокси перешифрование позволяет доверенному лицу (прокси) преобразовать шифртекст, полученный на одном (открытом) ключе, в шифртекст, который может быть расшифрован на другом (закрытом) ключе, входящим в другую ключевую пару. Прокси подпись позволяет передать право на генерацию цифровой подписи доверенному лицу без передачи своих секретных ключей подписи. К настоящему времени было разработано большое количество предложений по реализации прокси криптосистем, в основном с применением асимметричных криптоалгоритмов. Во многих приложениях данные хранятся зашифрованными с помощью симметричных шифров. Этому есть объяснение ввиду высокой скорости выполнения этими шифрами операций зашифрования и расшифрования больших объемов информации, где асимметричные шифры не столь эффективны. В случае использования симметричных шифров необходимость в прокси перешифровании также актуальна, но имеет некоторые отличия от асимметричного случая.

Классические симметричные шифры обеспечивают только секретность данных, в то время как современные шифры обеспечивают дополнительно и подлинность отправителя и целостность [2]. Это так называемое аутентифицированное шифрование (Authenticated Encryption - AE) и аутентифицированное шифрование с присоединенными данными (Authenticated Encryption with Associated Data - AEAD). В связи с этим возникает необходимость рассмотрения использования таких шифров в условиях передачи доверенной стороне выполнения этих операций. Конечно, прокси подпись решает задачу обеспечения подлинности данных, но она, как правило, использует вычислительно сложные асимметричные алгоритмы. К тому же обеспечиваемое цифровой подписью требование неотказуемости (non-repudation) может не являться необходимым в информационных системах. Поэтому актуальным является обеспечение только аутентичности информации с применением симметричных алгоритмов типа вычисления

[31] Варфоломеев Александр Алексеевич, к.ф.-м.н., доцент, МГТУ им. Н.Э. Баумана, г. Москва, a.varfolomeev@mail.ru

имитовставки или кода аутентификации сообщения (MAC), и использовать для краткости термин Прокси имитовставка или Прокси MAC (Proxy Re-Authentication – PRA).

Известные протоколы симметричной Прокси криптографии и комментарии к ним

Под термином Прокси - имитовставки или Прокси - MAC (Proxy Re-Authentication – PRA) можно понимать изменение по доверенности отдельным лицом (прокси) имитовставки, полученной на одном ключе какого-нибудь участника, на имитовставку на другом ключе этого участника без раскрытия ключей имитовставки этому лицу, а с помощью специального преобразования, зависящего от этих ключей. При этом сами данные остаются открытыми для чтения и копирования.

В одной из первых работ по прокси перешифрованию с симметричным шифром является работа [3]. Доверенный прокси является шлюзом между пользователями A и B и выполняет перешифрование сообщения. Предложенные 2 варианта реализации протокола используют двойное шифрование. В обоих вариантах отправитель A разделяет общий секретный ключ Kas с шлюзом S и ключ Kab с получателем B. В первом варианте B также имеет секретный ключ Kbs с шлюзом S. Передаваемый текст M не доступен прокси – шлюзу, так как шифруется на общем ключе A и B.

1 вариант.

A: E_Kas(E_Kab(M)) = C1 -→ S.

S: E_Kbs(D_Kas(C1) = C2 → B. (в этом варианте C2 = E_Kbs(E_Kab(M))).

B: D_Kab(D_Kbs(C2) = D_Kab(D_Kbs(E_Kbs(E_Kab(M)) = M.

2 вариант.

A: E_Kas(E_Kab(M)) = C1 -→ S.

S: D_Kas(C1) = C2 → B. (в этом варианте C2 = E_Kab(M)).

B: D_Kab(C2) = D_Kab(E_Kab(M)) = M.

Здесь через E и D обозначены преобразования зашифрования и расшифрования на соответствующих ключах любого выбранного шифра. Из приведенного описания следует, что во всех вариантах возможна замена шифрования на шифрование с аутентификацией и аутентификацией с присоединенными данными. Существуют варианты и со схемой прокси имитовставки. Но, в отличие от рекомендаций в работе [3], основанными на представленных атаках типа «встреча посередине», можно рекомендовать не исключать такие шифры в схемах перешифрования, а просто учитывать эти факты при выборе параметров безопасности.

В работе [4] предлагается следующий алгоритм преобразования двоичного открытого текста m = m0, m1, … , m(s-1), разделенного на s блоков по b бит.

1. Сначала ОТ преобразуется с помощью AONT преобразования в псевдо открытый текст из n блоков m’ = m’0, m’1, … , m’(n-1) по b бит.

2. Переставляются блоки псевдотекста m’ по перестановке P3, m’= Perm (P3, m’).

3. Далее блоки ШТ получаются по правилу

C_0 = Perm (P1, m’0) XOR Perm (P2, Kx),

C_i = Perm (P1, m’i) XOR Perm (P2, C(i-1), (*)

[можно сравнить с Cipher Feedback (CFB) - Ci = m’i XOR E(K, c(i-1)],

где секретными ключевыми перестановками являются перестановки P1 и P2 на b битах и P3 на n блоках, а также b битовый ключ Kx.

Подобный способ получения шифртекста из текста известен и обобщается для произвольных преобразований с ключом:

C_i = E(P1, m’i) XOR E(P2, C(i-1). m’i = DE(P1, (Ci XOR E(P2, C(i-1)).

Но дополнительное применение алгоритма зашифрования E(…, …) и обратного к нему преобразования DE(…, …) приводит к увеличению сложности всего процесса зашифрования - расшифрования. Перестановка Perm(…,…) координат векторов размера b требует гораздо большего времени, чем операция XOR, но не изменяет вероятностных

характеристик аргумента, оставляя количество нулей и единиц неизменным. Именно операция XOR меняет и выравнивает вероятностные характеристики слагаемых.
Например, если вероятность 1 в слагаемых Perm (P1, m'i) и Perm (P2, C(i-1) или m'i и C(i-1), равна p, то в самой сумме она равна 2p(1-p). (Для p=0,1;0,2;0,3;0,4;0,5 имеем 0,18;0,32;0,42;0,48;0,5 соответственно). Если использовать 2 сложения XOR, то выравнивание частот будет еще большим. Поэтому для ускорения шифрования можно предложить следующее соотношение

Ci = m'i XOR Perm (P2, C(i-1) XOR C(i-2)), положив C(-1) =0.

Дальнейшее ускорение операций зашифрования-расшифрования, при контроле за стойкостью, можно достичь изменением алгоритма выработки ключевых перестановок. При больших значениях числа блоков n и размера блоков b требуется большой размер памяти для перемещения элементов блоков и самих блоков. В исходной работе не обсуждается ни значения n и b, ни функция зашифрования E(k,p).

Можно предложить для сокращения временной и емкостной сложности, заменить алгоритм генерации перестановки на алгоритм генерации так называемой скользящей перестановки.

С работой [4], использующей преобразование AONT, связана работа [5], в которой описывается улучшенная схема повторного прокси шифрования для симметричного шифра, используя другой вариант функции AONT. Показывается, что предложенная схема безопасна при атаке по выбранному открытому тексту (CPA) для всех возможных типов противников.

В работе [6] симметричное прокси перешифрование (Symmetric Proxy Re-encryption) предлагается выполнять с использованием нового вводимого примитива, такого как гомоморфная по ключу псевдослучайная функция (Key Homomorphic PRF, KH-PRF). Безопасная псевдослучайная функция (PRF) F: K × X → Y называется гомоморфной по ключу**,** (или ключевой гомоморфной PRF – KH-PRF) если для заданных F(k1, x) и F(k2, x) существует эффективный алгоритм вычисления F(k1 ⊕ k2, x), где ⊕ обозначает групповую операцию над k1 и k2, такую как xor.

Пусть G — конечная циклическая группа простого порядка q, и пусть H1 :X →G — хэш-функция, рассматриваемая как случайный оракул. Определим функцию F_DDH : Zq ×X →G как F_DDH(k, x) = H1(x)^k, и заметим, что F_DDH(k1+k2, x) = F_DDH(k1, x) ▪ FDDH(k2, x). Наор, Пинкас и Рейнгольд [7] показали, что F_DDH — это безопасная PRF в модели случайного оракула, предполагая, что в G выполняется решательное предположение Диффи-Хеллмана.

Аналогично в работе строится гомоморфная по ключу PRF на основе предположений о трудности задач из теории решеток. В частности, рассматривается задача Обучения с Округлением (Learning with Rounding - LWR [8]. Однако очевидно, что эти предложения требуют большой вычислительной сложности, что не выполнимо при больших объемах информации.

Важным усовершенствованием схем прокси перешифрования из работы [6] являются схемы SA-PRE (symmetric authenticated proxy re-encryption), предложенные в работе [9]. Такие схемы обеспечивают не только секретность текста, но и аутентичность. В практическом плане предлагаемый вариант прокси перешифрования пригоден только при малых объемах защищаемого текста. При больших объемах текста, особенно размещаемого в облаках, более эффективны алгоритмы из работ [4] и [5] на основе перестановок блоков и содержания блоков текста. Кроме того, эти алгоритмы могут быть использованы для обеспечения аутентифицированного шифрования (AE) и аутентифицированного шифрования с присоединенными данными (AEAD).

Показательными являются работы [10] и [11], в первой из которых излагается протокол AKAPR (Authenticated Key Agreement mediated by a Proxy Re-Encryptor) согласования ключа между двумя пользователями с использованием прокси

перешифрования и центра генерации долговременных ключей. Во второй работе представлены атака маскировки и атака на форвардную секретность, которая должна обеспечивать безопасность предыдущих сеансовых ключей при компрометации настоящих долговременных ключей. Заслуживают в этом плане внимания и работы [12-18].

Выводы

В связи с увеличением значимости технологий облачных вычислений и облачного хранения данных, расширением технологий Интернета вещей, умными городами и зданиями, другими современными цифровыми технологиями возрос интерес к применению криптографических схем и протоколов прокси перешифрования, прокси подписи, а также прокси имитовставки с применением симметричных алгоритмов. Имеющиеся схемы и протоколы, решающие данные задачи могут быть усовершенствованы для обеспечения большего сервиса без снижения криптографической стойкости.

Найденные атаки не препятствуют использованию разработанных протоколов, а ведут к достижимому изменению параметров стойкости.

Работа проводилась при поддержке АНО НТЦ ЦК «Цифровая криптография».

Литература

1. Blaze M., Bleumer G., Strauss M. Divertible protocols and atomic proxy cryptography // EUROCRYPT. Lecture Notes in Computer Science. Vol. 1403 Berlin: Springer-Verlag, 1998 P. 127–144.

2. Математические основы информационной безопасности / Басараб М.А., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г. и др.: Под ред. Матвеева В.А. - М.: МГТУ им.Н.Э.Баумана, 2013. -244 с.

3. Cook, D.L., Keromytis, A.D.: Conversion and proxy functions for symmetric key ciphers. In: ITCC, pp. 662–667 (2005)

4. Syalim, T. Nishide, and K. Sakurai, "Realizing proxy re-encryption in the symmetric world," in International Conference on Informatics Engineering and Information Science. Springer Berlin Heidelberg, 2011, pp. 259–274.

5. Amril Syalim, Takashi Nishide, Kouichi Sakurai: Improved Proxy Re-encryption Scheme for Symmetric Key Cryptography

6. D. Boneh, K. Lewi, H.W. Montgomery, and A. Raghunathan, "Key homomorphic PRFs and their applications," in CRYPTO 2013, 2013, pp. 410–428.

7. Naor M., Pinkas B., Reingold O., Distributed Pseudo-random Functions and KDCs, Eurocrypt 1999, 327-346.

8. 7. Peikert C., Rosen A., Banerjee A., Pseudorandom Functions and Lattices, Eurocrypt 2012, 719-737/

9. Zhiniang Peng, Shaohua Tang, and Linzhi Jiang. A Symmetric Authenticated Proxy Re-encryption Scheme with Provable Security. Springer International Publishing AG 2017 X. Sun et al. (Eds.): ICCCS 2017, Part II, LNCS 10603, pp. 86–99.

10. K. T. Nguyen, N. Oualha, and M. Laurent. Authenticated key agreement mediated by a proxy re-encryptor for the internet of things. In European Symposium on Research in Computer Security, pages 339{358. Springer, 2016. ESORICS 2016.

11. 2016/1081 D. Nuñez, I. Agudo, J. Lopez , Attacks to a proxy-mediated key agreement protocol based on symmetric encryption

12. Canetti, R., Hohenberger, S.: Chosen-ciphertext secure proxy re-encryption. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 185–194. ACM (2007).

13. Hirose, S.: On re-encryption for symmetric authenticated encryption. In: Computer Security Symposium, CSS 2010 (2010).

14. Libert, B., Vergnaud, D.: Unidirectional chosen-ciphertext secure proxy re-encryption. IEEE Transactions on Information Theory 57(3), 1786–1802 (2011).

15. H. Sakazaki, K. Anzai, and J. Hosoya. Study of re-encryption scheme based on symmetric key cryptography. In 31st Symposium on Cryptography and Information Security (SCIS2014), 2014.

16. CELLOS Consortium. Evaluation report: Symmetric key re-encryption scheme with proxy (SK-REP). Technical report, CELLOS consortium, 2014.

17. W. C. Garrison, A. Shull, S. Myers, and A. J. Lee. On the practicality of cryptographically enforcing dynamic access control policies in the cloud. In 2016 IEEE Symposium on Security and Privacy (SP), pages 819{838, May 2016.

18. Dai Watanabe, Hisao Sakazaki, Kunihiko Miyazaki, Representative System and Security Message Transmission using Re-encryption Scheme Based on Symmetric-key Cryptography.

19. Rizky Putri, Meiliasari Amril, Syalim Setiadi Yazid, Performance Analysis of the Symmetric Proxy Re-encryption Scheme, October 2019 DOI:10.1109/IWBIS.2019.8935670 Conference: 2019 International Workshop on Big Data and Information Security (IWBIS).

On the schemes and protocols for implementing proxy cryptosystems based on symmetric cryptoalgorithms

Varfolomeev A.A.[32]

The article reviews and analyzes the main schemes and protocols of proxy cryptosystems that use only symmetric algorithms to ensure the secrecy and/or authenticity of large amounts of data being transmitted or stored. This limitation is due to the high computational complexity of asymmetric algorithms. Along with proxy re-encryption and proxy digital signature, proxy re-authentication is distinguished. Recommendations are given for improving the developed schemes and protocols for their more efficient use.

Keywords: cryptography, trust, secrecy, authentication

[32] Varfolomeev A.A., Ph.D., Associate Professor, BMSTU, Moscow, a.varfolomeev@mail.ru

УДК 004.89

О применении интеллектуальных агентов в вычислительных системах

Голосов П.Е.[33]

В данной статье показана возможность замены планировщика на два типа интеллектуальных агентов (ИА), встроенных в специализированную распределенную вычислительную систему (СРВС). Данная архитектура, использованная в имитационной модели СРВС и построенная в среде Simulink (SimEvent), классифицируется в теории массового обслуживания как G/G/n/∞ и ориентирована на параллельное выполнение определенного класса задач, разделяемых на подзадачи, независимые по данным. Отличительной особенностью таких систем является обработка непрерывных нестационарных потоки со строгим ограничением по времени выполнения задач. Необходимость использования таких агентов обусловлена жесткими требованиями ко времени обработки задач, превышение которого приводит к отказу всей системы. Применение таких интеллектуальных агентов позволяет отказаться от планировщика задач. В данной работе продемонстрировано управление с использованием двух интеллектуальных агентов, первый из которых позволяет регулировать количество подзаданий, на которые разделяется поступающая в систему задача, а второй — назначать повышенные приоритеты задачам при увеличении среднего времени их выполнения. Оба агента работают независимо друг от друга и обеспечивают выполнение всех поступивших задач за заданное время.

Ключевые слова: высокопроизводительные вычисления; планировщики; интеллектуальные агенты; задачи с ограничениями на время обработки.

1. Введение

Определение процесса планирования очерёдности выполнения процессов в операционной системе (ОС) является одной из ключевых задач при их разработке и эксплуатации. От качества работы планировщика зависит эффективность работы самой ОС. Поскольку планировщик обеспечивает балансировку использования основных ресурсов ОС, то от него в конечном счете зависит и производительность взаимосвязанных компонент вычислительной системы. С развитием вычислительной техники быстродействие процессоров существенно повысилось, увеличилось быстродействие оперативной памяти, механизмов обмена с файловыми носителями и существенно возросла скорость передачи информации по сетям. Все это привело к объединению компьютеров в сеть с образованием различных вычислительных архитектур. Для обеспечения их совместного функционирования необходим уже глобальный планировщик. Однако функции его мало изменились. Такие планировщики обеспечивают балансировку нагрузки отдельных серверов.

В настоящее время существенно возросли интенсивности входных потоков задач для подавляющего большинства вычислительных систем. Будем исследовать поведение многомашинного варианта — распределенной специализированной вычислительной системы (СРВС), решающей задачи специального класса, методы выполнения которых можно определить как случайный перебор с неизвестным исходом [1,2]. Для таких систем и поступающих задач характерны некоторые важные признаки: сами задачи при обработке разделяются на заранее неизвестное количество эквивалентных подзадач (ветвей), обладая независимостью по данным, кроме того, для каждого типа задачи заранее определено

[33] Голосов Павел Евгеньевич, к.т.н., руководитель научных проектов Исследовательского центра искусственного интеллекта Института общественных наук Российской академии народного хозяйства государственной службы при Президенте Российской Федерации, Москва, e-mail: golosov-pe@ranepa.ru

предельное время, за которое необходимо получить решение. В этих случаях входной поток нескольких классов одновременно поступающих задач становится нестационарным, а поведение системы обработки слабо поддается аналитическому прогнозированию эффективности работы.

Классическое планирование выполнения задач в таких системах обычно реализовано с использованием некоторой целевой функции, которая оптимизирует некоторый параметр. В ОС реального времени это сокращение времени обслуживания, а в ОС разделения времени — это балансировка времени выполнения всех задач в системе. Однако предварительные исследования показывают, что для решения задач за некоторое реальное время в этих системах имеется существенная избыточность вычислительных ресурсов. Этот факт объясняется тем, что элементарные планировщики, такие как FCFS (First Come First Served), SPN (Shortest process next), SJF (Shortest-Job-First), HRRN (Highest Response Ratio Next), RR (Round Robin), (MLFQ) Multi-Level Feedback Queue [3,4,5], просто не имеют целевой функции и не оптимизируют процесс балансировки. Сложные планировщики, такие как MAUI [6,7], DAGMan [8]. Pegasus [9], HEFT (Heterogeneous Earliest Finish Time) [10], FCP (Fast Critical Path) и DSC (Dominant Sequence Clustering) [11], MPQGA (Multiple priority queues genetic algorithm) [12] и многие другие основаны на пакетной обработке входного потока задач. Это означает, что они собирают некоторый набор задач и оптимизируют время его выполнения. Однако поступление новых задач с ограничениями на время обработки в период планирования (для алгоритмов с явной целевой функцией) инициирует процесс перепланирования, тем самым потенциально снижая загруженность системы. В некоторых системах такие процессы перепланирования занимают до 25% всего вычислительного времени. Поэтому основной задачей управления СРВС становится обеспечение своевременного обслуживания всех поступающих задач в систему с минимизацией вычислительных ресурсов. Для решения задачи рационального управления применены интеллектуальные агенты, которые позволяют отказаться от классических планировщиков и возложить управление вычислительной системой на них. Цель статьи заключается в демонстрации работы интеллектуальных агентов, применяемых для управления СРВС.

2. Постановка задачи и моделирование

Поскольку проведение экспериментов на реальной вычислительной системе невозможно по ряду причин, то проверка гипотезы о применении интеллектуальных агентов в качестве элементов обеспечения обработки задач была проведена в среде имитационного моделирования [13]. При рассмотрении различных систем имитационного моделирования выделяется среда Simulink как часть системы MatLab. Пакет SimEvent, входящий в Simulink, предоставляет наиболее развитую, совершенную среду событийного моделирования. Содержит все необходимые для моделирования блоки и позволяет дополнять их функциональность программно [14-16].

Рассмотрим СРВС, в которую поступает непрерывный поток задач разных классов. В данном случае закон распределения времени поступления задач не является предметом рассмотрения, так как после их поступления в систему они разделяются на заранее неизвестное число независимых по данным подзадач и обрабатываются параллельно. Очевидно, что такой поток подзадач становится нестационарным и его невозможно охарактеризовать ни математическим ожиданием, ни дисперсией. Однако, для такого потока можно ввести характеристику, названную удельной интенсивностью потока, относительно всего периода моделирования. Она будет рассчитываться как общая трудоемкость всех поступивших в систему задач, отнесенная к некоторому временному отрезку, исчисляемому от начала моделирования до текущего момента [17]. Пример графика такой удельной интенсивности представлен на рис. 1.

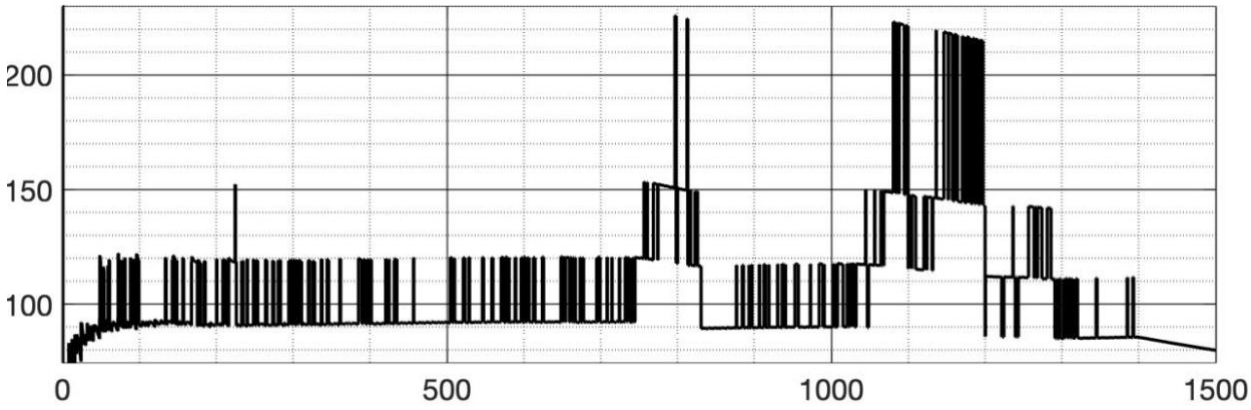


Рис. 1. Пример график поведения удельной интенсивности для нестационарного потока

С другой стороны, необходимо определить некоторую величину, характеризующую производительность вычислительной системы. Для её определения на выходе системы контролировался выходной поток решенных задач интенсивность которого определялась измерялась в значениях интегральной продуктивности [18].

Здесь нужно сделать замечание относительно максимальной производительности вычислительной системы. Пусть в системе имеется n-серверов (устройств обработки), предположим, что на вход системы поступает непрерывный поток задач единичной длины. Тогда максимальная производительность системы будут определяться данным количеством серверов. Значение средней удельной интенсивности входного потока должно соответствовать значению интегральной продуктивности выходного потока в силу закона Литтла.

В моделируемой системе классические планировщики были заменены на два типа интеллектуальных агентов. Интеллектуальный агент первого типа представляет собой систему спорадического управления количеством подзадач. Входом для него служит статистически усредненная длина очереди задач на выполнение. Выходом является число, характеризующие количество подзадач, на которое должна разделяется задача на входе системы.

Интеллектуальный агент второго типа основан таких же принципах спорадического управления и предназначен для изменения приоритетов задач. На его вход поступает статистическая информация о среднем времени выполнения задач каждого типа. На выходе этого агента подзадачи, направляемые в очередь, получают приоритет, который будет тем выше, чем большее время этот класс задач стоит в очереди.

Приведем реальные цифры результатов моделирования. Генерация задач в среде Matlab/Simulink проводилась на интервале 0-1400, при общем времени моделирования 0-1500. В модели было использовано 32 сервера, работающие на временном интервале 0-1400 с. Для моделирования были выбраны четыре типа задач со временем выполнения, равным 160, 100, 64 и 32 с. Были проведены несколько серий экспериментов, с равновероятным законом генерации задач с интервалами [0...18], [0...12], [0...8], [0...6] и общим среднем числом задач 1220 (155, 237, 352, 476) по классам, соответственно. Были получены следующие усредненные результаты.

Общая трудоемкость всех поступивших задач в систему – 92 896 с. Средняя интегральная продуктивность для всего периода моделирования – 18 973,75. Количество обслуженных подзадач – 35602. Среднее время нахождения задач в очереди – 2,107 с. Средняя длина очереди – 53,53. Остаточное количество задач в очереди - 0. Средняя мгновенная продуктивность системы – 63,24. Средняя удельная интенсивность поступления задач в очередь – 66,358.

Эти результаты свидетельствуют о полном выполнении закона Литтла. На входе 66,358 задач единичной длины в условиях нестационарности потока соответствуют 63,24 выполненным задачам единичной длины.

3. Выводы и заключение

Проведенные эксперименты по моделированию систем с нестационарными интенсивными входными потоками показало:

– Классические планировщики можно полностью заменить интеллектуальными агентами (ИА). Причем в данной конфигурации вычислительной системы эти агенты не взаимодействуют друг с другом. Два таких ИА работают абсолютно независимо друг от друга. Поэтому назвать такую систему управления СРВС мультиагентной системой в прямом смысле слова нельзя [19, 20], поскольку в ней нет механизмов взаимодействия агентов. Однако некоторые авторы относят такие системы к дискретным мультиагентным или к одноуровневой [архитектуре] мультиагентной системе, ориентированной на решение задач планирования [21, 22].

– Особенностью таких ИА является их полная независимость от размера и конфигурации вычислительной системы. То есть при масштабировании СРВС алгоритмические и технологические свойства агентов не требуется изменять.

– Еще одной особенностью таких ИА является их независимость от интенсивности входного потока и класса решаемых в вычислительной системе задач. То есть такие ИА обладают инвариантностью работы в системах с априорной неопределенности входных потоков.

На основании вышеизложенного можно сделать вывод о целесообразности применения ИА в различных вычислительных системах, предназначенных для решения задач в условиях ограниченного времени обработки и доступных ресурсов.

Список использованной литературы

1. Malashenko, Yu.E., Nazarova, I.A.: Control Model for Heterogeneous Computational Tasks Based on Guaranteed Estimates of Execution Times // J. Comput. Syst. Sci. Int. 2012. V. 51, P. 526–534;

2. Kupalov-Yaropolk, I.K., Malashenko, Y.E., Nazarova, I.A., Ronzhin, A.F.: Evaluation Methods for Efficiency and Directive Terms of Performance of Resource- intensive Computing Tasks // Informatika i Ee Primeneniya [Informatics and its Applications]. 2013. V.7. P. 17–25;

3. Silberschatz's Operating System Concepts. John Wiley & Sons.– 2019. – 896 p.

4. Michael L. Pinedo Scheduling Theory, Algorithms, and Systems. Springer Science New York 2008, DOI: 10.1007/978-0-387-78935-4

5. Stallings W. Operating systems: internals and design principles, 7th. ed., 2012

6.Maui Administrator's Guide. [Electronic resource]. – Access mode: http://www.adaptivecomputing.com/resources/docs/maui/pdf/mauiadmin.pdf.

7.MAUI scheduler [Electronic resource]. – Access mode: http://www.adaptivecomputing.com/products/open-source/maui/.

8. The directed acyclic graph manager, condor project. [Electronic resource]. – Access mode: http://www.cs.wisc.edu/condor/dagman/.

9. Deelman, E., Singh, G., Su, M.-H., Blythe, J., Gil Y., Kessel-man, C., Mehta, G., Vahi, K., Berriman, G.B., Good, J., Laity, A., Jacob, J.C., and Katz, D.S. Pegasus: a Framework for Mapping Complex Scientific Workflows onto Distributed Systems / E. Deelman, G. Singh, M.-H. Su, J. Blythe, Y. Gil, C. Kessel-man, G. Mehta, K. Vahi, G. B. Berriman, J. Good, A. Laity, J. C. Jacob, and D. S. Katz. // Scientific Programming Journal. – 2005, vol. 13, pp. 219-237.

10. Topcuoglu, H., Hariri, S., Wu, M.Y. Performance-effective and low complexity task scheduling for heterogeneous computing / H. Topcuoglu, S. Hariri, MY Wu // IEEE Transactions on Parallel and Distributed Systems. – 2002; No. 13(3), pp. 260–274.

11.181.Yoosefi, A. and Naji, H.R. A Clustering Algorithm for Communication-Aware Scheduling of Task Graphs on Multi-Core Reconfigurable Systems / Yoosefi and H.R. Naji // IEEE Transactions on Parallel and Distributed Systems. – 2017, vol. 28, no. 10, pp. 2718-2732.

12. Xu, Y. et al. A genetic algorithm for task scheduling on heterogeneous computing systems using multiple priority queues / Y. Xu et al. // Information Sciences, 2014, Vol. 270, pp. 255-287.

13. Моделирование компьютерных сетей / Басараб М.А., Колесников А.В., Коннова Н.С. - Москва, Издательство МГТУ им. Н. Э. Баумана, 2021. – 86 с.

14. MathWorks. 2016. Simulink User's Guide. MathWorks, R2016a, Natick, MA.

15. MathWorks. 2016. SimEvents, User's Guide. MathWorks, R2016a, Natick, MA.

16. MathWorks. 2016. Writing S-Functions. MathWorks®, Release R2016a, Natick, MA.

17. Голосов П.Е., Боловцов С.В., Полукошко М.М., Гостев И.М. О производительности специализированной распределенной вычислительной системы, построенной на основе интеллектуальных агентов. // Материалы XXVII Международной научной конференции Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2024) 2024.

18. Голосов П.Е., Гостев И.М. Анализ эффективности имитационных моделей облачных вычислений с использованием элементов искусственного интеллекта // Радиотехнические и телекоммуникационные системы. М. 2023. No 2. С. 29-39.

19. FIPA (Federation of Intelligent Physical Agents - Home Page). // URL: http://www.cselt.stet.it/fipa/fipa_rationale.htm.;

20. Haag, Stephen. «Management Information Systems for the Information Age», 2006. Pages 224—228;

21. M.Wooldridge and N.R.Jennings. Agent Theories, Architectures, and Languages: A Survey. In: Intelligent Agents. // ECAI-94 Workshop on Agent Theories, Architecture and Languages. Amsterdam, The Netherlands, August 8-9, 1994, (Eds. M.J.Wooldridge and N.R.Jennings). Proceedings. Springer Verlag: 3-39, 1994;

22. M.Wooldridge, J.M.Muller and M.Tambe. Agents, theories, architectures and languages. // (ATAL- 95) Springer Verlag Lecture Notes in Artificial Intelligence (LNAI 1037).

On the application of intelligent agents in computing systems

Golosov Pavel[34]

This paper shows the possibility of replacing the scheduler with two types of intelligent agents (IAs) embedded in a specialized distributed computing system (SDCS). The simulation model of the SDCS is built in the Simulink (SimEvent) environment and is classified as G/G/n/∞ in mass service theory. The system architecture is oriented on parallel execution of a certain class of tasks divided into data-independent subtasks. A distinctive feature of such systems is the necessity to process continuous non-stationary flows of input tasks with a strict limitation on execution time. This brings the necessity of using such agents. Exceeding of execution time leads to the failure of the whole system. The usage of such intelligent agents makes it possible to completely abandon the task scheduler. This paper demonstrates task management by two intelligent agents, the first of which allows to regulate the number of subtasks into which a task is divided, and the second assigns higher priorities to tasks when the average time of their execution increases. Both agents work independently and ensure that all incoming tasks are completed at a given time.

Keywords: high-performance computing; schedulers; intelligent agents; tasks with processing time constraints.

[34] Pavel E. Golosov, Ph.D., Scientific Project Supervisor of Artificial Intelligence Research Centre, Institute for Social Sciences, Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia, e-mail: golosov-pe@ranepa.ru

УДК 004.03

Blockchain как средство подтверждения подлинности дипломов

Давидюк Н.В.[35], **Немчинов Ф.Д.**[36]

Данная статья посвящена разработке системы проверки подлинности дипломов на основе технологии Blockchain. В современном образовательном контексте обеспечение достоверности документов играет критическую роль, и Blockchain предлагает эффективное решение благодаря своей децентрализации и криптографической безопасности. В статье рассматриваются различные виды Blockchain и их применимость для создания системы проверки дипломов. Особое внимание уделено приватному Blockchain как оптимальному выбору для обеспечения конфиденциальности данных и эффективности проверки подлинности.

Ключевые слова: верификация, приватный Blockchain, информационная безопасность, образовательные технологии

Введение

В современном мире, где образование играет ключевую роль в личной и профессиональной жизни, проверка подлинности дипломов становится все более актуальной задачей. Подделка дипломов не только нарушает доверие к образовательной системе, но и может привести к серьезным последствиям для лиц, использующих поддельные документы. Blockchain, благодаря своим уникальным свойствам, таким как децентрализация, неизменность данных и криптографическая безопасность, представляет собой оптимальное решение для создания надежной системы проверки подлинности дипломов. В этой статье приводится анализ существующих методов проверки подлинности и проектируется система проверки подлинности дипломов на основе Blockchain.

Виды Blockchain

Ключевым аспектом разработки системы на основе Blockchain является выбор его вида. Существуют 4 вида: публичный (Public), частный (Private), гибридный (Hybrid), консорциум (Consortium) [1]

Публичный Blockchain — это сеть, позволяющая общественности свободно участвовать в деятельности. Каждому пользователю предоставляются равные права на просмотр и проверку текущей деятельности Blockchain через узел. Узел позволяет пользователям взаимодействовать с другими пользователями, подобно виртуальному профилю, который в электронном виде отслеживает их действия в сети.

Разрешенный или частный Blockchain является противоположностью публичного Blockchain. Это Blockchain, к которому только избранные пользователи могут получить доступ и присоединиться по приглашению, что делает его более безопасным, чем другие. Так как Blockchain все так же работает автономно, даже владельцы Blockchain не могут изменить транзакции.

Гибридный Blockchain сочетает в себе элементы как частного, так и общедоступного Blockchain. Это позволяет организациям создавать закрытые системы на основе разрешений, параллельно с открытыми системами без разрешений. Такая комбинация позволяет контролировать доступ к определенным данным, хранящимся в Blockchain, и определять, какие данные будут доступны для общего просмотра.

Blockchain консорциума сочетает в себе несколько гибридных Blockchain, которые решают потребности организаций. Несколько гибридных Blockchain связаны между собой с помощью мостов, что дает преимущество в скорости, но ущерб безопасности, так как мост является самым уязвимым местом в Blockchain.

[35] Давидюк Надежда Валерьевна, к.т.н., доцент, АГТУ, Астрахань, davidyuknv@bk.ru
[36] Немчинов Федор Денисович, студент, АГТУ, Астрахань, nemchinow2018@mail.ru

Была составлена таблица преимуществ и недостатков каждого вида Blockchain, в рамках разработки системы проверки подлинности дипломов (табл.1).

Таблица 2.

Виды Blockchain

Вид	Преимущества	Недостатки
Публичный	Автономность	Прозрачность Безопасность
Частный	Контроль доступа Производительность Безопасность Автономность	Масштабируемость
Гибридный	Контроль доступа Производительность Безопасность Автономность	Прозрачность
Консорциум	Контроль доступа Масштабируемость	Прозрачность Безопасность

Анализ существующих решений

Для эффективного проектирования системы проверки подлинности дипломов на основе Blockchain, важно провести анализ текущих исследований и статей по этой тематике. Это позволит выявить существующие недостатки и ограничения, а также определить возможности для улучшения.

Так, в статье «Блокчейн как сервис защиты информации о подлинности дипломов об образовании» [2], авторы предлагают решение на основе консорциум Blockchain, что не является оптимальным решением. Да, этот вид Blockchain является одним из безопасных, но политика безопасности менее строга, чем в частных Blockchain. В данном виде Blockchain валидаторами выступают узлы из разных организаций, что в системе проверки подлинности дипломов не является логичным. Если эта система будет внедрена в разные учебные заведения, то лишь та организация, которая выдает дипломы, будет генерировать блок, а остальные организации будут “поставлены на поток” и автоматически его согласовывать. Гораздо более логичным будет использовать частный Blockchain, использовать группу валидаторов из узлов текущей организации, которые будут генерировать новый блок и согласовывать его. Примером другого подхода является статья «Верификация дипломов по технологии блокчейн» [3]. Автор использует приватную сеть Ethereum, в качестве инструмента развертывания был выбран Ganache с использованием технологии удаленного вызова процедур RPC и так же для дальнейшего взаимодействия со смартк-контрактами был выбран MyEtherWallet и язык программирования Solidity, что является относительно правильным решением на 2020 год. Но на данным момент существуют более подходящие технологии. Hyperledger fubricx [4-6], который был создан для удобного развертывания и взаимодействия с частными Blockchain сетями. Он использует технологию gRPC, в отличии от традиционного RPC, эта технология является более безопасной и эффективной, так как использует формат Protobuf вместо JSON. Данный формат является наиболее эффективным для сериализации и десериализации данных. Он имеет меньший размер, что при создании блока может быть критичным, и производительней, так как использует бинарный формат передачи данных. Так же Hyperledger поддерживает различные языки программирования: GO, JavaScript, Java, в отличии от Ethereum, который использует контрактно-ориентированный, ограниченный по функциональности язык Solidity[7-11].

В рассмотренных примерах были затронуты базовые ошибки, которые встречаются и у других авторах, за исключением выбора публичного Blockchain, что не выполняет требований конфиденциальности.

Верификация дипломов

Исходя из проведенного анализа было решено проектировать систему проверки подлинности диплома на базе частного Blockchain.

Система будет состоять из Blockchain и информационного хранилища. Информационное хранилище будет иметь структуру Ключ/Значение (map), где ключ – хэш диплома, а значение – файл/скан диплома (рис.1).

Ключ (хэш диплома)	Значение (файл/скан диплома)
e58f1e8c55fa105bdd	

Рис.1. Визуализация структуры Ключ/Значение

Перед выдачей диплома выпускнику, файл/скан диплома передается в цифровое хранилище, оно, в свою очередь, записывает хэш в свою структуру и возвращает его (рис.2).

Рис.2. Передача файла диплома

Блоки Blockchain будут так же состоять из структуры Ключ/Значение, но с добавлением хэша предыдущего блока (рис.3).

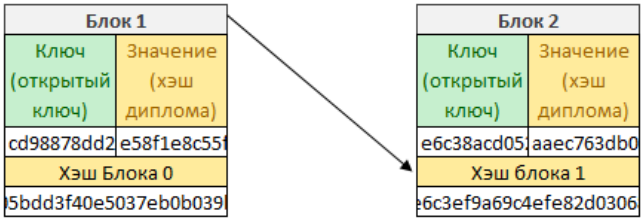


Рис.3. Визуализация структуры блока

После получения хэша диплома генерируется открытый ключ, далее хэш и ключ вносятся в новый блок Blockchain. После открытый ключ передается выпускнику (рис.4).

Если есть необходимость у работодателя проверить на подлинность диплом соискателя, он сможет это сделать с помощью WEB интерфейса, он должен запросить у выпускника его открытый ключ, который он должен вставить в поле ввода на интерфейсе, после чего ему будет выдан сам диплом соискателя, и он сможет проверить, существует ли он в базе университета, вносил ли выпускник изменения в бумажный диплом и соответствует ли он данным из университета (рис.5).

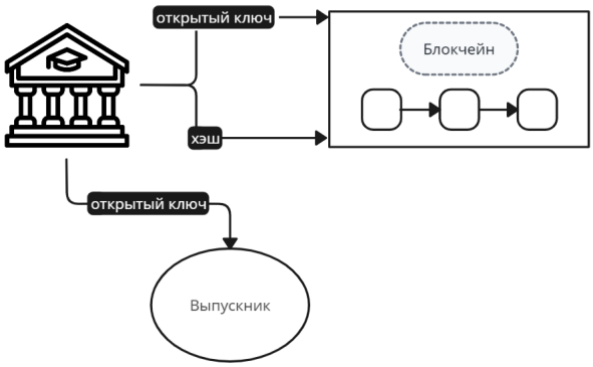


Рис.4. Передача данных

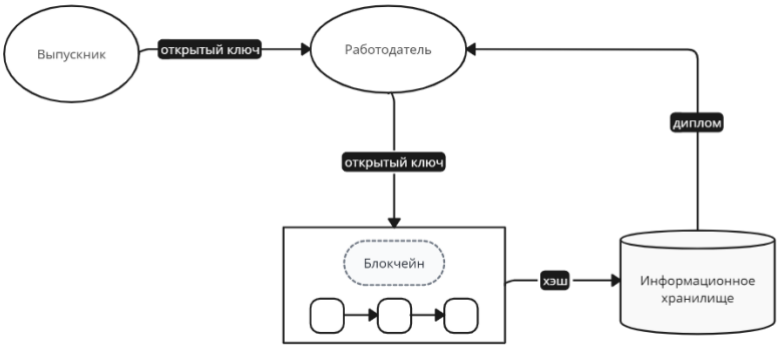


Рис.5. Верификация диплома

В данном случае все происходит в обратном порядке. После запроса от работодателя, происходит поиск блока, который содержим текущий открытый ключ. Так как, по сути, Blockchain является отсортированным, то есть блоки пронумерованы по возрастанию, есть возможность использовать алгоритм бинарного поиска, который сокращает количество перебранных блоков с n, до log n, где n – максимальное количество перебранных блоков. После нахождения нужного блока в информационное хранилище поступает хэш диплома, так как информационное хранилище представляет собой структуру данных map(таблица ключ/значение), поиск в ней занимает константное время O(1). Это значит, что время поиска не зависит от размера таблицы и остается постоянным. После нахождения нужного хэша работодатель получает проверенный диплом, с которым он может сравнить тот, который предоставил выпускник.

Вывод

Система разработана с целью повышения уровня информационной безопасности и сокращения времени, необходимого для проверки подлинности дипломов, интегрирует приватный Blockchain для обеспечения высокой степени защиты и отказоустойчивости. В сочетании с оптимизированными структурами данных и эффективными алгоритмами поиска, система способствует быстрому и безопасному доступу к информации о дипломах.

Литература

1. Какие бывают блокчейны и почему это важно знать. URL: https://www.ixbt.com/live/crypto/kakie-byvayut-blokcheyny-i-pochemu-eto-vazhno-znat.html (дата обращения: 24.09.2024).

2. В.В. Михаэлис, С.И. Михаэлис // Блокчейн как сервис защиты информации о подлинности дипломов об образовании // CyberLeninka URL: https://cyberleninka.ru/article/n/blokcheyn-kak-servis-zaschity-informatsii-o-podlinnosti-diplomov-ob-obrazovanii/viewer (дата обращения: 03.10.2024).

3. Ижик, В. А. Верификация дипломов по технологии блокчейн / В. А. Ижик, М. С. Жилин, Д. Г. Гочеев. — Текст : непосредственный // Юный ученый. — 2020. — № 5 (35). — С. 45-50. — URL: https://moluch.ru/young/archive/35/2052/ (дата обращения: 03.10.2024).

4. What Is Web3 and Why Does It Matter? // Binance Academy URL: https://academy.binance.com/en/articles/the-evolution-of-the-internet-web-3-0-explained (дата обращения: 26.09.2024).

5. Разработка и тестирование смарт-контрактов Hyperledger Fabric // Хабр URL: https://habr.com/ru/articles/426705/ (дата обращения: 11.09.2024).

6. Блокчейн и его влияние на экономику // Журнал экономики и бизнеса. — 2021. — Т. 12. — № 4. — С. 112-120. — URL: https://www.sciencedirect.com/science/article/pii/S1877042821001260 (дата обращения: 21.07.2024).

7. The Role of Blockchain in the Financial Sector // Journal of Financial Innovation. — 2022. — Vol. 8, Issue 1. — URL: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-022-00220-1 (дата обращения: 19.09.2024).

8. Санжаров, А. Б. Применение блокчейн-технологий в логистике / А. Б. Санжаров. — Текст : непосредственный // Научный вестник. — 2023. — № 2 (27). — С. 78-83. — URL: https://www.elibrary.ru/item.asp?id=47118996 (дата обращения: 03.10.2024).

9. Зеленов, Д. А. Блокчейн в управлении цепями поставок / Д. А. Зеленов. — Текст : непосредственный // Технологии и наука. — 2022. — № 3 (19). — С. 36-42. — URL: https://www.researchgate.net/publication/361234567_Blockchain_in_Supply_Chain_Management (дата обращения: 03.03.2024).

10. Blockchain Technology: Applications and Challenges // International Journal of Computer Applications. — 2021. — Vol. 174, No. 24. — URL: https://www.ijcaonline.org/archives/volume174/number24/28282-2021-04-11058068 (дата обращения: 21.09.2024).

11. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. -М.: НИИ РиЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.

Blockchain as a Means of Diploma Authentication

Davidyuk N.V.[37], Nemchinov F.D.[38]

This article focuses on the development of a diploma authentication system based on Blockchain technology. In the contemporary educational context, ensuring the authenticity of documents plays a critical role, and Blockchain offers an effective solution due to its decentralization and cryptographic security. The paper examines various types of Blockchain and their applicability for creating a diploma verification system. Special attention is given to private Blockchain as the optimal choice for ensuring data confidentiality and authentication efficiency

Keywords: verification, private Blockchain, information security, educational technologies

[37] Davidyuk Nadezhda Valeryevna, PhD (technical sciences), associate professor, Astrakhan State Technical University, Astrakhan, davidyuknv@bk.ru

[38] Nemchinov Fedor Denisovich Nemchinov, student, Astrakhan State Technical University, Astrakhan, nemchinow2018@mail.ru

УДК 004.932

Использование видеоданных и облака точек для предотвращения несанкционированного доступа

Дамдинов З.Ш.[39], **Дамдинова Т.Ц.**[40]

Аннотация

В современных условиях одним из основных факторов обеспечения информационной безопасности являются меры технической безопасности. Для предотвращения несанкционированного доступа к данным одним из наиболее важных инструментов выступают видеопотоки, которые могут служить надежным источником для анализа. Тема распознавания поведения человека с использованием нейронных сетей охватывает множество задач, включая анализ поз, распознавание действий, предсказание намерений и анализ эмоций. В последние годы применение технологий глубокого обучения, различных видов нейронных сетей, показали значительные успехи в решении этих задач. В статье представлены основные источники получения видеоданных, рассмотрено использование современных нейронных сетей для распознавания поведение человека.

Ключевые слова: защита информации, видеопоток, облако точек, искусственные нейронные сети, распознавание образов, распознавание поведения человека

Введение

Для организации мер технической защиты от несанкционированного доступа в информационной безопасности одним из ключевых способов является анализ данных видеопотока, которые могут использоваться для выявления фактов нарушения безопасности, подозрительного поведения человека. Обзор литературы последних лет показывает, что методы и средства получения и обработки цифровых данных продолжают развиваться и получили большой импульс благодаря использованию нейронных сетей. На протяжении последних лет ведутся активные исследования, направленные на улучшение качества получения, анализа и распознавания видеоданных [1-4]. Эти усилия способствуют повышению точности и надежности систем видеонаблюдения. Сочетание своевременного анализа, высоких стандартов автоматизации и качества видеопотока позволяет существенно повысить уровень безопасности и минимизировать риски несанкционированного доступа [5-7]. Научные исследования в данной области продолжат играть важную роль в разработке инновационных решений, обеспечивающих защиту данных.

Основные источники информации для распознавания поведения человека

В задачах распознавания поведения человека, рассматриваются следующие основные направления:

1. Распознавание позы и движений: Системы должны уметь детектировать положение человека в пространстве и его движения [8-12]. Это требует разработки моделей, которые работают с трехмерными данными или с последовательностями кадров для анализа динамики движений.

2. Анализ эмоций. При определении эмоционального состояние человека можно оценить по его мимике [13-15]. Это важно в контексте социального взаимодействия и систем управления взаимодействием с пользователями.

[39]Дамдинов Зоригто Ширипович, магистрант, Восточно-Сибирский государственный университет технологий и управления, г.Улан-Удэ, dzorigtoc@mail.ru

[40]Дамдинова Татьяна Цыбиковна, к.т.н., доцент, Восточно-Сибирский государственный университет технологий и управления, г.Улан-Удэ, dtatyanac@mail.ru

3. Распознавание действий [16-18]. Эта задача, связана с классификацией действий человека (например, ходьба, бег, прыжки и т.д.). Задача является достаточно сложной, поскольку каждое действие может быть представлено множеством вариаций.

4. Предсказание намерений. Эта задача, в которой система анализирует поведение и контекст, чтобы предсказать, что человек планирует сделать в будущем [19]. Решение данной задачи играет большую роль в информационной безопасности, где важно заранее предугадывать действия людей.

Основные источники информации для анализа и обработки данных, необходимых для распознавания поведения человека, могут быть представлены в виде видеопотока и получены с применением следующих устройств.

1. Аналоговые и цифровые камеры
2. Видеорегистраторы.
3. Смартфоны и планшеты, которые могут записывать видео и стримить его в реальном времени.
4. Системы видеоконференцсвязи, позволяющие обмениваться видеопотоками между пользователями в реальном времени.
5. Облачные платформы, которые могут транслировать и хранить видеопотоки с различных источников для последующего анализа.

Также для анализа данных используются информация в виде облака точек, которые представляют собой 3D-данные, содержащие информацию о геометрии объектов и их положении в пространстве [20-22]. Для их формирования могут быть использованы следующие устройства:

1. Стереокамеры позволяют генерировать облака точек с помощью анализа изображений, полученных с двух или более камер, что помогает реконструировать глубину сцены и пространственное положение объектов.
2. Современные RGB-камеры с алгоритмами оценок глубины сцены для создания облаков точек на основе цветного изображения.
3. Мобильные устройства со встроенными сенсорами и камерами для создания облаков точек с помощью программного обеспечения для дополненной реальности.
4. Беспилотники и дроны, оснащенные камерами и другими датчиками, способные осуществлять сканирование местности и объектов, генерируя облака точек для создания их 3D-модели в реальном времени.
5. Профессиональные 3D-сканеры, которые создают точные трехмерные карты объектов и окружающей среды, создают сетку из точек, представляющих геометрию объектов.
6. Лидарные датчики, используемые для создания трехмерных моделей окружающей среды, формируя плотное облако точек с высокоточной информацией о расстояниях до объектов.

Основные подходы распознавания на основе нейронных сетей.

Для автоматического обнаружения агрессивных действий или подозрительного поведения используются следующие виды нейронных сетей:

- **Сверточные нейронные сети (CNN)**. Эти сети показывают высокую эффективность в распознавании объектов и анализе изображений. Сверточные нейронные сети применяются для обработки изображений или видео для распознавания поз и движений. Они хорошо работают с двумерными изображениями, но для анализа 3D-данных (например, с использованием глубинных камер или 3D-сканеров) используются специализированные архитектуры, такие как 3D-CNN, которые обрабатывают последовательности кадров, позволяя выявлять динамические паттерны движений [23]. Эти сети обрабатывают отдельные кадры видео, позволяя идентифицировать и классифицировать объекты и действия. Они эффективны для распознавания поз, жестов и действий.

- **Рекуррентные нейронные сети (RNN)**. RNN-сети подходят для анализа временных зависимостей. Они могут эффективно обрабатывать последовательности данных, что позволяет предсказать следующее действие на основе предыдущих. Сети данного типа используются для анализа последовательностей кадров, что позволяет учитывать временные зависимости между действиями. Особенно популярны архитектуры LSTM (Long Short-Term Memory) для работы с временными рядами данных и широко применяются для обработки последовательностей данных, что необходимо для анализа временной динамики действий человека [24, 25].
- **Объединенные подходы**: **Гибридные сети (CNN + RNN)**: Одним из наиболее успешных подходов является использование гибридных сетей [26], которые объединяют возможности CNN и RNN для решения сложных задач распознавания поз и поведения на видео. CNN может обрабатывать отдельные кадры, извлекает пространственные характеристики с изображений, а RNN анализирует последовательность этих кадров и их временные зависимости между последовательными кадрами, что позволяет делать предсказания на основе контекста. Совмещение различных архитектур, например CNN для извлечения признаков и RNN для анализа динамики, может значительно повысить точность распознавания поведения.
- **Модели с использованием графов (GNN).** Сети, работающие на графовых структурах [27] позволяют более точно моделировать отношения между частями тела человека при анализе движений. Это может помочь в распознавании поз и взаимодействий.
- **Трансформеры.** Трансформеры нашли свое применение в видеоанализе, предлагая гибкие архитектуры для обработки последовательностей кадров [28]. Они могут учитывать более широкий контекст и предоставлять более точные результаты при распознавании сложных движений. Эти модели способны учитывать глобальные зависимости в данных и могут эффективно справляться с задачами классификации действий.

Выбор нейросетевых архитектур

Для решения задачи распознавания поведения человека в работе [2] применяются рекуррентные нейронные сети (RNN). Эти сети идеально подходят для анализа временных рядов на видео. Они способны запоминать информацию о предыдущих действиях, что позволяет им распознавать сложные паттерны поведения. В случае видеонаблюдения, где поведение человека может быть неочевидным и зависеть от контекста, использование RNN позволяет более точно определять действия, такие как ходьба, бег или взаимодействие с объектами. В статье упоминается использование скрытых марковских моделей (HMM) для классификации поведения с определенной вероятностью переходов между ними. Также используются гауссовские нечеткие модели для обучения параметров объектов в пространстве и методов кластеризации для обработки изображений. Нечеткие модели учитывают неопределенности в данных, что позволяет более эффективно работать с реальными видеопотоками, где условия освещения и качества могут варьироваться. Таким образом, выбор нейросетевых архитектур и алгоритмов в статье [2] обусловлен тем, что они специально адаптированы для обработки сложных, многослойных данных, свойственных видео. В статье [3] обсуждается новая система распознавания человеческих действий на видео, разработанная с акцентом на использование технологий глубокого обучения в условиях ограниченных ресурсов. Для решения задачи распознавания действий в реальном времени используется комбинация сетей, таких как MobileNetV2 и LSTM. MobileNetV2 выбрана за свою легкость и эффективность в извлечении признаков из изображений. Система использует подход, при котором вместо обработки всего изображения анализируются лишь ограниченные области, соответствующие обнаруженным объектам (bounding boxes). Это значительно снижает вычислительную нагрузку. Для точного определения действия, особенно в ситуациях, когда действия происходят быстро или накладываются друг на друга были выбраны LSTM сети. Основным преимуществом данного набора сетей является его способность выполнять задачи глубокого обучения в реальном времени на периферийных устройствах, что делает его применимым для широкого спектра сценариев, включая системы видеонаблюдения, мониторинг за поведением людей в разных областях.

В работе [17] рассматривается применение двухпотоковой архитектуры глубокого обучения для распознавания человеческих действий с возможностью одновременной обработки двух различных типов данных — видеопотока и дополнительных параметров, таких как информация о скелете или глубина. Эта комбинация позволяет модели не только захватывать пространственные характеристики изображений, но и анализировать временные аспекты действий. Использование CNN в данной архитектуре применяются для извлечения ключевых особенностей на изображении, начиная с простых форм, таких как линии и углы, и заканчивая более сложными структурами, такими как лица или тела. Рассмотрены RNN для распознавания динамических действий. Дополнительным преимуществом является внедрение механизмов внимания, которые позволяют модели сосредоточиться на наиболее значимых частях входных данных.

В [18] рассматривается применение глубоких нейронных сетей для распознавания действий человека на инфракрасных изображениях. Предлагается подход с использованием простой, но эффективной структуры с двумя слоями свертки. Адаптивный алгоритм RMSprop был использован для оптимизации процесса обучения, позволяя сети быстрее сходиться к оптимальным параметрам. Это особенно важно в контексте больших наборов данных, где требуется быстрая обработка и обучение. В результате, достигнутая точность в 87.44% значительно превосходит традиционные методы.

В [24] выделяется применение нейросетевых подходов, таких как LSTM и SNFIR (Sparse Nonlinear Function Input Regression). Как упоминалось, LSTM сети эффективно улавливают динамику изменений, SNFIR модели, в свою очередь, представляют собой регрессионные методы, оптимизирующие представление данных и выделяющие значимые признаки, что приводит к созданию разреженных моделей с активными коэффициентами, снижая риск переобучения. SNFIR. Этот метод отличается более быстрым временем обучения по сравнению с LSTM, что делает его практичным для реальных приложений.

В работе [25] представлен подход, который объединяет три передовые нейросетевые архитектуры: трехмерные свёрточные нейронные сети 3D CNN, нейронные LSTM сети с длинной краткосрочной памятью и механизм внимания. Этот гибридный метод обеспечивает более высокую точность и надежность распознавания действий. 3D CNN извлекают пространственно-временные признаки из видеопотока. Их способность одновременно анализировать изменения как в пространственном, так и во временном аспектах делает их идеальными для распознавания динамичных действий. Использование предварительно обученной модели Inflated 3D сокращает вычислительные затраты и ускоряет процесс обучения. Механизм внимания дополнительно усиливает эту систему, позволяя модели динамически фокусироваться на наиболее значимых признаках в видео. Это важно для фильтрации менее значимых фрагментов и выделения ключевых временных моментов, что в свою очередь повышает общую точность распознавания. В итоге, данный гибридный подход, который объединяет возможности 3D CNN, LSTM и механизма внимания, подчеркивает силу и гибкость современных нейросетевых архитектур.

В исследовании [26] разработана гибридная модель глубокого обучения для распознавания человеческих действий в видео, которая объединяет несколько мощных методов: Gaussian Mixture Model (GMM), Kalman Filter (KF) и Gated Recurrent Neural Network (GRNN). Этот подход выделяется своей способностью эффективно справляться с сложными задачами классификации действий, что делает его особенно привлекательным для динамичных видеопотоков. GMM используется для точного выделения движущихся объектов даже в шумных и сложных сценах. Данная модель реагирует на изменения фона, игнорирует статичные элементы и фокусируется на движении человека для обеспечения надежного трекинга. KF используется для оптимального предсказания при уточнении траектории движения. Вместе эти методы образуют гибридную модель, в которой трекинг и классификация работают в тесном взаимодействии. Такой интегрированный подход не

только снижает вычислительные затраты, но и улучшает устойчивость к изменениям в сцене, обеспечивая высокую точность на сложных наборах данных.

Заключение

Использование нейросетей для распознавания поведения и поз человека в области информационной безопасности открывает новые горизонты в защите данных и предотвращении угроз. Эти технологии позволяют не только эффективно идентифицировать потенциальные риски. Это значительно повышает уровень безопасности, позволяя оперативно реагировать на инциденты и минимизировать возможные потери. Системы, основанные на глубоких нейронных сетях, способны анализировать поведение пользователей в реальном времени, выявляя аномалии и подозрительные действия. Обзор исследований также указывают на необходимость дальнейших разработок гибридных моделей для решения сложных сцен и множественных действий. В целом, нейросети представляют собой мощный инструмент в арсенале информационной безопасности, и их дальнейшее развитие будет способствовать созданию более безопасной цифровой среды.

Литература

1. *Human Behavior Recognition of Video Surveillance System Based on Neural Network. https://www.sciencedirect.com/science/article/pii/S187705092301832X*
2. *A new framework for deep learning video based Human Action Recognition on the edge https://www.sciencedirect.com/science/article/pii/S0957417423027227*
3. *Азаренко К.А., Каунг Мьят Ньейн, Белов Ю.С. Обзор методов для распознавания действий человека // E-Scio. 2019. №5 (32).*
4. *Дамдинова Т.Ц. Способы формирования цифровых изображений и анализ их погрешностей // Вопросы кибербезопасности. 2014. № 5 (8). С. 43-46.*
5. *Гаврилов Д.А., Ловцов Д.А. Автоматизированная оптико-электронная система наземно-космического мониторинга для систем безопасности реального времени // Вопросы кибербезопасности. 2020. № 5 (39). С. 52-60.*
6. *Козьминых С.И., Татаренков В.С. Метод обнаружения подозрительных транзакций банковских клиентов на основе системы распознавания эмоций // Вопросы кибербезопасности. 2024. № 3 (61). С. 129-140.*
7. *Марков А.С. Техническая защита информации. М. АИСНТ. 2020. 234 с.*
8. *Squirrel Search Optimization with Deep Convolutional Neural Network for Human Pose Estimation. https://www.sciencedirect.com/org/science/article/pii/S1546221822003770*
9. *Human action recognition using a convolutional neural network based on skeleton heatmaps from two-stage pose estimation. https://www.sciencedirect.com/science/article/pii/S2667379722000249*
10. *Тимофеева О.П., Неимущев С.А., Неимущева Л.И., Тихонов И.А. Распознавание эмоций по изображению лица на основе глубоких нейронных сетей // Труды НГТУ им. Р. Е. Алексеева. 2020. №1 (128)*
11. *Бурякова О.С., Решетникова И.В., Черкесова Л.В. Система интеллектуального распознавания эмоций на основе технологии свёрточных нейронных сетей // Современные наукоемкие технологии. – 2022. – № 9. – С. 44-52*
12. *Галичий Д.А., Афанасьев Г.И., Нестеров Ю.Г. Распознавание эмоций человека при помощи современных методов глубокого обучения // E-Scio. 2021. №5 (56).*
13. *Human Pose Estimation Guide (2023) https://softwaremill.com/human-pose-estimation-2023-guide/*
14. *Two-Stream Deep Learning Architecture-Based Human Action Recognition. https://www.sciencedirect.com/org/science/article/pii/S1546221822003496*

15. Deep learning approach for human action recognition in infrared images. https://www.sciencedirect.com/science/article/abs/pii/S1389041717302206)

16. Human action recognition based on spatial–temporal relational model and LSTM-CNN framework https://www.sciencedirect.com/science/article/abs/pii/S2214785321076756

17. Применение нейронных сетей для предсказания физических действий человека / А.В. Подопросветов [и др.] // Препринты ИПМ им. М.В.Келдыша. 2021. № 109. 16 с. https://doi.org/10.20948/prepr-2021-109 https://library.keldysh.ru/preprint.asp?id=2021-109.

18. Дамдинова Т.Ц., Абатнин А.А Геометрическое моделирование объектов по облаку точек. В сборнике: VIII международная конференция Проблемы механики современных машин. Сборник статей конференции. Улан-Удэ, 2022. С. 380-386.

19. Дамдинова Т.Ц., Абатнин А.А., Мандаров Э.Б., Бальжинов В.В. Трансформация облака точек в формате stl в геометрические объекты. Свидетельство о регистрации программы для ЭВМ RU 2020611189, 27.01.2020. Заявка № 2020610379 от 21.01.2020.

20. Damdinova T.T. New method of boundary points description with given accuracy for objects recognition // CEUR Workshop Proceedings, 2021. Vol. 3035. P. 33-39.

21. Уздяев Михаил Юрьевич Распознавание агрессивных действий с использованием нейросетевых архитектур 3d-cnn // Известия ТулГУ. Технические науки. 2020. №2.

22. Development of a vision-based pose estimation system for robotic machining and improving its accuracy using LSTM neural networks and sparse regression. https://www.sciencedirect.com/science/article/abs/pii/S0736584521001423

23. Advancing human action recognition: A hybrid approach using attention-based LSTM and 3D CNN. https://www.sciencedirect.com/science/article/pii/S2468227623002521

24. A new hybrid deep learning model for human action recognition. https://www.sciencedirect.com/science/article/pii/S1319157819300412

25. Циликов Н.С., Федосин С.А. Графовые нейронные сети // Вестник МГУ. 2012. №2.

26. Трансформеры: новая эра в нейросетях https://sky.pro/wiki/python/transformery-novaya-era-v-nejrosetyah/

Using Video Data and Point Cloud to Prevent Unauthorized Access

Damdinov Z.[41], Damdinova T.[42]

In modern conditions, one of the key factors of ensuring information security is technical security measures. To prevent unauthorized access to data, one of the most important tools are video streams, which can serve as a reliable source for analysis. The topic of human behavior recognition using neural networks covers many tasks, including pose analysis, action recognition, intention prediction and emotion analysis. In recent years, the use of deep learning technologies, various types of neural networks, have shown significant success in solving these problems. The article presents the main sources of obtaining video data, considers the use of modern neural networks for recognizing human behavior.

Keywords: information security, video stream, point cloud, artificial neural networks, pattern recognition, human behavior recognition

[41]Zorigto Damdinov, undergraduate student, East-Siberia State University of Technology and Management, Ulan-Ude,

[42]Tatyana Damdinova, PhD., Associate Professor, East-Siberia State University of Technology and Management, Ulan-Ude, dtatyanac@mail.ru

УДК 004.056

Способы определения эффективности алгоритмов многоклассовой классификации компьютерных атак

Добкач Л.Я.[43(*)]

Аннотация. Задача распознавания компьютерных атак включает в себя не только необходимость обнаружения вторжения, но и решение многоклассовой задачи классификации, при которой множество компьютерных атак разбивается на несколько классов. Главная проблема заключается в том, что, в отличие от бинарной классификации, возникает неопределённость, как следует правильно обрабатывать ошибки распознавания, если алгоритм верно определил факт атаки, но неправильно её классифицировал. В настоящей статье рассматриваются три подхода к расчёту метрик эффективности, в соответствии с которыми определяется точность алгоритмов выявления атак.

Ключевые слова: системы обнаружения вторжений, бинарная задача, многоклассовая классификация, компьютерные атаки, метрики эффективности.

Введение

Первичная задача систем обнаружения вторжения (СОВ) — отличить попытку вторжения от нормального события [1]. Под идентификацией попытки вторжений мы можем понимать выявление такой попытки.

Практические реализации систем обнаружения вторжений обеспечивают не только факт выявления компьютерной атаки, но также определяют её вид, способы пресечения, а в случае систем предотвращения вторжений — предпринимают меры по блокированию злонамеренных действий. Таким образом, задача обнаружения вторжений расширяется до задачи распознавания, что предполагает работу с несколькими классами.

Для эффективного распознавания атак необходимо не только собрать значимые данные, но и должным образом разбить их величины на классы. От того, насколько подробно СОВ настроена классифицировать атаки, зависит её производительность и эффективность [2-8]. Таким образом, следует определить способы расчёта эффективности алгоритмов распознавания атак при многоклассовой классификации.

Обнаружение как бинарная задача классификации

Поскольку обнаружение вторжений не предполагает глубокого анализа событий безопасности, соответствующую задачу можно отнести к бинарным задачам классификации. СОВ должна отличить нормальное событие от попытки вторжения. Соответственно, с точки зрения производительности такой классификатор будет наиболее выдающимся, однако не позволяет использовать специфические меры против атак различных видов.

Бинарная задача, как и следует из наименования, предполагает разбиение входных данных на два класса: нормальных событий и попыток вторжений (они же атаки или аномалии). Наиболее подходящими метриками эффективности можно назвать меру F1 и уровень обнаружения DR [4, 9]. Они основаны на долях верно и ошибочно распознанных событий, что наглядно видно в рамках бинарной задачи классификации:

TP (True positives) — число нормальных сессий, классифицированных как нормальные без ошибки;

FP (False positives) — число нормальных сессий, ошибочно классифицированных как атаки (ошибка второго рода);

[43] Добкач Леонид Яковлевич, акционерное общество «Аксофт», Москва, dobkachleo@mail.ru

FN (False negatives) — число аномальных сессий, классифицированных как нормальные (ошибка первого рода);

TN (True negatives) — число аномальных сессий, классифицированных как атаки без ошибки.

В зависимости от расстановки приоритетов, смысловые значения положительных и отрицательных показателей могут меняться местами [10], что лишь отчасти влияет на расчёт метрик эффективности.

От обнаружения к распознаванию: многоклассовая задача классификации

Бинарная задача классификации, как правило, решается не как самоцель, а как промежуточный этап в многоклассовой задаче классификации [8]. Под таковой понимается задача распознавания атак, когда, помимо отличия подозрительного события от нормального, СОВ должна отнести оное к одному из классов атак.

Составленный в 1999 году набор данных KDD Cup 1999 [11] фактически задал стандарт для классификации, хотя за минувшие десятилетия появились и другие наборы данных [12], в частности CICIDS 2017, отличающийся более актуальным перечнем видов атак и расширенным множеством признаков [13].

Набор KDD Cup 1999 содержит пять классов: нормальных событий и четыре класса атак. Набор CICIDS 2017 разбит на 15 классов: нормальные события по-прежнему собраны в одном классе, а остальные 14 представляют собой различные виды атак. Некоторые из них можно свести к более общим классам раннего набора, например, DOS [14, 15]. Очевидно, при определении конкретного класса атаки вероятность от неё защититься выше, а значит, многоклассовая классификация лучше отвечает требованиям безопасности.

Однако алгоритмы распознавания атак вынуждены анализировать события безопасности более глубоко, нежели чистые алгоритмы обнаружения вторжений. Снижается их производительность, возникают сомнения в их полезности. Чтобы адекватно применять метрики эффективности, следует верно переопределить или дополнить вышеприведённый список показателей. Отсюда вытекают три способа:

1) Строгий: TN включает в себя только те атаки, чей класс определён верно. FN включает в себя и пропущенные атаки, и неверно классифицированные. Имеет наибольшую производительность, обеспечивает предъявление высоких требований к классификатору, но пренебрегает атаками, отнесённых не к своим классам. Эффективность можно определить через меру F1 по формуле (1):

$$F_1 = 2\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2\text{TP}}{\text{TP} + \text{N} - \text{TN}} \quad (1)$$

2) Подробный: FN и TN относятся к каждому классу атак. В связи с увеличением числа показателей (так, для 4 видов атак показателей станет не 4, а 10), что наглядно отражает формула (2), производительность классификатора неизбежно снизится, зато повысится вычисленная точность.

$$F_1 = 2\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2\dfrac{\text{TP}}{\text{TP} + \text{FP}} \times \dfrac{TP}{TP + \sum_{i=1}^{n} FN_i}}{\dfrac{\text{TP}}{\text{TP} + \text{FP}} + \dfrac{TP}{TP + \sum_{i=1}^{n} FN_i}} \quad (2)$$

3) Гибкий: вводится вспомогательный показатель FNT, куда относятся верно выявленные, но неверно классифицированные атаки. По производительности лишь немного уступает строгому способу, но лучше устанавливает точность классификатора. Влияние оказывается на уровень обнаружения DR, в соответствии с формулой (3):

$$DR = \frac{\mathrm{TN} + \mathrm{FN}_\mathrm{T}}{\mathrm{FN} + \mathrm{FN}_\mathrm{T} + TN} \quad (3)$$

Таким образом, гибкий способ наиболее оптимален с точки зрения определения эффективности алгоритмов классификации компьютерных атак [16], но и другие способы имеют свои преимущества.

Заключение

Переход от бинарной задачи обнаружения вторжений к многоклассовой задаче распознавания компьютерных атак обуславливает пересмотр основных показателей, по которым можно определить эффективность алгоритмов классификации. Распознавание атак из нескольких классов находит применение, например, во фрактальном анализе [8] и актуальном в настоящее время машинном обучении [17].

Чтобы пресечь любые ошибки, подходит строгий способ. Тщательное определение точности в подробном способе приводит к снижению производительности алгоритма. Наиболее оптимален учёт неверно распознанных, но непропущенных атак, что позволяет после уведомления от СОВ своевременно отреагировать на попытку вторжения.

Список источников

1. Барабанов А., Марков А., Цирлов В. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.

2. Басараб М.А., Строганов И.С. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30-40.

3. Вишневский А.С., Ключарев П.Г. Обнаружение целенаправленных атак веб-ориентированной обманной системой, основанной на алгоритме антиклассификации // Нейрокомпьютеры: разработка, применение. 2020. Т. 22. № 3. С. 5-17.

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

5. Коноваленко С.А. Методика оценивания информационной устойчивости гетерогенной системы обнаружения компьютерных атак // Вопросы кибербезопасности. 2023. № 6 (58). С. 67-80.

6. Кузнецова Е.О., Петренко С.А. Подход к обнаружению кибератак на основе вычислительного когнитивизма // Известия СПбГЭТУ ЛЭТИ. 2021. № 6. С. 23-35.

7. Новикова Е.С., Котенко И.В., Мелешко А.В., Израилов К.Е. Обнаружение вторжений на основе федеративного обучения: архитектура системы и эксперименты // Вопросы кибербезопасности. 2023. № 6 (58). С. 50-66.

8. Шелухин О. И., Рыбаков С. Ю., Раковский Д. И. Классификация компьютерных атак с использованием мультифакторного спектра фрактальной размерности. // Вопросы кибербезопасности, 2024, № 2 (60), с. 107–119.

9. Krishnaveni S., Sivamohan S., Sridhar S. S., Prabakaran S. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. Cluster Computing, 2021, vol. 24, iss. 3, pp. 1761–1779.

10. Ieracitano C., Adeel A., Gogate M., et al. Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection. Proceedings of the 9th Intern. Conf. on Brain Inspired Cognitive Systems (BICS 2018), 2018, pp. 759–769.

11. Aggarwal P., Sharma S. K. Analysis of KDD Dataset Attributes — Class wise For Intrusion Detection. Procedia Computer Science. 3rd Intern. Conf. on Recent Trends in Computing 2015 (ICRTC-2015), 2015, № 57, pp. 842–851.

12. Alıguliyev R. M., Hajirahimova M. S. Classification Ensemble Based Anomaly Detection in Network Traffic. Review of Computer Engineering Research, 2019, т. 6, № 1, с. 12–23.

13. Sharafaldin I., Lashkari A. H., Ghorbani A. A. A Detailed Analysis of the CICIDS2017 Data Set. Intern. Conf. on Inf. Systems Security and Privacy: сборник трудов Межд. науч. конф., 2018, с. 172–188.

14. Abdulraheem M.H., Ibraheem N.B. A detailed analysis of new intrusion detection dataset. J. Theor. Appl. Inf. Technol., 2019, vol. 97, iss. 17, pp. 4519–4537.

15. Al-Harbi A., Jabeur R. An Efficient Method for Detection of DDoS Attacks on the Web Using Deep Learning Algorithms. Int. J. of Advanced Trends in Computer Sci. and Engineering, 2021, vol. 10, iss. 4, pp. 2821–2829. DOI: 0.30534/ijatcse/2021/271042021.

16. Елагин В. С. Модель классификации трафика в программно-конфигурируемых сетях с элементами искусственного интеллекта // Труды уч. заведений связи, 2023, т. 9, № 5, с. 66–78.

17. Sharif H. U., Ahmed S. U. Efficient cyber intrusion detection technique based on an ensemble classifier. J. Theor. Appl. Inf. Technol., 2022. Т. 100, № 16, с. 5265–5290.

Научный руководитель: Цирлов Валентин Леонидович, к.т.н., доцент кафедры ИУ8, v.tsirlov@npo-echelon.ru.

Modes of Determining the Algorithms Efficiency of Multi-Class Classification of Computer Attacks

Dobkacz L.Ya.[44(*)]

Abstract. The problem of recognizing computer attacks includes not only the need to detect an intrusion, but also solving a multi-class classification problem, when a set of computer attacks is divided into several classes. The main issue is that, unlike binary classification, there is uncertainty about how to correctly handle recognition errors if the algorithm correctly identified the fact of an attack, but incorrectly classified it. This article considers three approaches to estimating efficiency metrics, according to which the accuracy of attack detection algorithms is determined.

Keywords: intrusion detection systems, binary problem, multi-class classification, computer attacks, efficiency metrics.

[44] Leonid Dobkacz, Joint-Stock Company Axoft, Moscow, dobkachleo@mail.ru

УДК 004.056

Исследование возможностей реализации атаки прослушивания идентификаторов LF-диапазона

Дородняя А.А.[45]

В России в системах контроля и управления доступом широко используются низкочастотные карты формата EM-Marine. Это обусловлено низкой ценой идентификаторов и широкой совместимостью с оборудованием разных производителей. О теоретической возможности перехвата передаваемой информации между картой и считывателем высказывалось ранее, но не давалось практической оценки о достижимости этого на практике. В данной статье проводится исследование практической реализации данного рода атак. В ходе исследования проводится анализ возможности извлечения идентификатора LF-карт путём пассивного перехвата эфира. Также осуществляется выбор необходимых для реализации атаки аппаратных и программных компонентов.

Ключевые слова: СКУД, RFID, идентификатор, EM-Marine, SDR.

Введение. Радиочастотная идентификация (RFID) представляет собой технологию автоматической идентификации объектов с использованием RFID-меток, которые передают данные через радиосигналы [1]. RFID-метки делятся на два типа: низкочастотные (LF, 125 кГц) и высокочастотные (HF, 13,56 МГц). Низкочастотные метки просты и доступны и имеют единственный идентификатор (UID).

Дистанционные атаки на RFID-идентификаторы представляют собой серьезную угрозу безопасности [2]. Существуют два основных типа дистанционных атак:

- считывание — это попытка получить идентификационный номер или дополнительную информацию, хранящуюся на карте, путем имитации взаи ействия с картой от имени считывателя;
- прослушивание — это длительный перехват сигнала, передаваемого между считывателем и картой, без взаимодействия с атакуемым объектом.

В случае считывания злоумышленнику требуется большая мощность для осуществления атаки, а также необходимо учитывать множество переменных, таких как уровень сигнала, его местоположение и время перехвата сигнала [3]. В то же время, атаки с прослушиванием довольно просты в исполнении и требуют меньше ресурсов, что делает их более привлекательными для злоумышленников. Однако в этом случае возникает необходимость в сложной обработке сигнала из-за помех и более низкого уровня сигнала по сравнению с уровнем сигнала при считывании.

В данной статье будут рассмотрены методы атаки на низкочастотные карты, на примере протокола EM-Marine. В ходе исследования будет проведён анализ возможности извлечения идентификатора LF-карт из прослушиваемого эфира, а также выбор необходимых аппаратных и программных компонентов.

Стандарт Em-Marine. EM-Marine представляет собой микросхему для идентификации объекта по КМОП технологии, доступную только для чтения. Схема питается от внешней катушки, помещенной в электромагнитное поле, и получает свои основные тактовые импульсы от того же поля через один из выводов катушки. При включении и выключении модулирующего тока микросхема отправляет 64 бита информации, содержащейся в предварительно запрограммированном на заводе массиве памяти [4-6]. Программирование чипа осуществляется путем лазерного сплавления поликремниевых звеньев с целью сохранения уникального кода на каждом чипе [7].

[45] Дородняя Алёна Александровна, МГТУ им. Н.Э. Баумана, Москва, Dorodnyaya.alena@yandex.ru

Карты, работающие на частоте 125 кГц, в силу отсутствия достаточной мощности, не защищены от копирования, поэтому при общении с считывателем в эфире RFID-метка непрерывно передаёт свой 64-битный UID. Благодаря этому существует возможность получить полезную информацию из пассивного прослушивания эфира.

Системы класса SDR. В последние годы всю большую популярность приобретают системы класса Software Defined Radio (SDR), благодаря своей простоте и возможности программно определять свою конфигурацию [8]. SDR позволяет устанавливать и изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность. Значительные объемы обработки сигналов передаются процессору общего назначения, а не выполняются в аппаратных средствах специального назначения (электронных схемах) [9]. Такая конструкция позволяет создавать радиоприемник, который может принимать и передавать самые разные радиопротоколы (иногда называемые формами сигналов) исключительно на основе используемого программного обеспечения [10].

К основным компонентам SDR относят следующие элементы: антенна, аналого-цифровой преобразователь (АЦП), цифровой сигнальный процессор (DSP), программируемая пользователем вентильная матрица (FPGA), программные компоненты, пользовательский интерфейс (UI), программный анализ [11].

Чтобы зафиксировать сигналы, передаваемые LF-картами считывателю, необходимы SDR-приёмники, позволяющие принимать сигнал с несущей частотой 125 кГц и дивиацией порядка 10 кГц. Исходя из цены и доступности на территории Российской Федерации для проведения дальнейших экспериментов был выбран SDR-приёмник RSP1 от компании SDRPlay.

Атака дистанционного прослушивания. Чтобы изучить возможность осуществления атаки на прослушивание карты формата EM-Marine, была проведена серия экспериментов. Цель экспериментов — из принятого SDR-play RSP1 взаимодействия карты EM4100 со считывателем, в качестве которого был использован proxmark3 Easy, получить идентификатор карты.

В ходе эксперимента применяются следующие аппаратные компоненты: ноутбук с операционной системой Ubuntu (версия 22.04 или позднее), программно- определяемое радио SDR-play RSP1, proxmark3 и LF-карта формата EM-Marine. В качестве инструмента обработки сигнала приёмника был выбран инструмент с открытым исходным кодом «GNU Radio», с установленным дополнительно модулем для работы с SDR-play RSP1 «gr-sdrplay3». Экспериментальная установка представлена на рисунке 1.

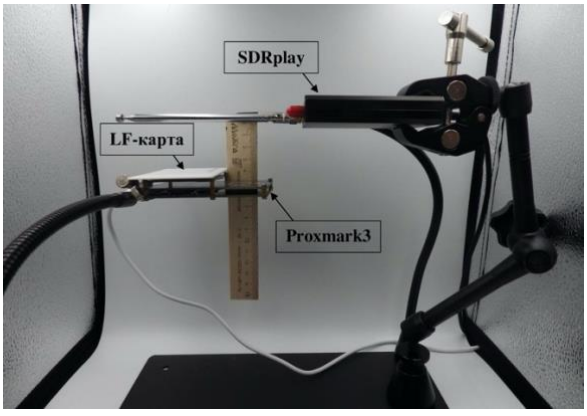


Рис. 1 – Экспериментальная установка

Процесс приёма и обработки был разбит на три этапа. На первом этапе SDR принимает аналоговый сигнал и сохраняет его в бинарный файл. На втором этапе эти данные подвергаются необходимой обработке и преобразовываются в промежуточное

представление сигнала. На третьем, заключительном этапе, из промежуточного представления сигнала выделяется максимально возможное количество корректных идентификаторов. В дальнейшем «посылкой» будут называться данные взаимодействия, полученные приёмником после одного прикладывания карточки (или после одной команды на чтение от proxmark3). При каждом прикладывании (то есть в каждой посылке) карта непрерывно отправляет одну и ту же последовательность длиной 64 бита.

На этапе формирования промежуточного представления сигнала необходимо установить значение амплитуды, которое будет использоваться для определения уровней единичного и нулевого значений, то есть порога. Если речь идёт об одной посылке, то это можно сделать вручную, вычислив средний уровень сигнала, однако такой способ не очень эффективен. Для нахождения уровня порога в общем случае специальный граф GNU Radio генерирует файл, который сохраняет среднее значение сигнала для некоторого постоянного числа выборки. Затем этот файл анализируется с помощью программы на языке Python. Результатом работы программы являются график и средние значения сигнала для каждой посылки. На рис. 2 продемонстрирован результат получения идентификаторов из прослушанного эфира при прикладывании двух различных карт.

Проведя эксперимент для различных дистанций между картой и считывателем, была доказана возможность дистанционного выделения идентификатора из прослушанного эфира. При этом для дистанции менее 10 см результативность атаки очень высокая — вероятность обнаружения корректного идентификатора более 60 %. Для дистанции до 14 см эта вероятность меньше, однако это не исключает возможность накопления и исправления ошибок приёма. На дистанции более 14 см в рамках созданного стенда и алгоритмов обработки сигналов перехват идентификатора был невозможен. На рисунке 3 представлен график зависимости вероятности успешного перехвата идентификаторов от дистанции проведения атаки.

```
3. FIND UID
File name: Signal_13-08-2024_16:35:01
Save binary files  Card_... generated by GNURadio? (y/N)

Automatic mode: start = 0, stop = 9500400,, threshold = -0.4432.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 3600CB501F |   15  |
| 2 | 350048B712 |   15  |
+---+------------+-------+

Run processing each Package? (Y/n)
  #    Index    Threshold
---  -------  -----------
  1    42845     -0.4444
  2    72658     -0.4445
  3   112116     -0.4446
  4   273622     -0.4432
  5   310258     -0.4433
  6   342477     -0.4433

Package (#1): start = 42845, stop = 72658, threshold = -0.4444.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 3600CB501F |   5   |
+---+------------+-------+

Package (#2): start = 72658, stop = 112116, threshold = -0.4445.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 3600CB501F |   5   |
+---+------------+-------+

Package (#3): start = 112116, stop = 273622, threshold = -0.4446.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 3600CB501F |   5   |
+---+------------+-------+

Package (#3): start = 112116, stop = 273622, threshold = -0.4446.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 3600CB501F |   5   |
+---+------------+-------+

Package (#4): start = 273622, stop = 310258, threshold = -0.4432.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 350048B712 |   5   |
+---+------------+-------+

Package (#5): start = 310258, stop = 342477, threshold = -0.4433.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 350048B712 |   5   |
+---+------------+-------+

Package (#6): start = 342477, stop = 9500400, threshold = -0.4433.
Wait...OK!
Find UID...OK!
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 350048B712 |   5   |
+---+------------+-------+

------------------------------------------------
Save to file UID_13-08-2024_16:35:01.txt
(in table only IDs with a count > 1)
+---+------------+-------+
| # |     ID     | Count |
+---+------------+-------+
| 1 | 3600CB501F |   15  |
| 2 | 350048B712 |   15  |
+---+------------+-------+
```

Рис. 2 – Нахождение идентификаторов для двух карт

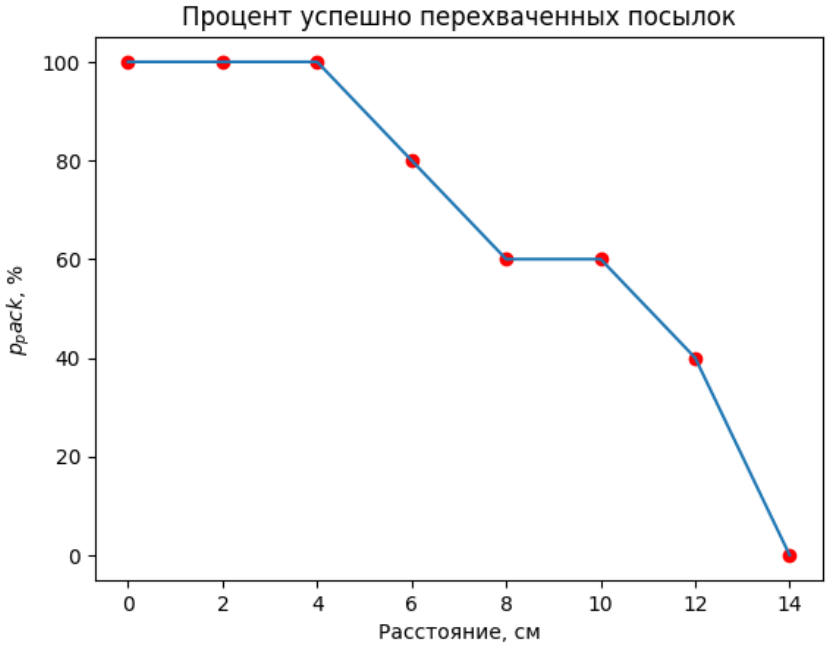


Рисунок 3 – Вероятность успешного перехвата идентификаторов

Выводы

Исследование показало, что с помощью SDR-play RSP1 и универсального считывателя proxmark3 можно прослушать низкочастотные карты EM-Marine. Для проведения разработанной атаки не требуется сложного оборудования, достаточно записать эфир во время идентификации карты. Это снижает затраты на оборудование, однако ограничивает цель — атаке подвергаются только те карты, информацию о которых можно извлечь из эфира.

Атака на карты EM4100 включает в себя этапы прослушивание эфира, анализ и обработку сигнала, а также выделение идентификаторов из обработанных данных. В рамках экспериментальной установки атака успешно проводится на расстоянии до 15 см, на больших расстояниях сигнал распознаётся с ошибками. Чтобы увеличить дистанцию, необходимо увеличить размер антенн, чувствительности приёмника и использовать другие алгоритмы обработки.

Экспериментально было показано, что использование доступных компонентов позволяет реализовать прослушивание идентификатора низкочастотной карты как минимум на расстоянии 15 см. Применение других антенн, приёмных усилителей и алгоритмов обработки позволит увеличить расстояние перехвата целевого идентификатора и использовать его для прохода в контролируемую зону.

Литература

1. Сагидова, М. Л. Современные системы контроля и управления доступом / М. Л. Сагидова // Международный журнал гуманитарных и естественных наук. – 2022. – № 9-1(72). – С. 64-68. – DOI 10.24412/2500-1000-2022-9-1-64-68.

2. Басараб М.А., Колесников А.В., Коннова Н.С. Моделирование компьютерных сетей Москва, Издательство МГТУ им. Н. Э. Бауман, 2021. – 86 с.

3. Петров, А. Н. Внедрение NFC технологии для системы контроля и управления доступа / А. Н. Петров, М. Р. Хамидуллин // Приоритетные направления инновационной деятельности в промышленности : Сборник научных статей по итогам пятой международной научной конференции, Казань, 30–31 мая 2020 года. Том Часть 2. – Казань: Общество с ограниченной ответственностью "КОНВЕРТ", 2020. – С. 78-79.

4. Неклюдов, Д. Н. Исследование атак на бесконтактные смарт-карты и RFID-метки / Д. Н. Неклюдов, А. С. Лебедь, У. В. Кузьмина // Вестник УрФО. Безопасность в информационной сфере. – 2023. – № 4(50). – С. 53-59. – DOI 10.14529/secur230405.

5. Цапов А.Е., Литвинова А.В., Лукьянов Г.И. Оценка безопасности СКУД на базе RFID-системы / Баранкова И.И., Михайлова У.В., Лукьянов Г.И. // Актуальные проблемы современной науки, техники и образования. 2021. Т.1. С. 404.

6. Белов А. Технологии SDR и перспективы её применения в ЗССС // Системы синхранизации, формирования и обработки сигналов. – 2021. – Т. 12, № 6. – С. 21-29.

7. Фокин Г. Технологии программно-конфигурируемого радио. Учебное пособие для вузов //. Т. 316. — Москва : Горячая линия - Телеком, 2019.

8. Горохов, А. В. Программно-определяемая радиосистема (SDR) / А. В. Горохов, М. С. Косьянова, А. К. Колесов // Инновационная деятельность в вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 13–14 октября 2022 года. – Санкт-Петербург. – С. 108-116.

9. Петров, С. Н. Физическая защита RFID-меток от клонирования / С. Н. Петров, К. С. Булавин, А. О. Ворожцов // Ломоносов : сборник статей IX Международного конкурса молодых учёных, Пенза, 05 июля 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 7-13.

10. Готовщиков, А. А. Совокупность параметров, определяющих размеры RFID антенны для считывания движущейся метки / А. А. Готовщиков // Научно-технический вестник: Технические системы в АПК. – 2021. – № 1(9). – С. 43-53.

11. Павлова, Т. А. Расчет дальности считывания RFID системы / Т. А. Павлова, Р. Т. Сафин, Ю. М. Гармашова // Энергетика, инфокоммуникационные технологии и высшее образование : Международная научно-техническая конференция. Электронный сборник научных статей по материалам конференции В 3-х томах, Алматы, Казань, 20–21 октября 2022 года. Том 1. – Казань: Казанский государственный энергетический университет, 2023. – С. 518-527. – EDN DFFJFF.

Научный руководитель: Колесников Александр Владимирович, к. т. н., доцент, МГТУ им. Н. Э. Баумана, Москва, avkolesnikov@bmstu.ru.

Exploration of the possibility of realising LF tags sniffing attacks

Dorodnyaya A. A.[46]

In Russia, low-frequency EM-Marine format cards are widely used in access control and management systems. The reason for this is the low price of identifiers and wide compatibility with equipment from different manufacturers. The theoretical possibility to intercept the transmitted information between the card and the reader has been expressed before, but no practical assessment has been made about the achievability of this in practice. In this paper, a study of the practical implementation of this kind of attacks is carried out. This paper analyzes the possibility of LF card identifier extraction by passive interception of the airwaves. It also specifies the hardware and software components required to implement the attack.

Keywords: ACS, RFID, identifier, EM-Marine, SDR.

[46] Alyona Dorodnyaya, Bauman Moscow State Technical University, Moscow, Dorodnyaya.alena@yandex.ru

УДК 004.75

Построение сценариев таргетированных атак на туманную инфраструктуру

Драмбян Д.Г.[47]**, Марков А.В.**[48]

В настоящей работе описана модель состояний информационной системы при применении в организации туманной инфраструктуры в соответствии с жизненным циклом атаки, построенная на основе сетей Петри. Данная модель описывает Марковские процессы, где используется конечное число состояний информационных систем, событие перехода из первого состояния в следующее зависит только от начального состояния, и не зависит от того, при каких условиях система попала в первое состояние. Даны рекомендации и сделаны выводы по использованию туманной инфраструктуры для обеспечения безопасности данных на предприятии.

Ключевые слова: информационная безопасность, облачные вычисления, туманные вычисления, защита инфраструктуры, цепь Маркова, сеть Петри

Введение

Одним из инновационных подходов к обеспечению безопасности информации является использование туманной инфраструктуры, которая позволяет улучшить защиту данных, обеспечивая доступ к информации только определенным пользователям в определенных сегментах сети [1-6]. Она представляет собой децентрализованную модель обработки, хранения и передачи данных, распределяющая вычислительные ресурсы между центральным облаком и локальными устройствами, находящимися ближе к источникам данных. Ввиду развития APT-группировок, необходимо выделить мероприятия по оценке уровня защищенности внешней инфраструктуры предприятия посредством моделирования различных векторов атак [7]. В данной работе на основе сетей Петри построена модель состояний информационной системы в соответствии с жизненным циклом атаки. В основу построения графа состояний информационной системы, подверженной вредоносному воздействию, ложатся состояния информационной системы в разные промежутки времени, которые являются вершинами графа скомпрометированных состояний информационной системы.

Построение сетей Петри

Последовательность вершин графа, обозначающих скомпрометированные состояния информационной системы, следует называть цепями Маркова, так как процессы описанные данной моделью напрямую соответствуют требованиям Марковских процессов: процесс состоит из конечного количества вершин, на переход из состояния S_1 в состояние S_2 не зависит от ранее происходящих событий, а зависит только от условий возникших в состоянии S_1, т.е. состояние S_1 с определённой долей вероятности способствует появлению события S_2 [8-11].

Для дальнейшего описания переходов в цепях Маркова, образующих сеть Петри, скомпрометированные состояния информационной системы описаны с помощью множества $S = \{S_j\}$, где $j \in N$.

Переходы между вершинами графа, характеризуются вероятностью наступления скомпрометированного состояния информационной системы P_{ij} (вероятностью перехода). При этом следует учитывать, что вероятность перехода из начального состояния в

[47] Драмбян Давид Грачьяевич, Финансовый университет при Правительстве РФ, Москва, daviddrambyan@mail.ru
[48] Марков Алексей Викторович, Финансовый университет при Правительстве РФ, Москва, MarkovAlexeyV@yandex.ru

следующие состояния должна равняться 1, т.е. сумма вероятностей возможных переходов из начального состояния в последующие возможные состояния должна давать единицу. Исходная вершина графа (состояние S_1) определяет состояние информационной системы, при котором все функции информационной системы выполняются в штатном режиме, негативное воздействие со стороны хакера не осуществляется. Переход в скомпрометированное состояние из состояния S_1 возможен только при осуществлении негативного воздействия со стороны специалистов.

Для построения модели таргетированной атаки была проанализирована матрица MITRE ATT&CK[49], что дало представление о том, каким актуальным техникам атак подвержена туманная инфраструктура на данный момент. В итоге было разработано множество скомпрометированных состояний туманной инфраструктуры $S = \{S_{1,}S_{2,\dots,}S_{10}\}$, которые возникают при реализации компьютерных атак (табл.1).

Таблица 1.

Множество скомпрометированных состояний туманной инфраструктуры

Название состояния инфраструктуры при компрометации злоумышленником, S	Описание состояния туманной инфраструктуры при воздействии на нее специалистов, имитирующих действия злоумышленника.
S_1	Состояние информационной системы в условиях отсутствия негативного воздействия на нее.
S_2	Инфраструктура во время пассивного этапа атаки, сканирование и сбор информации о внешнем периметре организации.
S_3	Преодоление периметровых средств защиты: обход правил доступа МЭ, получение доступа к информационным ресурсам в обход правил разграничения доступа, присутствие к корпоративной сети от имени легитимного пользователя, внедрение вредоносного ПО.
S_4	Заражение информационной системы через каналы электронной почты, веб-портал.
S_5	Реализация утечки информации и заражение информационной сети.
S_6	Активность специалистов внутри периметра: внедрение эксплойтов в программное обеспечение и сетевые компоненты, модификация таблиц маршрутизации, сканирование сетевого трафика.
S_7	Закрепление злоумышленника во внутреннем периметре организации: получение доступа к конечным точкам сети и критически значимым компонентам инфраструктуры.
S_8	Состояние ИС, когда сервисы на периметре локальной сети не доступны (DDoS)
S_9	Закрепление программ-rootkit внутри контура локальной сети
S_{10}	Информационная система некорректно выполняет возложенные на ней бизнес-функции, вследствие ошибок и сбоев компонентов ИС.

Чтобы определить вектор атаки на инфраструктуру, построим сеть Петри, которая будет включать в себя весь путь атакующего. На рисунке 1 изображены сети Петри, показывающие переходы между скомпрометированными состояниями информационных систем без учета противодействия активности злоумышленника со стороны системы защиты информации [12].

[49] https://attack.mitre.org/

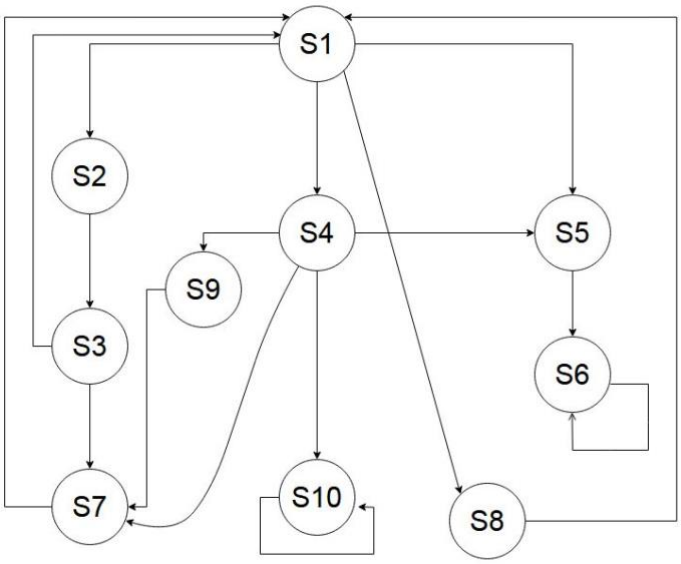


Рис.1. Граф скомпрометированных состояний туманной инфраструктуры при тестировании на проникновение

В графе существуют переходы из некоторых состояний в начальное, что свидетельствует о том, что даже без учета возможных используемых средств защиты информации данный тип инфраструктуры на стадии внедрения может противостоять некоторым векторам атак злоумышленников.

Граф состояний был дополнен обратными переходами (рис.2), реализованными благодаря наличию в системе безопасности соответствующих механизмов защиты информации. Множество механизмов защиты информации $Pr = \{Pr_{1,}Pr_{2,\ldots,}Pr_5\}$ представлено в таблице 2 [13].

Таблица 2.

Множество механизмов защиты информации для туманной инфраструктуры

Название механизма ЗИ, Pr	Описание
Pr1	Шлюз прикладного уровня для фильтрации входящего трафика
Pr2	Централизованная система антивирусной защиты (Anti-malware)
Pr3	Система контроля утечки данных (DLP)
Pr4	Система резервирования данных (Backup)
Pr5	Контроль целостности файлов операционной системы (Модуль доверенной загрузки)

На основе матрицы качественной оценки вероятности реализации угрозы на графах скомпрометированных состояний информационной системы была определена вероятность реализации угроз кибербезопасности (рис.2) [14].

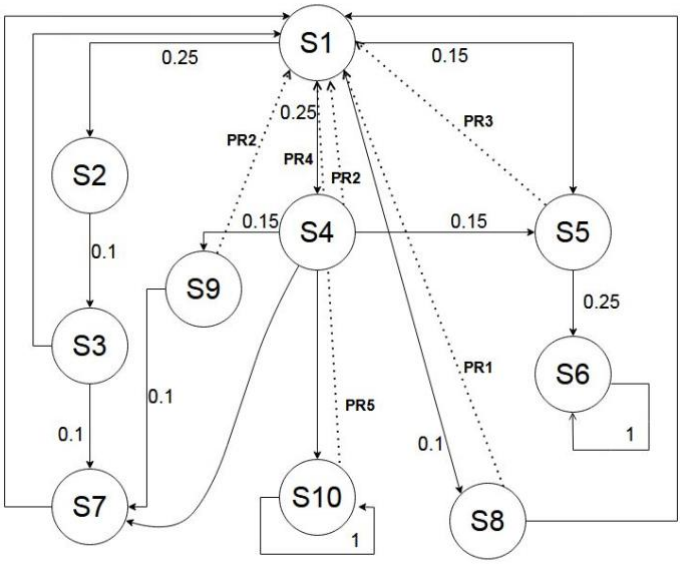


Рис.2. Вероятности реализации угрозы на графе скомпрометированных состояний туманной инфраструктуры

Как можно увидеть, используемые механизмы не могут защитить от всех векторов компрометации, однако в силу архитектурных особенностей туманной инфраструктуры некоторые вектора атак невозможны.

Построение Марковских цепей

Для более детального анализа построены Марковские цепи, показывающие последовательность этапов компрометации информационной системы, где вероятность наступления события (S_n) зависит от состояния, полученного на предыдущем этапе (S_{n-1}) (рис.3).

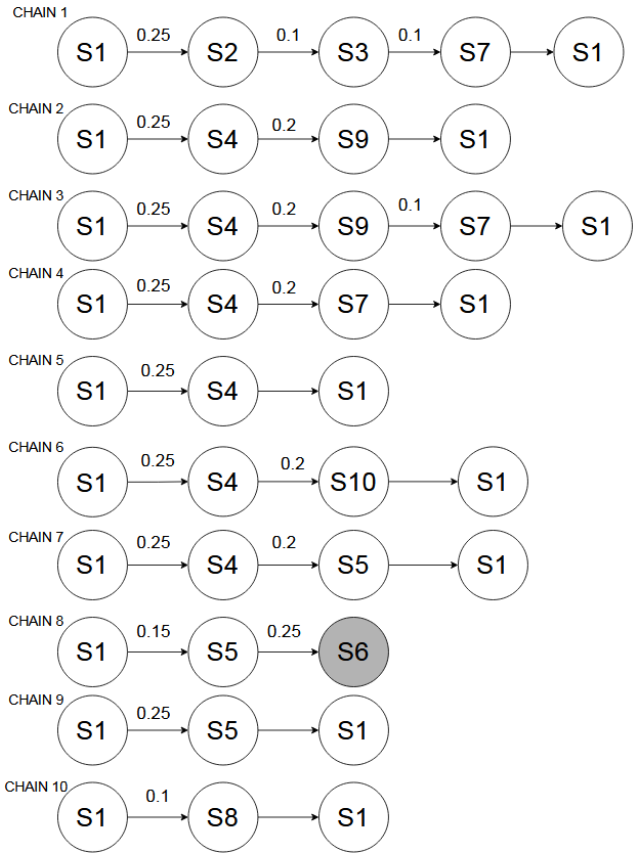


Рис.3. Марковские цепи скомпрометированных состояний туманной инфраструктуры

После построения Марковских цепей необходимо провести их ранжирование по качественной шкале оценки, где цепи делятся на три категории: «критично-опасные», «опасные», «незначимые». К опасным цепям отнесем следующую последовательность скомпрометированных состояний:

$$\text{Chain } 8 = \{S1 - S5 - S6\} \quad (1)$$

Проведя анализ опасных Марковский цепей, можно прийти к выводу, что система защиты информации за счет использования туманный инфраструктуры обеспечивает защиту от большинства рассмотренных угроз.

Опираясь на Марковские цепи, сделан вывод о том, что туманная инфраструктура, за счет своей архитектуры и встроенных механизмов позволяет защититься от ряда атак, которые могли бы привести к компрометации всей инфраструктуры.

Выводы

В ходе исследования было выявлено, что обеспечение безопасности данных предприятия при организации туманной инфраструктуры представляет собой сложную задачу, требующую комплексного подхода и использования современных технологий защиты информации. Были построены модели состояний инфраструктуры на основе Сетей Петри с использованием Марковских цепей. На основе используемых злоумышленниками векторов атак, были построены возможные конечные состояния инфраструктуры. Анализ графов и цепей Маркова, показал эффективность туманной инфраструктуры вместе с использованием предложенных механизмов защиты. На основе проведенной работы можно сделать вывод о допустимости использования туманной инфраструктуры, в качестве решения по повышению уровня безопасности в организации.

Литература

1. Довгаль В. А. Методы повышения безопасности в сфере «Облачных» технологий // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2014. №4 (147). С. 170-174.

2. Stojmenovic, I.; Wen, S.; Huang, X.; Luan, H. An overview of Fog computing and its security issues. Concurr. Comput. Pr. Exp. 2015, 28, 2991–3005,

3. Ахметов, У. Р. Обзор моделей построения туманных вычислений / У. Р. Ахметов, А. А. Корнилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 года. – Уфа: Башкирский государственный университет, 2022. – С. 120-122.

4. Востроилова, П. О. О проблемах применения технологий туманных вычислений / П. О. Востроилова // Проблемы развития современного общества: Сборник научных статей 8-й Всероссийской национальной научно-практической конференции. В 4-х томах, Курск, 19–20 января 2023 года / Под редакцией В.М. Кузьминой. Том 3. – Курск: Юго-Западный государственный университет, 2023. – С. 221-223.

5. Десницкий, В. А. подход к построению компонентов защиты систем Интернета вещей на основе концепции туманных вычислений / В. А. Десницкий // Перспективные направления развития отечественных информационных технологий : Материалы VI межрегиональной научно-практической конференции, Севастополь, 22–26 сентября 2020 года / Науч. ред. Б.В. Соколов. – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2020. – С. 249-250.

6. Черепенин, В. А. Отличия и перспективы развития технологий облачных, туманных и граничных вычислений / В. А. Черепенин, С. П. Воробьев, В. В. Синявцев // Инженерный вестник Дона. – 2023. – № 11(107). – С. 47-56.

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

8. Щеглов К. А., Щеглов А. Ю. Марковские модели угрозы безопасности информационной системы // Приборостроение. 2015. №12. С. 957-965.

9. Бочков М.В., Васинев Д.А. Моделирование устойчивости критической информационной инфраструктуры на основе иерархических гиперсетей и сетей Петри // Вопросы кибербезопасности. 2024. № 1 (59). С. 108-115.

10. Шрейдер М.Ю., Боровский А.С. Разработка моделей описания обработки информации в задачах управления системой защиты объекта на основе сетей петри // Вопросы кибербезопасности. 2018. № 1 (25). С. 46-53.

11. Язов Ю.К., Панфилов А.П. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз безопасности информации // Вопросы кибербезопасности. 2024. № 2 (60). С. 53-65.

12. Котов, В. Е. Сети Петри / В. Е. Котов. – Москва: Федеральное государственное унитарное предприятие "Академический научно-издательский, производственно-полиграфический и книгораспространительский центр "Наука", 1984. – 160 с.

13. Трапезников, Е. В. Выбор средств защиты информации в автоматизированных системах на основе марковских моделей кибератак / Е. В. Трапезников // Безопасность информационных технологий. – 2023. – Т. 30, № 4. – С. 102-113. – DOI 10.26583/bit.2023.4.06.

14. Анализ информационных рисков в системах обработки данных на основе "туманных" вычислений / А. А. Финогеев, А. Г. Финогеев, И. С. Нефедова [и др.] // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 4. – С. 38-46.

Научный руководитель: Марков Алексей Сергеевич, д.т.н., профессор МГТУ им. Н.Э.Баумана, Москва, a.markov@bmstu.ru

Building scenarios for targeted attacks on fog infrastructure

Drambyan D.H.[50]**, Markov A.V.**[51]

This paper describes a model of information system states when using a fog infrastructure in an organization in accordance with the attack life cycle, built based on Petri nets. The model describes Markov processes, where a finite number of information system states are used, the event of transition from the first state to the next depends only on the initial state and does not depend on the conditions under which the system got to the first state. Recommendations are given and conclusions are made on the use of fog infrastructure to ensure data security at the enterprise.

Keywords: information security, cloud computing, fog computing, infrastructure protection, Markov chain, Petri net

[50] David Hrachyaevich Drambyan, Financial University under the Government of the Russian Federation, Moscow, daviddrambyan@mail.ru

[51] Alexey Viktorovich Markov, Financial University under the Government of the Russian Federation, Moscow, MarkovAlexeyV@yandex.ru

УДК 004.056

Актуальные вопросы кибербезопасности в энергетике

Дураковский А.П.[52] **, Марков А.С.**[53]

Доклад посвящен обзору актуальных угроз кибербезопасности в сфере энергетикb. Приведены примеры инцидентов и атак на объекты энергетики. Отмечены особенности защиты информации на объектах энергетики.

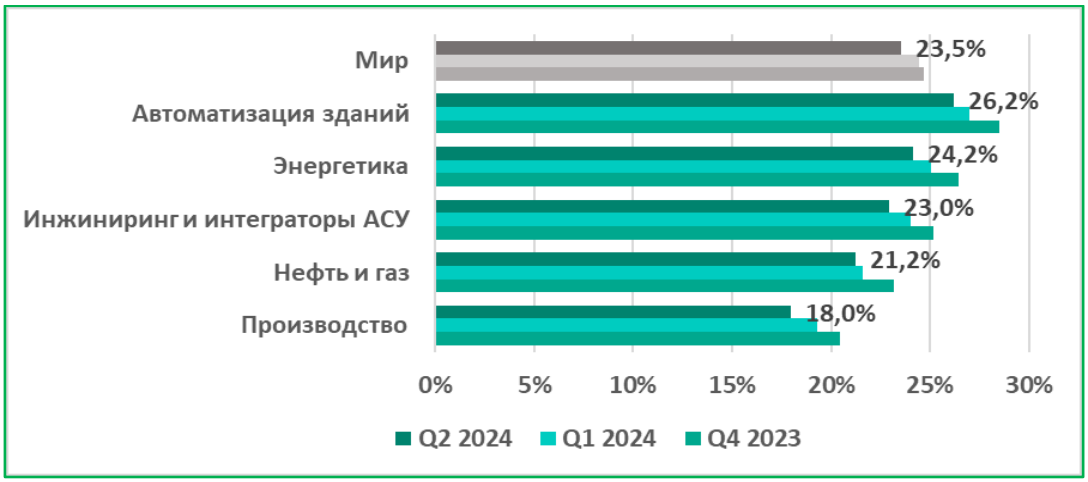
Ключевые слова: информационная безопасность, ТЭК, электроэнергетика, безопасность информации, АСУ ТП,

Введение

Вопросам комплексной безопасности в энергетике всегда уделяют самое пристальное внимание, максимально регламентируя безопасность, надежность и устойчивость функционирования процессов жизненного цикла подсистем. При этом последние тенденции в области безопасности объектов энергетики свидетельствуют о росте значимости киберугроз [1-16]. В подтверждение указанному ниже приведен краткий анализ востребованности тематики.

События и внимание мирового сообщества

Примечательно, но исторически популярность термина «*кибербезопасность»* вообще связывают как раз с атакой на объекты атомной энергетики (так называемая операция США-Израиля «Олимпийские игры», где использовалось кибероружие Stuxnet [17]). В последнее годы опубликован ряд аналитических отчетов, посвященных исследованию проблем кибербезопасности в сфере энергетики, например, отчеты Лаборатории Касперского, Ernst & Young, Ростелекома, ESC, ENISA, KonBriefing и др. Согласно названным отчетам, отмечается устойчивый рост компьютерных атак на объекты энергетики, причем рост выше, чем в среднем по объектам критической инфраструктуры в целом (рис. 1).



Источник: ics-cert.kaspersky.ru

Рис. 1. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

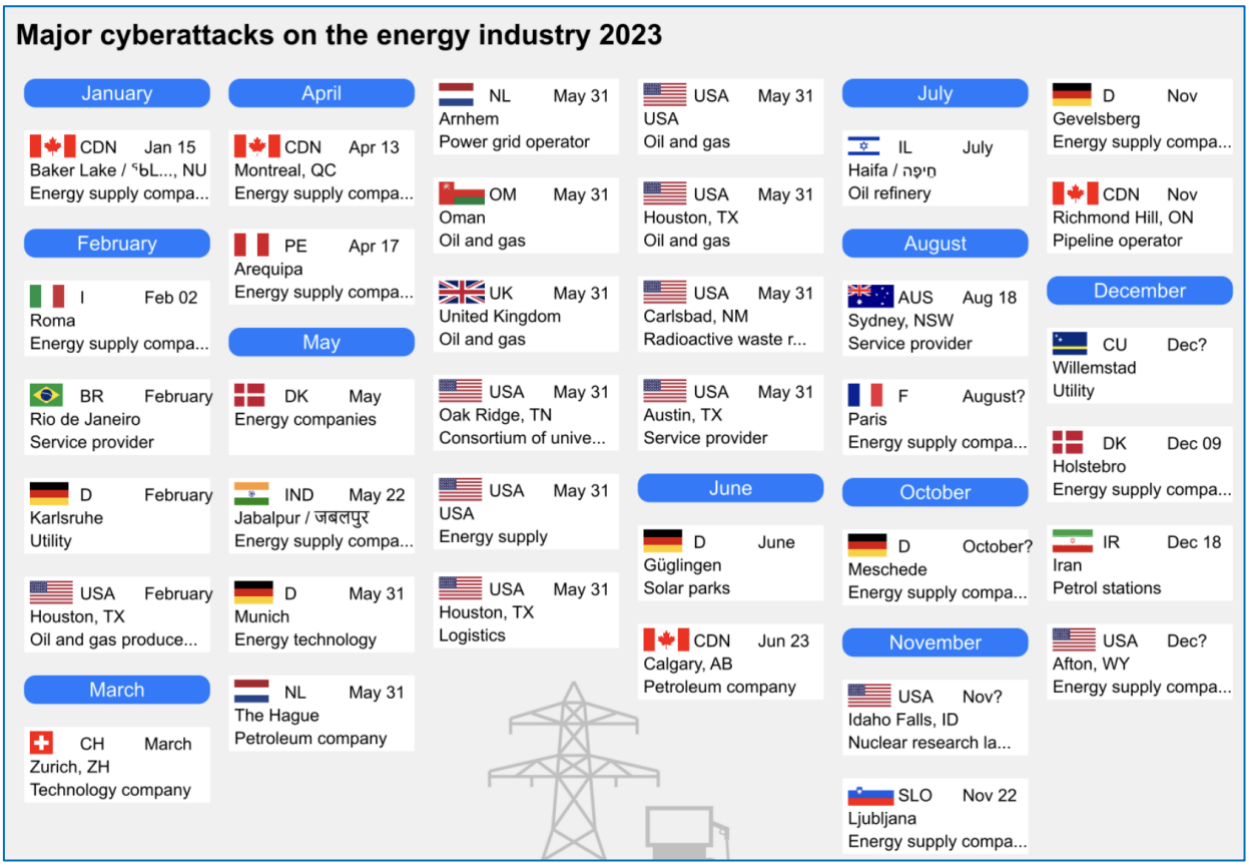
Ниже приведены наиболее нашумевшие в прессе инциденты в сфере энергетики за прошедший год:

[52] Дураковский Анатолий Петрович, к.т.н., доцент, НИЯУ МИФИ, APDurakovskiy@mephi.ru
[53] Марков Алексей Сергеевич, д.т.н., с.н.с., МГТУ им. Н.Э.Баумана, a.markov@bmstu.ru

- атака на Schneider Electric (время простоя подразделения два дня);
- атака с использованием программы-вымогателя на BHI Energy (похищены 767 файлов и ключевые данные);
- атака на Национальную ядерную лабораторию Айдахо (массовая утечка ПДн о 45 тысячах сотрудниках);
- атака шифровальщика на словенскую энергетическую компанию Holding Slovenske Elektrarne (поражены корпоративные сети);
- атаки на заправочные станции в Иране (около 70% заправочных станций страны перестали работать в результате кибератаки);
- атака на немецкий производитель ветровых турбин Nordex SE (более 2000 турбин оказались без мониторинга со стороны производителя).

В качестве иллюстрации масштабности атак можно привести пример 12-часовой атаки на поставщиков электроэнергии (City Power) в Йоханнесбурге, в результате чего пострадало 250 000 жителей.

Согласно отчету ENISA, только в 2023 г. зарегистрировано более 200 киберинцидентов, направленных на энергетический сектор, которые разбирались на национальных уровнях. На рис. 2 приведены наиболее значимые атаки на объекты энергетики за прошлый год согласно отчету KonBriefing Research.



Источник: konbriefing.com

Рис. 2. Наиболее известные APT-атаки на объекты энергетики

Можно добавить, что ряд вредоносных программ ориентированы именно на объекты энергетики, например: Shamoon, PIPEDREAM, Industroyer I/II и др.

Зачастую, за кибероперациями на энергетические объекты прямо или косвенно стоят прогосударственные кибергруппировки. В этом плане показательна концепция министерства обороны США «Операции, основанные на воздействии» (Effects-based

Operations). Согласно указанной концепции, энергетика является одной из ключевых целей военных.

Следует указать, что понятийный аппарат кибербезопасности объектов энергетики в мире уже сложился. Наглядным примером являются систематики, таксономии (например, ATT@CK for ICS) и каталоги угроз (например, Каталог угроз и ущербов КИИ ЕС).

Что касается стандартов ISO/IEC и NIST, то вопросы безопасности ИТ/ОТ или АСУ ТП затронуты более, чем в десяти стандартах (NIST SP 800-82r3, линейка ANSI/ISA-62443 и др.). Можно добавить государственные инициативы по повышению уровня кибербезопасности объектов энергетики, например: AESCSF, FERC Order No. 893 и др. В рамках ряда международных инициатив сформированы центры коллаборации по кибербезопасности объектов энергетики, как-то: Joint Cyber Defense Collaborative, U.S. Department of Energy (DOE) Energy Threat Analysis Center, Defense Industrial Base Collaborative Information Sharing Environment (DCISE) и др. В мире постоянно проводятся международные киберучения на защите объектов энергетики.

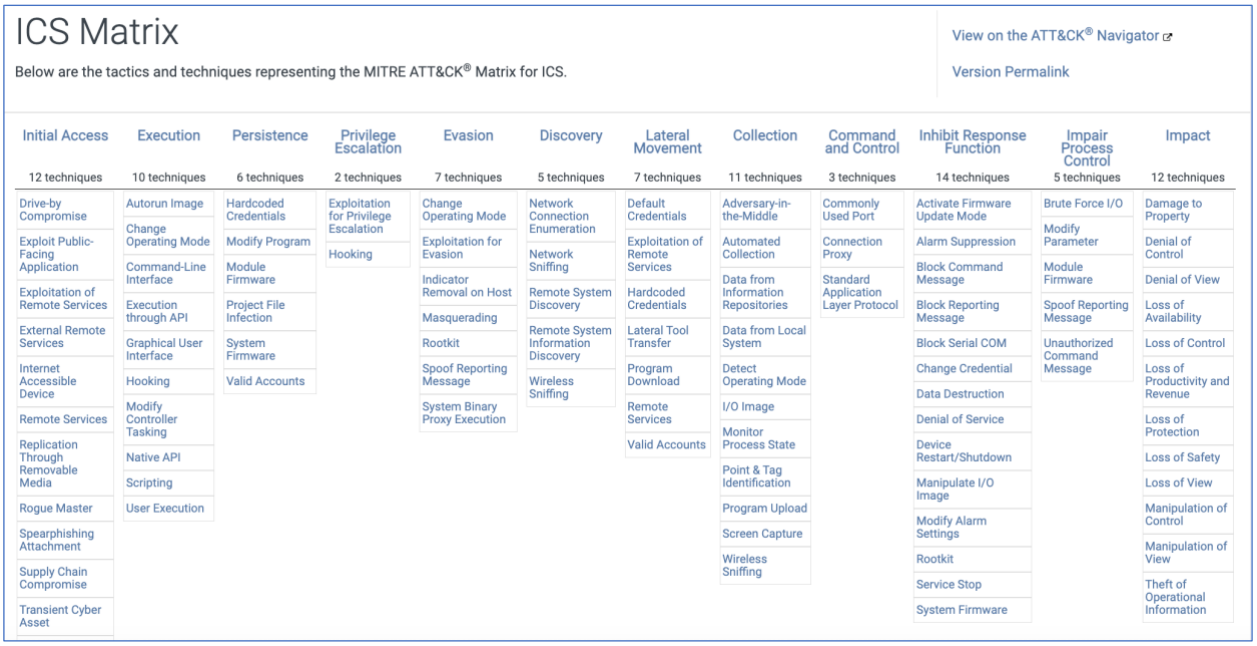


Рис. 3. Матрица целей и методов кибератак на АСУ ТП

Организация защиты информации на объектах энергетики в РФ

Можно констатировать, что в Российской Федерации и нормативная, и техническая базы информационной безопасности объектов энергетики сложились и находятся в постоянном развитии.

Собственно информационная безопасность (ИБ) объекта энергетики как значимого объекта КИИ РФ находится в сфере компетенции ФСТЭК России (и ФСБ России), а безопасность объекта энергетики как объекта топливно-энергетического комплекса, электроэнергетики или энергопринимающих установок находится еще и в сфере компетенции Минэнерго России.

Как известно, ФСТЭК России регулирует информационную безопасность объектов КИИ РФ, руководствуясь приказами 31, 235 и 239, а также 77 (аттестация) и др. При этом приказами Минэнерго России утверждены Перечень типовых отраслевых объектов КИИ РФ, функционирующих в сфере энергетики[54], и Перечень типовых отраслевых объектов

[54] https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-2023

КИИ РФ, функционирующих в сфере ТЭК[55]. Как правило, в них речь идет о разного рода АСУ ТП и пр.

Постановление Правительства РФ № 244 от 2017 г. «О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики ...» возложило обязанности на Минэнерго России по обеспечению ИБ в сфере электроэнергетики РФ, в том числе по:

- требованиям в отношении базовых (обязательных) функций и ИБ объектов электроэнергетики при создании и последующей эксплуатации на территории РФ систем удаленного мониторинга и диагностики энергетического оборудования;
- требованиям к безопасности объектов электроэнергетики и энергопринимающих установок.

Указанные требования уточнены в двух приказах Минэнерго России:

- приказ Минэнерго России 2018 г. № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и ИБ объектов электроэнергетики при создании и последующей эксплуатации на территории РФ систем удаленного мониторинга и диагностики энергетического оборудования»;
- приказ Минэнерго России 2023 г. № 1215 «Об утверждении дополнительных требований по обеспечению безопасности значимых объектов КИИ, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатации состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике».

Особо следует отметить «Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса», согласованные совместно Минэнерго России от 31.07.2019 № ЧА-8630/15 и ФСТЭК России от 26.08.2019 № 240/25/4048.

Указанное говорит о пристальном внимании государственных и отраслевых регуляторов к тематике. Кстати, в 2022 г. было сообщение Минэнерго России о запуске пилотного проекта Единого отраслевого центра координации и противодействия кибератакам (Energy CERT).

Заключение

Отмеченные тенденции позволяют сделать следующие выводы:

1. Наблюдается рост значимости объектов энергетики в области информационной и кибербезопасности;
2. Требования сформированы и развиваются, можно сказать, ужесточаются.

По мнению экспертов, наиболее проблемные моменты следующего года следующие:

1. Переход на доверенные программно-аппаратные комплексы (отечественные) с вытекающими проверками со стороны регуляторов в перспективе;
2. Подготовка кадров, востребованность в высокопрофессиональных специалистах по защите информации со знанием специфики.

Литература

1. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42-49.

2. Гурина Л.А., Зорина Т.Г., Томин Н.В., Прусов С.Г. Угрозы и уязвимости объектов киберфизической энергетической системы при цифровой трасформации ее свойств // Вестник Казанского государственного энергетического университета. 2022. Т. 14. № 3 (55). С. 89-98.

[55] https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-tek-2023

3. 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.

4. Зорина Т.Г., Панасюк В.В. Анализ энергетической безопасности регионов Республики Беларусь в условиях устойчивого развития и цифровой трансформации // Вестник Казанского государственного энергетического университета. 2023. Т. 15. № 3 (59). С. 118-129.

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

6. Куликов, А.Л., Зинин В.М. Требования к информационной безопасности в электроэнергетике и их реализация в интеллектуальных устройствах цифровых подстанций // Интеллектуальная электротехника. - 2022. - № 3 (19). - С. 49 - 78.

7. Лившиц И.И. Оценка методических подходов для формирования систем безопасности сложных промышленных объектов топливно-энергетического комплекса // Вопросы защиты информации. 2016. № 1 (112). С. 56-61.

8. Массель А.Г., Массель Л.В., Гаськова Д.А. Кибербезопасность в критических инфраструктурах (на примере энергетики) // Сб. трудов Седьмой Всероссийской научно-технической конференции "Безопасные информационные технологии" (БИТ-2016) / Под ред. В.А. Матвеева. - М.: МГТУ им. Н.Э.Бауман, 2016. С. 197-199.

9. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17). С. 2-10.

10. Минзов А.С. Современные угрозы топливно-энергетическому комплексу России // Инновационные, информационные и коммуникационные технологии. 2016. № 1. С. 482-485.

11. Минзов А.С., Невский А.Ю., Пасова М.А. Управление непрерывностью процессов на объектах критической информационной инфраструктуры в энергетике с позиций информационной безопасности // Вестник Московского энергетического института. 2023. № 5. С. 182-189.

12. Натальсон А.В. Формирование цифровых компетенций в области кибербезопасности объектов цифровой энергетики // Вестник НЦБЖД. 2023. № 3 (57). С. 54-60.

13. Пилюгин С.М., Мардамшина А.Р., Каменева Е.В., Мошуров Н.П. Кибербезопасность энергетического сектора России // Наукосфера. 2024. № 3-2. С. 250-256.

14. Borisyuk N.K., Kutsenko E.I., Kirkhmeer L.V., Berezhnaya L.Y. Economics Restructuring Model on the Base of Fuel and Energy Complex Clustering Quality // Access to Success. 2020. T. 21. № 176. C. 130-135.

15. Petrenko S.A., Makoveichuk K.A. Ontology of Cyber Security of Self-Recovering Smart GRID // CEUR Workshop Proceedings. 2017. V. 2081. P. 98-106.

16. Voropai N.I., Kolosok I.N., Korkina E.S., Osak A.B. Issues of Cybersecurity in Electric Power Systems // Energy Systems Research. 2020. V. 3. No 2 (10). P. 19-28.

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

Current issues of cyber security in the energy sector

Durakovsky A.P.[56], Markov A.S.[57]

The report is devoted to the review of current cybersecurity threats in the energy sector. Examples of incidents and attacks on energy facilities are given. The specifics of information protection at energy facilities are noted.

Keywords: information security, fuel and energy complex, electric power industry, information security, automated process control systems

[56] Anatoly P. Durakovsky, Ph.D., National Research Nuclear University MEPhI, apdurakovskiy@mephi.ru.
[57] Aleksey S. Markov, Dr.Sc., Bauman Moscow State Technical University, a.markov@bmstu.ru

УДК 004.056

Аудит безопасности разрабатываемых и развёрнутых API

Евсеев В.Л.[58], Линев Н.В.[59], Мамонтов А.С.[60], Печерский В.А.[61], Мамонтов В.С.[62], Апарина А.А.[63]

Аннотация: целью работы является исследование методов и инструментов аудита безопасности API. Проанализированы тенденции в атаках на API. Рассмотрены ключевые уязвимости и угрозы, характерные для API. Проведён анализ современных подходов к выявлению уязвимостей и обеспечению безопасности API на этапе разработки и развёртывания, с акцентом на автоматизацию процессов тестирования и мониторинга безопасности. Особое внимание уделено интеграции механизмов защиты API в цикл разработки программного обеспечения (SDLC) для минимизации рисков и предотвращения угроз.

Ключевые слова: SDLC, OpenAPI, безопасность интерфейсов, автоматизация тестирования, Swagger.

Введение

В последние годы API играют все более важную роль, так как современные приложения строятся на взаимодействии разных сервисов и систем. В связи с этим, в данной статье рассмотрены ключевые аспекты тестирования API на предмет безопасности.

API — это набор правил и протоколов, позволяющий различным компонентам информационной системы взаимодействовать друг с другом. В условиях стремительно растущей цифровизации API стал важной частью архитектуры приложений, обеспечивая интеграцию и взаимодействие между различными сервисами и платформами.

Тенденция уязвимостей API

На сегодняшний день количество API-интерфейсов в инфраструктуре организаций увеличивается каждый год примерно на 50%, а количество атак с каждым годом растет почти в 2 раза. Отмеченная тенденция наблюдается вследствие основного источник угроз – доступности данных [1]. Следует указать, что основная угроза связана с доступностью таких данных, как персональные и финансовые данные.

Методы автоматизированного выявления уязвимостей API

Для исследования использовались виртуальные машины с ОС Kali Linux и Ubuntu, а также тестовое приложение VAmPI с уязвимым API [2, 3]. Для анализа поведения системы выявлена необходимость подробного изучения контента, отдаваемого веб-сервером. К примеру, при анализе HTTP-запросов с помощью BurpSuite при использовании скрипта Bambda удается выявить нестандартные заголовки, характерные для API: x-rphost, x-api-key, x-user-actions.

На следующем шаге поиска уязвимостей представлен фаззинг [4-6]. При анализе данной технологии удалось доказать ее практическую эффективность в тестировании безопасности API. Для изучения возможности доступа к информации без авторизации выполнялись ручные запросы с различными вариациями путей. В связи со значительными

[58] Евсеев Владимир Леонович, к.т.н., доцент, НИЯУ МИФИ, Москва, vlevseev@mephi.ru
[59] Линев Николай Владимирович, НИЯУ МИФИ, Москва, nikol.linev@gmail.com
[60] Мамонтов Александр Сергеевич, НИЯУ МИФИ, Москва, acmamontov@gmail.com
[61] Печерский Владислав Альбертович, НИЯУ МИФИ, Москва, pecherskiyvl@gmail.com
[62] Мамонтов Валентин Сергеевич, Swordfish security, Москва, vmamontov@swordfishsecurity.ru
[63] Апарина Алёна Артуровна, ФГБОУ ВО «Технологический университет», Королёв, yelenaaparina@yandex.ru

трудозатратами при ручном тестировании, было принято решение использовать специализированные сканеры по поиску API. В ходе исследования были рассмотрены такие общедоступные утилиты, как: Kiterunner, CATS, OFFensive Api Tester, RESTler, ffuzer, OWASP ZAP [7]. В ходе оценки функционала и актуальности словарей, было принято решение использовать OWASP ZAP.

Выявлена необходимость использование актуального и подходящего словаря для перебора. Решением данной задачи стал парсинг документации Swagger на существующих интернет-порталах, которые были обнаружена с использованием Google BigQuery [8]. На основе полученных данных удалось получить словарь из 36 677 значений.

В ходе экспериментов удалось выявить способ уменьшения времени подбора методов путем использования метод OPTIONS, поскольку при его корректной работе он смог вернуть все используемые HTTP-методы API.

Также были осуществлены атаки, нацеленных на конкретный тип API: на примере JWT-токенов [9], эффективными атаками определены: подмена ключа, подмена подписи токена и эксплуатация уязвимостей шифров. По итогу атак выявлены и устранены недостатки исходного кода, составлены рекомендации по безопасной разработке.

На основании результатов исследования предложен следующий алгоритм аудита безопасности API:

— Обнаружение конечных точек API
— Фаззинг HTTP-параметров конечных точек API
— Поиск ключей или токенов API
— Атаки на HTTP-параметры API
— Атаки, направленные на используемый тип API

Рекомендации по безопасности API

Для обеспечения безопасности API выявлена необходимость проведения инвентаризации API-интерфейсов. Отдельно отмечено требование создание политики аутентификации и авторизации. Эффективным методом тестирования на уязвимости на разных этапах разработки предложен фаззинг. Рассмотрены механизмы безопасности CI\CD. Предложен регулярный аудит безопасности API, основанный на рекомендациях OWASP Top 10, для оперативного устранения уязвимостей и минимизации рисков [10, 11]. Также рекомендована настройка белого списка атрибутов, доступных для изменения через API, контроль и дополнение заголовков HTTP и настройка мониторинга. Отмечена необходимость исключить из доступных полей чувствительные параметры, такие как "роль" или "привилегии". [12]

Выводы

В результате проведенного исследования установлено, что обеспечение безопасности API требует комплексного подхода на всех этапах жизненного цикла разработки программного обеспечения (SDLC). Опираясь на рекомендации OWASP и применяя современные инструменты тестирования, удалось выявить и устранить большинство потенциальных уязвимостей.

Достоверность в части исследования методов автоматизированного выявления уязвимостей представлена практическими экспериментами с использованием виртуальных машин с уязвимым веб-приложением и сканеров, которые показали, что автоматизация существенно снижает трудозатраты и увеличивает покрытие возможных сценариев атак.

Достоверность в части рекомендаций по обеспечению безопасности API подтверждается как практически, путем применения предложенных мер на исследуемый API-интерфейс веб-приложения с закрытием выявленных уязвимостей, так и теоретически, на основании отечественных и международных методик по информационной безопасности. [13, 14].

Таким образом, в данной работе были предложены новые механизмы защиты API-интерфейсов в области информационной безопасности.

Литература

1. *Садовая Е.Н. Современные вызовы и угрозы информационной безопасности REST API и способы их предотвращения // Молодой исследователь Дона. 2023. № 8 (3). С. 67-71.*
2. *Белых, М. И. Разработка стенда по исследованию компьютерных атак на веб-сервер / М. И. Белых // Информационная безопасность и защита персональных данных: Материалы XII Межрегиональной научно-практической конференции, Брянск, 30 апреля 2020 года / Под редакцией О.М. Голембиовской, М.Ю. Рытова. – Брянск: Брянский государственный технический университет, 2020. – С. 3-7. – EDN SKQQLG.*
3. *Жиренкин, А. В. Развитие элементов архитектуры современных веб-приложений и их влияние на разработку / А. В. Жиренкин, А. К. Старосельский // Вестник науки. – 2023. – Т. 3, № 6(63). – С. 869-872. – EDN ZNMGYR.*
4. *Арустамян С.С., Антипов И.С. Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ. В сборнике: Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. С. 11-15.*
5. *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,*
6. *Станкевичус, А. А. Современное тестирование программного обеспечения. Технология автоматизированного тестирования - фаззинг // Сборник докладов 20-й научно-технической конференции, Саров, 2022 – ФГУП «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики», 2023. – С. 559-565. – DOI 10.53403/9785951505460_559. – EDN REIRUK.*
7. *Федоренко, Б. Н. Оценка эффективности коммерческих сканеров безопасности веб-приложений / Б. Н. Федоренко, М. Д. Шеламов, И. Ф. Михалевич // Приложение к журналу "Мир транспорта". – 2022. – № 1(11). – С. 29-34. – EDN TJWWAL.*
8. *Gutiérrez, S. L. A Cloud Pub/Sub Architecture to Integrate Google Big Query with Elasticsearch using Cloud Functions / S. L. Gutiérrez, Ya. Pérez Vera // International Journal of Computing. – 2022. – P. 369-376. – DOI 10.47839/ijc.21.3.2694. – EDN MLDSUO.*
9. *О некоторых особенностях JWT аутентификации в веб-приложениях / А. Б. Бетелин, И. Б. Егорычев, А. А. Прилипко [и др.] // Труды научно-исследовательского института системных исследований Российской академии наук. – 2021. – Т. 11, № 1. – С. 4-10. – DOI 10.25682/NIISI.2021.1.0001. – EDN VRXEVL.*
10. *Тушнов А.А., Трофимов В.В. Риски, управление рисками при внедрении IoT-систем и API для сбора данных в агропромышленном комплексе // Сборник трудов конференции. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2024. С. 27-33*
11. *Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p.*
12. *Grigoryan D., Brazhenko D. Effective REST API Security Technique Using Dynamic Hash Key // Инновации и инвестиции. 2024. № 2. С. 246-250.*
13. *Голушко А.П. Информационная безопасность REST API на этапе их проектирования и разработки // Труды Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнева. 2023. С. 368-371.*
14. *Barabanov A., Dergunov D., Makrushin D., Teplov A. Automatic detection of access control vulnerabilities via API specification processing. // Voprosy Kiberbezopasnosti [Cybersecurity issue], 2022, no. 1 (47), pp. 49-65.*

Security audit of APIs deployed or under development

Evseev V.L.[64]**, Linev N.V.**[65]**, Mamontov A.S.**[66]**, Pechersky V.A.**[67]**,**
Mamontov V.S.[68]**, Aparina A.A.**[69]

A

bstract. The purpose of the work is to study security audit methods and tools for APIs (Application Programming Interfaces) under development and APIs deployed in various information systems. The key vulnerabilities and threats specific to the APIs were considered, including the risks associated with unauthorized access, data leaks and privilege abuse. The analysis of modern approaches to identifying vulnerabilities and ensuring security of APIs at their development and deployment stages was carried out, with an emphasis on automation of testing and security monitoring processes. Particular attention was paid to the integration of APIs' protection mechanisms into the Software Development Life Cycle (SDLC) to minimize risks and prevent threats.

Keywords: SDLC, OpenAPI, interface security, test automation, Swagger.

[64] Vladimir Evseev, Ph.D., Associate Professor, National Research Nuclear University MEPhI, Moscow, vlevseev@mephi.ru
[65] Nikolay Linev, National Research Nuclear University MEPhI, Moscow, nikol.linev@gmail.com
[66] Alexander Mamontov, National Research Nuclear University MEPhI, Moscow, acmamontov@gmail.com
[67] Vladislav Pechersky, National Research Nuclear University MEPhI, Moscow, pecherskiyvl@gmail.com
[68] Valentin Mamontov, Swordfish security, Moscow, vmamontov@swordfishsecurity.ru
[69]Alena Aparina, Leonov Moscow Region University of Technology, Korolev, yelenaaparina@yandex.ru

УДК 004.056

Инновационные решения в управлении доступом и сетевой сегментации в телекоммуникациях транспортной отрасли

Желенкова М.Б.[70]

Аннотация: В данной работе рассмотрены классические методы управления доступом и сегментации сети, выделены основные недостатки существующих методов., Предложен неочевидный подход, базирующийся на использовании адаптивных моделей управления доступом и микросегментации с помощью машинного обучения. Применение данных решений значительно повысило уровень эффективности сетевой безопасности путем повышения точности обнаружения угроз, снижения человеческого фактора и ресурсозатрат. Эти решения применимы в любых системах, где требуется высокая степень контроля, автоматизация и устойчивость к динамическим угрозам, поэтому их можно использовать не только в транспортной отрасли, но и в иных сферах.

Ключевые слова: микросегментация, информационная безопасность, адаптивное управление, машинное обучение

Введение

Существует несколько ключевых элементов обеспечения безопасности, которые должны быть отражены в создаваемой инфраструктуре безопасности: управление доступом; управление угрозами; управление конфиденциальностью; ведение контрольных журналов и мониторинг [1]. В условиях стремительного роста уровня цифровизации и усложнения работы телекоммуникационных систем транспортной отрасли во всем мире технологии управления доступом и сегментации сети получают роль одного из ключевых элементов обеспечения информационной безопасности. Традиционные подходы, основанные на тонко настраиваемых политиках и физическом разделении сегментов, уже не отвечают требованиям и возможностям современных инструментов, таких как облачные технологии, работа на удаленных устройствах, а также развитым возможностям злоумышленников.

Основные методы управления доступом внутри сети и ее сегментация

Управление доступом в сети включает в себя реализацию механизмов, которые определяют, какие пользователи или устройства имеют право на доступ к тем или иным ресурсам. Активно используемых механизмов-основ в решении данного вопроса не так много: ролевое управление, контроль на основе атрибутов, уровневый доступ, а также концепт «нулевого доверия».

Ролевое управление доступом предполагает, что каждому пользователю или устройству присваивается роль, которая определяет доступ к определенным ресурсам. Основная идея – максимальное приближение логики работы системы к разделению функций персонала в организации [2]. Этот метод эффективен для организаций транспортной отрасли с четко обусловленной иерархией и предсказуемым взаимодействием источников через конкретные потоки данных. Неоспоримые плюсы ролевой модели: возможность контроля доступа с точностью до объекта; в больших организациях авторизация роли сразу для нескольких пользователей облегчает задачу управления политикой безопасности [3]. Однако он слабо адаптируется к динамическим изменениям. Схожей концепцией обладает механизм многоуровневого доступа, который используется для сегментации на основе уровней конфиденциальности или критичности данных.

[70] Желенкова Маргарита Борисовна, Российский Университет Транспорта (МИИТ), г. Москва, vfhujirf5@mail.ru

Контроль доступа на основе атрибутов учитывает набор определенных характеристик информации, таких как местоположение, тип устройства, время суток и уровень доверия. Централизованная политика определяет, какие комбинации атрибутов пользователя и объекта требуются для выполнения того или иного действия [4]. Данный подход обеспечивает большую гибкость, но усложняет управление из-за необходимости обрабатывать множество условий и правил.

Метод, носящий название «нулевое доверие», предполагает, что ни один пользователь или устройство не получают доступ по умолчанию. В этой модели безопасности каждый запрос на доступ к ресурсам должен быть строго аутентифицирован и авторизован, независимо от местоположения и статуса устройства [5]. Это значительно минимизирует риски, но все еще является крайне ресурсозатратным способом обеспечения безопасности. При проектировании систем информационной безопасности предприятия на основе архитектуры нулевого доверия необходим сбор большого объема данных [6].

Сегментация сети представляет собой еще один способ обеспечения защиты телекоммуникаций. Она предполагает разделение на изолированные части для максимального ограничения последствий потенциального инцидента безопасности.

Физическая сегментация считается устаревшим относительно нынешних реалий способом. Она обеспечивает высокий уровень изоляции, используя отдельное оборудование и каналы передачи данных. Этот подход является дорогим и сложным в масштабировании, поэтому крайне невыгоден для постоянно расширяющихся организаций, особенно в контексте транспортной отрасли.

Виртуальная сегментация является более предпочтительной. Она куда доступнее для реализации, поскольку производится с помощью виртуальных локальных или частных сетей, позволяя логически изолировать сегменты внутри одной физической инфраструктуры. Примерно на том же уровне популярности и простоты использования находится и микросегментация, которая применяется преимущественно в облачных средах и виртуализированных системах. Основное преимущество микросегментации заключается в том, что для злоумышленников, взломавших один сегмент, другие остаются закрытыми [7]. Этот подход помогает ограничить латеральное перемещение потенциальных злоумышленников внутри сети, существенно снижая риски атак и утечек данных. Кроме того, микросегментация увеличивает видимость взаимодействий внутри сети, позволяя оперативно реагировать на подозрительную активность и предотвращать возможные нарушения безопасности [8]. Она управляет доступом на уровне отдельных приложений или процессов, что обеспечивает гибкость и высокую точность контроля.

Перечисленные методы имеют определенный ряд преимуществ, однако все еще обладают крупными недостатками и ограничениями:

– сложность в управлении большими сетями с быстро меняющимися потоками данных;

– неэффективность против современных угроз, таких как сложные целевые атаки;

– низкая адаптивность к новым условиям, включая гибридные и облачные инфраструктуры.

Эти проблемы стимулируют разработку и внедрение инновационных решений.

Адаптивное управление доступом и сегментация через машинное обучение

Большинство недостатков современных методов управления доступом и сегментации может быть устранено или уменьшено с помощью внедрения алгоритмов машинного обучения (далее – АМО). Этот подход позволяет анализировать огромные объемы сетевого трафика, выявлять аномалии и адаптировать политики управления доступом в реальном времени.

АМО способны проводить анализ поведения пользователей и устройств внутри сети, выявляя отклонения от нормы, заявленные администратором в настройках. Например, если

пользователь внезапно запрашивает доступ к ресурсам, которые не связаны с его ролью, система может заблокировать запрос или потребовать произведение дополнительного уровня аутентификации.

Также на основе данных логирования АМО могут прогнозировать потенциальные атаки и автоматически усиливать или ослаблять защиту определенных сегментов сети. Таким образом появляется возможность реализации адаптивной системы регулирования правил и выстраивания приоритетов в телекоммуникационных системах. Вместо жестких и перманентных настроек, система динамически формирует политики доступа на основе контекста, подключая результаты обработки текущего состояния сети, поведение пользователей и уровня угроз. Никто не мешает при этом подключить централизованное управление для произведения более тонких настроек, редактуры шаблонов правил администраторами в любом из сегментов сети.

Не менее облегчить управление и усилить механизмы защиты поможет микросегментация сети с применением все тех же АМО.

Все еще благодаря способности АМО анализировать сетевой трафик и журналы аудита сети имеется возможность автоматического создания сегментах, основанных на естественных потоках данных. Это значительно упрощает процесс управления и снижает риски ошибок конфигурации, которые могут возникнуть при разделении сегментов вручную.

Также АМО имеют возможность динамического управления уже реализованными сегментами. Настройки внутри сегментов могут автоматически изменяться или адаптироваться под текущие условия. Например, при обнаружении подозрительной активности в одном из сегментов доступ к нему может быть мгновенно ограничен.

Таким образом внедрение АМО может обеспечить следующие положительные эффекты:

– повышенная точность за счет беспрерывного анализа данных в реальном времени;

– уменьшение зависимости от ручного администрирования и перераспределение нагрузки на человеческий ресурс исключительно для централизованного направления;

– высокая скорость реакции на возникновение новых угроз или подозрительной активности внутри сети.

Для внедрения адаптивного подхода с использованием АМО рекомендуется выполнить ряд необходимых шагов.

В первую очередь это создание набора данных, путем сбора информации о сетевом трафике, поведении пользователей и уже определенных инцидентах безопасности и их классификации. Далее необходимо провести обучение алгоритмов на основе данных обучающей выборки, чтобы они могли корректно идентифицировать аномалии и прогнозировать угрозы. После окончания тестирования и обучения важно правильно интегрировать АМО с существующей инфраструктурой.

Стоит отметить, что для использования всех преимуществ АМО необходимо постоянно анализировать результаты и обновлять модели для того, чтобы они оставались эффективными в изменяющихся условиях, а также для предотвращения возможных ошибок в работе.

Выводы

В данной работе рассмотрены методы управления доступом и сегментации сети, включая традиционные подходы, такие как ролевое управление, контроль на основе атрибутов и концепция «нулевого доверия». Проведен анализ их ограничений, в частности, низкая адаптивность к динамичным условиям и сложность масштабирования. Основное внимание уделено инновационному подходу, основанному на применении машинного обучения для адаптивного управления доступом и динамической микросегментации.

В настоящее время технологии машинного обучения и нейросетей применяются для решения множества задач классификации, прогнозирования и принятия решений [9, 10]. Ожидаемый эффект заключается в формировании новой парадигмы управления сетевой безопасностью, которая сочетает в себе возможности аналитики больших данных и АМО. Это открывает новые горизонты в научной области информационной безопасности, предоставляя инструменты для автоматизации, повышения точности выявления угроз и адаптивного реагирования на них. Вклад данной работы состоит в интеграции методов анализа поведения и динамического управления политиками доступа в контексте современной гибридной инфраструктуры.

Практическая достоверность предлагаемого подхода подтверждена реальными кейсами внедрения адаптивных систем безопасности на основе АМО. Такие решения уже показали свою эффективность в ведущих компаниях, успешно предотвращая инциденты и снижая нагрузку на администраторов.

Одним из примеров является MaxPatrol SIEM от Positive Technologies. Система может быть адаптируема к любой IT-инфраструктуре и работает для всех уровней управления – от рядового администратора до руководителя подразделения [11]. В компании успешно внедряют рекомендательные системы и анализ цепочек процессов с помощью АМО. Например, подобные модели уже помогают определять аномалии в поведении пользователей и процессов. Использование матриц взаимодействий «пользователь – процесс» позволяет находить несоответствия в привычных действиях, минимизируя ложные срабатывания. Эти решения используются в продуктах компании для повышения уровня информационной безопасности и оперативности реагирования на угрозы Указанная SIEM-платформа использует АМО для обнаружения поведенческих аномалий, путем отслеживания нетипичного поведения пользователей. Это позволяет системе быстрее реагировать на подозрительные действия и снижать количество ложноположительных тревог.

Список литературы

1. Акулов, А. А. Проблемы управления доступом к ресурсам локальной сети / А. А. Акулов // Modern Science. – 2020. – № 12-3. – С. 193;

2. Цветков, А. Ю. Сравнение мандатной, дискреционной и ролевой модели управления доступом / А. Ю. Цветков, Е. Ю. Рузманов // Инновации. Наука. Образование. – 2021. – № 29. – С. 73;

3. Бирюков, М. А. Особенности реализации дискреционной модели управления доступом средствами ролевой модели / М. А. Бирюков, Е. В. Волкова, И. Б. Саенко // Региональная информатика и информационная безопасность, Санкт-Петербург, 01–03 ноября 2017 года. Том Выпуск 4. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. – С. 48;

4. Кибербезопасность. RBAC vs. ABAC / А. В. Аменицкий, И. В. Рухович, Л. А. Аменицкая, Д. А. Аменицкий // Современная наука, общество и образование: актуальные вопросы, достижения и инновации : монография. – Пенза : Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 217;

5. Пашкин, М. С. Сравнение модели нулевого доверия и традиционной модели безопасности информации / М. С. Пашкин, С. А. Молоденков // Современные научные исследования и инновации. – 2023. – № 11(151);

6. Валеев, С. С. Паттерны проектирования архитектуры нулевого доверия / С. С. Валеев, Н. В. Кондратьева // Инженерный вестник Дона. – 2023. – № 9(105). – С. 76;

7. Кучер, В. А. Микросегментация в информационной безопасности / В. А. Кучер // Молодой исследователь Дона. – 2021. – № 3(30). – С. 54;

8. Репетий, Е. О. Микросегментация сети как ключевой элемент стратегии Zero Trust / Е. О. Репетий // Научный аспект. – 2024. – Т. 44, № 4. – С. 5788;

9. Букин, А. В. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей / А. В. Букин, А. В. Самонов, Э. И. Тихонов // Вопросы кибербезопасности. – 2022. – № 5(51). – С. 61-73. – DOI 10.21681/2311-3456-2022-5-62.

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

11. Оболонская, А. В. Функциональные возможности и архитектура системы выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз / А. В. Оболонская, Г. В. Мелузов // Охрана, безопасность, связь. – 2024. – № 9-2. – С. 136.

Научный руководитель: Марков Алексей Сергеевич, профессор, доктор технических наук, президент группы компаний «Эшелон», НПО Эшелон, a.markov@npo-echelon.ru.

Innovative solutions in access control and network segmentation in telecommunications of the transport industry

Zhelenkova M.B.[71]

Abstract: In this article, classical methods of access management and network segmentation were analyzed, and the main shortcomings of existing methods were identified. An unconventional approach, based on the use of adaptive access management models and micro-segmentation with the help of machine learning, was proposed. The application of these solutions significantly increased the efficiency of network security by improving threat detection accuracy, reducing human error, and optimizing resource costs. These solutions are applicable to any systems requiring a high level of control, automation, and resilience to dynamic threats, and can therefore be utilized not only in the transport sector but also in other industries.

Keywords: microsegmentation, information security, adaptive control, machine learning

[71] Zhelenkova Margarita Borisovna, Russian University of Transport (MIIT), Moscow, vfhujirf5@mail.ru

УДК 004.056

Особенности обеспечения доверия программно-аппаратных комплексов для критической информационной инфраструктуры

Жуков И.Ю.[72]

Статья посвящена анализу проблем внедрения доверенных программно-аппаратных комплексов на объектах критической информационной инфраструктуры. Рассмотрены прототипы технических решений, позволяющие блокировать санкционное вредоносное вмешательство в ряд отечественных отраслевых инфраструктур ТЭК России после начала СВО. Сделан вывод, что необходимо разработать такие решения для всех КИИ государства, обеспечивающие бесшовный переход с импортных на отечественные решения, сохраняя устойчивое одновременное функционирование отечественного и зарубежного оборудования.

Ключевые слова: критической информационной инфраструктуры, программно-аппаратные комплексы, информационная безопасность, доверенные комплексы.

Современные информационные технологии позволяют, независимо от географического размещения оборудования и области его применения, осуществлять постоянный контроль состояния и контролировать выполнение потребителями лицензионных соглашений, определять геолокацию и область применения промышленного оборудования и транспортных средств, позволяют дистанционно обновлять перечень сервисов, а в случае нарушения лицензионных соглашений, имеют возможность анализировать все события и информационные потоки контролируемого оборудования, а также принимать решения на блокирование как части функций, так и оборудования в целом [1, 2].

Производители оборудования обладают инструментами, позволяющими ему «следить» за проданными ИТ-изделиями, за их пользователями, за технологическим оборудованием, а также вмешиваться в функционирование систем с враждебными целями.

В связи с ужесточением санкционной политики со стороны недружественных стран, резко возросла угроза блокирования или перехвата управления технологическим оборудованием особо важных объектов критической информационной инфраструктуры государства [3-9].

В соответствии с Указом Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» Минпромторг провел большую работу по стимулированию разработки оборудования и в первую очередь компьютерной техники (hardware) российскими производителями. В части перехода ИТ-рынка на отечественное ПО (software) ряд важных мер предпринял Минцифры России.

Решением МВК Совета безопасности РФ Госкорпорация «Росатом» определена головной по обеспечению безопасности КИИ России. Создано АО «НПО «Критические информационные системы», основными направлениями деятельности являются: разработка, производство, техподдержка и сервисное обслуживание доверенных ПАВК для КИИ, модулей для комплектации ПАК и ПО, организация разработки ключевой отечественной ЭКБ для доверенных ПАК, создание САПР для проектирования микроэлектроники, разработка национальных стандартов в КИИ (ТК-167) [10].

В целом наметилась положительная тенденция по развитию российской ИТ-промышленности, микроэлектроники и программного обеспечения. Но несмотря на успехи и недостатки данных Программ следует обратить внимание, что даже положительное

[72] Жуков Игорь Юрьевич, д.т.н., Группа компаний «Инфотактика», НИЯУ МИФИ, Москва, e-mail: izhukov@infotaktika.ru

решение поставленных задач к 2030 году не обеспечит устойчивого функционирования КИИ России. Это связано с тем, что в существующую критическую информационную инфраструктуру вложены десятки-сотни триллионов долларов. Отраслевые КИИ используют весь спектр достижений мировых ИТ-гигантов и отраслевых лидеров. При этом в задачах импортозамещения оборудования и программного обеспечения решаются задачи создания отечественных аналогов, которые являются зачастую репликами западных решений, воспроизводимые на территории РФ, повторяя проприетарные протоколы и механизмы, архитектуру, сохраняющие монопольный контроль международных компаний и холдингов нашей КИИ.

Устраняя этот недостаток постепенно достигается более высокий уровень функциональности отечественных решений с обеспечением совместимости с их замещаемым зарубежным аналогом. Однако достижение 100% совместимости практически невозможно [10-15].

В качестве примера стоит вспомнить опыт создания отечественного ПО. Основатель Линус Торвальдс месяц назад принял решение об изоляции российских программистов. После сертификации и принятии на снабжения МСВС 3.0 (предтеча AstraLinux) функционируют под MS Windows [11]. Понадобилось 20 лет, чтобы «отечественные» ОС стали базисов российских ГИС. Аналогично. Отечественные САПР (типа Компас) настойчиво повышают свою функциональность и совместимость с западными САПР типа Siemense NX, но ведущие российские компании вынуждены продолжать работать на западном ПО.

В этой связи выработаны технические решения, позволяющие блокировать санкционное вредоносное вмешательство в ряд отечественных отраслевых инфраструктур ТЭК России после начала СВО.

Необходимо разработать такие решения для всех КИИ государства, обеспечивающие бесшовный переход с импортных на отечественные решения, сохраняя устойчивое одновременное функционирование отечественного и зарубежного оборудования.

Литература

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

2. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении. -Иннополис: Издательский Дом «Афина», 2017. 440 с.

3. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры / Горбатов В.С., Жуков И.Ю., Кравченко В.В., Правиков Д.И. // Безопасность информационных технологий. 2022. Т. 2.

4. Марков А.С. Проблемные вопросы повышения достоверности идентификации ресурсов критически важной инфраструктуры // В сборнике: Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. Сборник докладов участников XVI международного форума. НАМИБ. 2022. С. 86-91.

5. Петренко С.А. О решении проблемы раннего предупреждения компьютерного нападения на критическую информационную инфраструктуру российской федерации // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 15-19.

6. Состояние и перспективы развития механизмов доверия критической информационной инфраструктуры / Жуков И.Ю., Муравьев С.К., Комаров Т.И. // Методы и технические средства обеспечения безопасности информации. 2024. № 33. С. 112-113.

7. Технологическая платформа реализации концепции сети кибербезопасности / Горбатов В.С., Жуков И.Ю., Кравченко В.В., Правиков Д.И. // Безопасность информационных технологий. 2023. Т. 30. № 4. С. 25-38.

8. Функциональность сети кибербезопасности критической информационной инфраструктуры / Горбатов В.С., Жуков И.Ю., Кравченко В.В., Правиков Д.И. // Безопасность информационных технологий. 2023. Т. 30. № 1. С. 27-39.

9. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры / Наталичев Р.В., Горбатов В.С., Гавдан Г.П., Дураковский А.П. // Безопасность информационных технологий. 2021. Т. 28. № 3. С. 6-27.

10. Кессаринский Л.Н. Доверенная электроника на форуме «Микроэлектроника 2024» // Вопросы кибербезопасности. 2024. № 5, С. 115-119.

11. Тюлин А, Жуков и., Ефанов Д. На страже конфиденциальной информации // Открытые системы. СУБД 2001 № 10. URL: https://www.osp.ru/os/2001/10/180520.

12. Захаренков А.И., Бутусов И.В., Романов А.А. Степень доверенности программно-аппаратных средств как показатель качества замещения импорта // Вопросы кибербезопасности. 2017. № 4 (22). С. 2-9.

13. Палехов В.С., Басараб М.А. Необходимость применения методов безопасной разработки при создании доверенных программно-аппаратных платформ // В сборнике: Безопасные информационные технологии. Материалы XII Международной научно-технической конференции, посвященной 25-летию кафедры ИУ8. Москва, 2024. С. 98-101.

14. Повышение защищенности систем автоматизации управления зданиями от компьютерных атак / Стариковский А.В., Жуков И.Ю., Михайлов Д.М., Шептунов А.А., Савчук А.В., Крымов А.С. // Спецтехника и связь. 2012. № 4. С. 2-5.

15. Шелухин О.И., Раковский Д.И. Разработка программно-аппаратного комплекса моделирования многозначных компьютерных атак // Вопросы кибербезопасности. 2024. № 4 (62). С. 116-130.

Trustworthiness for hardware and software systems for critical information infrastructure

Zhukov I.Yu[73].

The article is devoted to analysing the problems of implementing trusted hardware and software complexes at critical information infrastructure facilities. Prototypes of technical solutions that allow blocking sanctioned malicious interference in a number of domestic industry infrastructures of the Russian fuel and energy complex after the beginning of the SWO are considered. It is concluded that it is necessary to develop such solutions for all the state's CII, providing a seamless transition from imported to domestic solutions, while maintaining sustainable simultaneous operation of domestic and foreign equipment.

Keywords: critical information infrastructure, software and hardware complexes, information security, trusted complexes.

[73] Igor Yuryevich Zhukov, PhD (technical sciences), Infotactica Group of Companies, National Research Nuclear University MEPhI, Moscow, e-mail: izhukov@infotaktika.ru

УДК 004.75

Применение прокси-подписи в различных информационных системах

Зарифьянц М.А.[74]**, Пушкин Н.Д.**[75]**, Тырнов Ф.А.**[76]**,**
Давыдов Н.Н.[77]**, Давыдов Г.Н.**[78]

Аннотация

Прокси-подпись позволяет одному объекту информационной системы делегировать полномочия на подпись другому объекту. Данная схема потенциально имеет множество применений, например, в распределённых системах обработки данных, где часто используется процесс делегирования. В отличие от других вариантов делегирования прав в информационной системе применение прокси-подписи позволит не только ускорить сам процесс вследствие решения таких проблем, как необходимость дополнительной подписи или генерирования новых ключей, но и сохранить все требуемые от электронной подписи свойства безопасности, например, неотказуемость, которая легко нарушается при полном делегировании.

Ключевые слова

Прокси-подпись, электронная подпись, делегатор, прокси, распределённая система, открытый ключ, закрытый ключ.

Введение

Во многих информационных системах возникает вопрос передачи прав между пользователями, например, на подпись документов (цифровой аналог печати) [1]. Можно выделить три варианта делегирования прав на подпись: полное делегирование, делегирование с ордером и частичное делегирование с использованием прокси-подписи [2]. Первый вариант простейший, однако, в таком случае делегатор просто передаёт прокси свой закрытый ключ, что может привести к нарушению безопасности. Второе решение вводит в систему ордер, что увеличивает время, затрачиваемое на проверку вдвое. Прокси-подпись позволяет объекту информационной системы, называемому делегатором или основным подписывающим, передавать права на подпись от своего имени другому объекту, называемому делегированным лицом или прокси [3]. Прокси-подпись может быть проверена любым пользователем, имеющим доступ к открытому ключу делегатора. Схема прокси-подписи состоит из: схемы стандартной электронной подписи (протокола, который используют оба пользователя, для того чтобы делегатор назначил второго пользователя в качестве подписывающего доверенного лица); алгоритма подписи, который будет использоваться подписывающими доверенными лицами (он в свою очередь может отличаться от используемого для стандартной подписи) и соответствующего алгоритма проверки для прокси-подписи. Впервые, алгоритм прокси-подписи был реализован M. Mambo, K. Usada, E. Okamoto [4]. Данная реализация основана на проблеме дискретного логарифмирования.

Примеры реализации прокси-подписи

Предложенная схема прокси-подписи - электронная подпись с открытым ключом, основанная на проблеме дискретного логарифмирования.

$$v \equiv g^{s} \bmod p \quad (1)$$

$$s \in \mathbb{Z}_{p-1} \backslash \{0\} \quad (2)$$

[74] Зарифьянц Михаил Алексеевич, стажёр, АНО «НТЦ ЦК», Москва, Россия, misha.zarif@mail.ru
[75] Пушкин Никита Дмитриевич, стажёр, АНО «НТЦ ЦК», Москва, Россия, ndp2012@yandex.ru
[76] Тырнов Филипп Александрович, стажёр, АНО «НТЦ ЦК», Москва, Россия, fil.tyrnov@yandex.ru
[77] Давыдов Николай Никитич, стажёр, АНО «НТЦ ЦК», Москва, Россия, nn_davydov@mail.ru
[78] Давыдов Григорий Никитич, стажёр, АНО «НТЦ ЦК», Москва, Россия, davy.grig.n@mail.ru

В данной схеме v - открытые данные делегатора, s - секрет делегатора, g - генератор из мультипликативной группы целых чисел по основанию p, где p - простое число длиной более, чем 512 бит.

Шаг 1 - генерация прокси. Делегатор выбирает случайное число k, вычисляет значение открытого ключа прокси K, а затем вычисляет значение закрытого ключа прокси σ с использованием своего закрытого ключа (секрета).

$$k \in \mathbb{Z}_{p-1} \setminus \{0\} \quad (3)$$

$$K = g^k \bmod p \quad (4)$$

$$\sigma = s + kK \bmod p - 1 \quad (5)$$

Шаг 2 - передача прокси. Делегатор безопасным образом передает прокси пару значений (σ, K).

Шаг 3 - проверка прокси. Прокси проверяет соотношение:

$$g^{\sigma} \equiv vK^K \bmod p \quad (6)$$

Если переданная пара значений удовлетворяет равенству, то прокси считается корректным, иначе запрос на верификацию отклоняется.

Шаг 4 - прокси-подпись документа. Прокси подписывает документ от имени делегатора, используя σ как альтернативу s.

Шаг 5 - проверка прокси-подписи. Проверка прокси-подписи происходит в том же порядке, что и верификация обычной электронной подписи, но с добавлением вычисления проверки прокси (6). Использование в процессе подписи открытого значения v делегатора подтверждает его вовлеченность в процесс подписи, что как раз и сохраняет свойство неотказуемости.

Характерные применения прокси-подписи.

Возможные применения данной технологии крайне обширны, так, множество авторов с момента её изобретения предлагали варианты эффективного использования, среди которых: цифровой аналог печати (обычное делегирование подписи документов), авторизация в распределенных системах [5-7], использование в облачных вычислениях [8], в электронном голосовании [9], применение мобильными агентами [10], а также как доказательство пути в графе [11]. В выступлении будет рассмотрен механизм подписи, предложенный M. Mambo, K. Usada, E. Okamoto, и возможность его применения для делегирования прав в распределенных системах.

Выводы

Проведенная работа показала, что прокси-подпись - это эффективное средство для делегирования полномочий в различных информационных системах. Она облегчает процесс передачи прав в распределённых системах, позволяя не генерировать лишние ключи, как в случае с делегированием с ордером, и в то же время сохраняет все требуемые от электронной подписи свойства безопасности. Стандартов по использованию механизма прокси-подписи в РФ нет, тем не менее исследования по всему миру показывают, что её применения крайне обширны, например, при авторизации в распределенных системах, использовании в облачных вычислениях, в электронном голосовании, применении мобильными агентами. Таким образом, можно сделать вывод, что внедрение прокси-подписи в стране необходимо, особенно с учетом стремительного развития цифровых технологий. В процессе работы был рассмотрен механизм подписи, предложенный M. Mambo, K. Usada, E. Okamoto, являющийся основополагающим в исследованиях в данном направлении.

Работа проводилась при поддержке АНО НТЦ ЦК «Цифровая криптография».

Литература

1. *Математические основы информационной безопасности / Басараб М.А., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г. и др.: Под ред. Матвеева В.А. - М.: МГТУ им.Н.Э.Баумана, 2013. -244 с.*
2. *Leiwo, Jussipekka & Hänle, Christoph & Homburg, Philip & Tanenbaum, Andrew. (2000). Disallowing Unauthorized State Changes Of Distributed Shared Objects. 381-390. 10.1007/978-0-387-35515-3_39.*
3. *Boldyreva, Alexandra & Palacio, Adriana & Warinschi, Bogdan. (2003). Secure Proxy Signature Schemes for Delegation of Signing Rights. Journal of Cryptology. 25. 10.1007/s00145-010-9082-x.*
4. *M. Mambo, K. Usuda, E. Okamoto. Proxy signatures for delegating signing operation. In Proc. 3rd ACM Conference on Computer and Communications Security, 1996.*
5. *B. C. Neuman. Proxy based authorization and accounting for distributed systems. In Proceedings of the 13th International Conference on Distributed Computing Systems, pages 283–291, 1993.*
6. *V. Varadharajan, P. Allen, and S. Black. An analysis of the proxy problem in distributed systems. In Proceedings of 1991 IEEE Computer Society Symposium on Research in Security and Privacy, pages 255–275, 1991.*
7. *A. Bakker, M. Steen, and A. S. Tanenbaum. A law-abiding peer-to-peer network for free-software distribution. In IEEE International Symposium on Network Computing and Applications (NCA'01), 2001.*
8. *Weissman J,Ramakrishnan S. Using Proxies to Accelerate Cloud Applications.Proceedings of the Workshop on Hot Topics in Cloud Computing. 2009. p.14–19.*
9. *R.Lu, Z.Cao. Designated verifier proxy scheme with message recovery. Applied Mathematics and Computation, 169(2), 2005, 1237-1246.*
10. *Park, Hee-Un & Lee, Im-Yeong. (2001). A Digital Nominative Proxy Signature Scheme for Mobile Communication. 451-455. 10.1007/3-540-45600-7_49.*
11. *Ateniese, Giuseppe & Hohenberger, Susan. (2005). Proxy Re-Signatures: New Definitions, Algorithms, and Applications.. IACR Cryptology ePrint Archive. 2005. 433. 10.1145/1102120.1102161.*

Научный руководитель: Варфоломеев Александр Алексеевич, доцент, к. ф.- м. н., доцент, МГТУ им. Н.Э. Баумана, a.varfolomeev@mail.ru

Application of proxy-signature in distributed data processing systems

Zarifyants M.A. , Pushkin N.D. , Tyrnov F.A. , Davydov N.N. , Davydov G.N.

Abstract

Proxy-signature allows one object of data processing system to delegate its signing rights to another object. Such scheme has a great number of possible applications, for example, in distributed data processing systems where delegation of rights is in common. Unlike other delegation schemes usage of proxy-signature allows us not only make the delegation process faster due to solving such problems as usage of additional signatures or generation of additional keys, but also preserve all security properties, such as non-repudiation, which is so easily violated in full delegation schemes.

Keywords: Proxy-signature, signature, delegator, proxy, distributed systems, public key, secret key.

УДК 004.75

Применение прокси перешифрования в распределенных системах обработки данных

Зарифьянц М.А.[79]**, Пушкин Н.Д.**[80]**, Тырнов Ф.А.**[81]**,**
Давыдов Н.Н.[82]**, Давыдов Г.Н.**[83]

Аннотация

Работа посвящена актуальной проблеме обеспечения безопасности данных в современном цифровом мире методами криптографии. Рассматривается технология прокси перешифрования, ее принципы работы и практическое применение в различных популярных сферах. Проведен детальный анализ схемы прокси перешифрования, предложенной в статье Blaze, Bleumer и Strauss "Atomic Proxy Cryptography", являющейся основополагающей в данном направлении, рассмотрены преимущества и ограничения данной технологии, а также предлагаются рекомендации по ее дальнейшему развитию. Обсуждаются найденные в литературе области применения прокси перешифрования, такие как медицина, файловое хранение, блокчейн, облачное хранение данных и облачные вычисления и др.

Ключевые слова

Криптография, шифрование, прокси перешифрование, электронная медицина, распределенные системы, облачные хранилища, облачные вычисления, ключ прокси перешифрования.

Введение

В современном цифровом мире защита конфиденциальности данных стала одной из наиболее актуальных проблем. Постоянно растущие угрозы кибербезопасности вынуждают искать новые эффективные методы защиты информации во многих сферах: от банковской до здравоохранения [1]. Одним из таких методов является прокси перешифрование. В данном докладе мы рассмотрим принцип работы этой технологии, ее преимущества и недостатки, а также области применения в различных сферах производства. В 1998 году Blaze, Bleumer и Strauss впервые формализовали понятие прокси перешифрования (Proxy Re-encryption, PRE) для шифрования с открытым ключом, определив набор алгоритмов, необходимых для реализации этой схемы. Прокси-шифрование — это тип шифрования с открытым ключом, который позволяет прокси преобразовывать шифротексты, зашифрованные одним открытым ключом, в шифротексты, зашифрованные другим открытым ключом, без раскрытия открытого текста и соответствующих закрытых ключей [2]. В общем случае принцип работы прокси перешифрования можно описать шестью шагами. Пусть есть некоторая система связи, в которой есть три субъекта: Алиса (делегатор), Боб (делегат) и прокси. Тогда процесс делегирования права на шифрование происходит следующим образом: согласование общедоступных параметров, генерация ключей, генерация ключа прокси перешифрования, шифрование, перешифрование, расшифрование.

Примеры реализации прокси перешифрования

В докладе рассматривается схема прокси перешифрования, предложенная в статье Blaze, Bleumer и Strauss. Данная схема основывается на проблеме дискретного логарифмирования и состоит из следующих этапов.

[79] Зарифьянц Михаил Алексеевич, стажёр, АНО «НТЦ ЦК», Москва, Россия, misha.zarif@mail.ru
[80] Пушкин Никита Дмитриевич, стажёр, АНО «НТЦ ЦК», Москва, Россия, ndp2012@yandex.ru
[81] Тырнов Филипп Александрович, стажёр, АНО «НТЦ ЦК», Москва, Россия, fil.tyrnov@yandex.ru
[82] Давыдов Николай Никитич, стажёр, АНО «НТЦ ЦК», Москва, Россия, nn_davydov@mail.ru
[83] Давыдов Григорий Никитич, стажёр, АНО «НТЦ ЦК», Москва, Россия, davy.grig.n@mail.ru

1. Согласование общедоступных параметров. Сначала выбирается p - простое число, равное $2q+1$, где q - также простое число. Далее задаётся циклическая группа $G=<g>$, размерность которой равна $|G|=|\mathbb{Z}_p^*|=2q$. Параметры p и g являются общедоступными глобальными параметрами системы.

2. Генерация ключей. После объявления глобальных параметров каждый пользователь создает свой закрытый ключ, случайно выбирая число $a: 0<a<p$ и $a \in \mathbb{Z}_{2q}^*$, т.е. a должно быть взаимно просто с числом $2q$. Далее пользователь вычисляет и публикует открытый ключ равный

$$g^a \bmod p \quad (1)$$

3. Генерация ключа перешифрования. Пусть делегатор Алиса имеет закрытый ключ a и соответствующий открытый ключ g^a, а делегат Боб имеет закрытый ключ b и соответствующий открытый ключ g^b. Тогда ключ прокси перешифрования рассчитывается

$$rk_{a\to b}=a^{-1}\cdot b \quad (2)$$

4. Шифрование. Для шифрования сообщений пользователь выбирает уникальный секретный параметр $k: k \in \mathbb{Z}_{2q}^*$. Далее, чтобы зашифровать сообщение m для пользователя A, имеющего открытый ключ g^a, отправитель вычисляет шифротекст $c=(c_1, c_2)$ следующим образом:

$$c_1 = m g^k \bmod p \quad (3)$$

$$c_2 = (g^a)^k \bmod p \quad (4)$$

5. Перешифрование. Стоит обратить внимание, что первая компонента шифротекста - c_1 не зависит от открытого ключа получателя сообщения. Открытый ключ встроен только во вторую компоненту - c_2, поэтому прокси для преобразования шифротекста, предназначенного для пользователя A, в шифротекст, предназначенный для пользователя B, необходимо изменить экспоненту c_2 следующим образом:

$$c_2^* = c_2^{rk_{a\to b}} \bmod p = \left(g^{a\cdot k}\right)^{a^{-1}\cdot b} \bmod p = (g^b)^k \bmod p \quad (5)$$

Таким образом, преобразованный шифротекст будет равен $c=(c_1, c_2^*)$.

6. Расшифрование. Для расшифровки полученного сообщения $c=(c_1, c_2)$ пользователь A сначала восстанавливает g^k с помощью своего закрытого ключа.

$$g^k = (c_2)^{a^{-1}} \bmod p = (g^{a\cdot k})^{a^{-1}} \bmod p \quad (6)$$

Затем, пользуясь полученным значением g^k, пользователь может восстановить исходное сообщение.

$$m = c_1 \cdot g^{k^{-1}} \bmod p \quad (7)$$

Характерные применения прокси перешифрования

В научных трудах множества авторов предлагаются различные способы эффективного применения прокси-шифрования, в частности рассматривается упрощенное распределение ключей, распределенные файловые системы [3], многоадресная рассылка [4], безопасность электронной почты [5], в средствах защиты авторских прав [6,7], использование для контроля доступа [8], передача электронных медицинских карт [9-12], безопасность Интернета вещей [13, 14], в системах подписчик-издатель [15], при облачном хранении данных и облачных вычислениях[16].

Выводы

Исследование показало, что технология прокси перешифрования (PRE) обладает широкими возможностями для применения в различных областях и является перспективным механизмом для обеспечения конфиденциальности и подлинности данных.

Основными направлениями её использования являются распределённые файловые системы, системы электронных медицинских карт и Интернет вещей, облачные вычисления и хранение.

Большой интерес и наибольшее количество публикаций связано с технологиями прокси перешифрования с использованием открытых ключей (асимметричной криптографии), примером которого является первая предложенная схема Блейза, Блюмера и Штраусса, описанная в статье "Atomic Proxy Cryptography" и основанная на проблеме дискретного логарифмирования. Дальнейшие разработанные схемы прокси перешифрования развивают новые разновидности схем шифрования с дополнительными свойствами в условиях их применения с третьей доверенной стороной.

Работа проводилась при поддержке АНО НТЦ ЦК «Цифровая криптография».

Литература

1. Математические основы информационной безопасности / Басараб М.А., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г. и др.: Под ред. Матвеева В.А. - М.: МГТУ им.Н.Э.Баумана, 2013. -244 с.
2. Blaze, Matt & Strauss, Martin. (1999). Atomic Proxy Cryptography.
3. Ateniese, Giuseppe & Fu, Kevin & Green, Matthew & Hohenberger, Susan. (2006). Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. 9. 1-30.
4. Y-P. Chiu, C-L. Lei, and C-Y. Huang (2005) Secure multicast using proxy encryption. In ICICS 2005, volume 3783 of LNCS, pages 280–290.
5. H. Khurana and H-S. Hahm. Certified mailing lists. In ASIACCS 2006, pages 46–58, 2006.
6. G. Taban, A.A. C´ardenas, and V.D. Gligor. Towards a secure and interoperable drm architecture. In ACM DRM 2006, pages 69–78, 2006.
7. Conference Paper (2012) Proxy Re-Encryption in a Privacy-Preserving Cloud Computing DRM Scheme
8. A. Talmy and O. Dobzinski. Abuse freedom in access control schemes. In AINA 2006, pages 77–86, 2006.
9. Mrs. Rashi Saxena1, N. Yogitha2, G. Swetha Reddy3, D. Rasika (2018) Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for Electronic Health Cloud
10. Yang, Yang & Ma, Maode. (2015). Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds. IEEE Transactions on Information Forensics and Security. 11. 1-1. 10.1109/TIFS.2015.2509912.
11. Bruno Rodrigues, Ivone Amorim, Ivan Silva & Alexandra Mendes (2014) Patient-Centric Health Data Sovereignty: An Approach Using Proxy Re-Encryption.
12. Matthew Green, Giuseppe Ateniese (2006) Identity-Based Proxy Re-Encryption.
13. Daniel Díaz-Sánchez; R. Simon Sherratt; Patricia Arias; Florina Almenares; Andrés Marín López (2016) Proxy re-encryption schemes for IoT and crowd sensing.
14. SuHyun Kim, ImYeong Lee (2017) IoT device security based on proxy re-encryption.
15. Himanshu Khurana, Radostina K. Koleva (2006) Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems.
16. Feixiang Zhao, Huaxiong Wang, Jian Weng (2024) Constant-Size Unbounded Multi-Hop Fully Homomorphic Proxy Re-Encryption from Lattices.

Научный руководитель: Варфоломеев Александр Алексеевич, доцент, к. ф.- м. н., доцент, МГТУ им. Н.Э. Баумана, a.varfolomeev@mail.ru

Application of proxy encryption in distributed data processing systems

Zarifyants M.A. , Pushkin N.D. , Tyrnov F.A. , Davydov N.N. , Davydov G.N.[84]

The work is devoted to the urgent problem of ensuring data security in the modern digital world by cryptographic methods. The technology of proxy re-encryption, its operating principles and practical application in various popular areas are considered. A detailed analysis of the proxy re-encryption scheme proposed in the article by Blaze, Bleumer and Strauss "Atomic Proxy Cryptography", which is fundamental in this area, is carried out, the advantages and limitations of this technology are considered, and recommendations for its further development are offered. The areas of application of proxy re-encryption found in the literature are discussed, such as medicine, file storage, blockchain, cloud data storage and cloud computing, etc.

Keywords. Cryptography, encryption, proxy re-encryption, electronic medicine, distributed systems, cloud storage, cloud computing, re-encryption key.

[84] Zarifiantz Mikhail A., Intern, ANO STC CK, Moscow, Russia, misha.zarif@mail.ru
Pushkin Nikita D., Intern, ANO STC CK, Moscow, Russia, ndp2012@yandex.ru
Tyrnov Filipp Aleksandrovich, Intern, ANO STC CK, Moscow, Russia, fil.tyrnov@yandex.ru
Davydov Nikolay Nikitich, Intern, ANO STC CK, Moscow, Russia, nn_davydov@mail.ru.
Davydov Grigory Nikitich, Intern, ANO STC CK, Moscow, Russia, davy.grig.n@mail.ru

УДК 004.056.5

Механизмы инкапсуляции ключа: причины внедрения, особенности и области применения

Зеленецкий А.С.[85]

В последнее время во многих криптографических протоколах совместно с выработкой ключа на базе схемы Диффи-Хеллмана стал применяться механизм инкапсуляции ключа. В этой работе рассматриваются причины, по которым происходит внедрение механизмов инкапсуляции ключа. Кроме того, в работе исследуются отличительные особенности данного примитива в сравнении с классической схемой выработки общего ключа, а также области его применения.

Ключевые слова: механизм инкапсуляции ключа, схемы выработки общего ключа, постквантовая криптография, криптографические протоколы.

Введение

В современной криптографии особое место занимают схемы выработки общего секретного ключа. Они используются в различных криптографических протоколах с целью установления защищенного соединения. Сформированный общий секретный ключ используется сторонами для обеспечения конфиденциальности и целостности передаваемой по открытому каналу информации. Однако в последнее время все более распространенным становится механизм инкапсуляции ключа, целью которого является безопасная передача секретного ключа от одной стороны другой. Одной из основных причин этому является тот факт, что традиционные схемы выработки общего ключа, основанные на задаче Диффи-Хеллмана [1], не являются устойчивыми к атакам с применением квантовых компьютеров [2]. За последние годы были предложены десятки схем инкапсуляции ключа, среди которых наиболее известными стали Kyber [3], Saber [4] и NTRU [5]. В этой работе мы рассматриваем отличительные особенности механизмов инкапсуляции ключа, причины их внедрения и области их применения.

Схемы выработки общего секрета

Схемы выработки общего секрета — это криптографические примитивы, позволяющие двум сторонам, обменивающимся сообщениями по открытому каналу, выработать общий секретный ключ. Наиболее распространенной схемой выработки общего ключа является схема Диффи-Хеллмана (DH, Diffie Hellman) [1], появившаяся еще в 1976 году. Безопасность данной схемы основана на сложности задачи Диффи-Хеллмана, которая в свою очередь оценивается сложностью решения задачи дискретного логарифмирования в мультипликативной группе конечного поля. В связи с развитием алгоритмов решения последней задачи, было предложено расширение классической схемы Диффи-Хеллмана, в которой вместо мультипликативной группы конечного поля используется циклическая группа точек эллиптической кривой. Такая версия схемы Диффи-Хеллмана называется ECDH (Elliptic Curve Diffie Hellman), она, например, используется в отечественном стандарте ГОСТ Р 34.10-2001/2012 [6]. Благодаря более высокой сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, ECDH обладает существенно более короткими ключами, чем классический DH, что снижает нагрузку на сеть.

Особенностью DH и ECDH можно назвать то, что обе стороны вносят одинаковый вклад в формирование общего ключа. Также оба варианта схемы подвержены атаке «человек посередине» (MITM, Man In The Middle), что привносит дополнительное требование в виде использования только аутентифицированного канала в процессе формирования общего ключа. DH и ECDH используются в множестве криптографических

[85] Зеленецкий Алексей Сергеевич, ООО «КуАпп», ООО «МЦКТ», МГТУ им. Н.Э. Баумана.

протоколов. В двух последних версиях протокола TLS, ECDH используется для формирования сессионного ключа, в прошлых версиях вместо него использовался классический DH. Причем последняя версия протокола, TLS 1.3, допускает гибридный обмен ключом — совместное использование постквантового механизма инкапсуляции ключа вместе с ECDH. В протоколе IPsec, который используется при установлении VPN-соединений, ECDH и DH используются при первоначальной установке соединения в ходе протокола IKE (Internet Key Exchange).

Как было отмечено ранее, криптографическая стойкость обеих версий схемы Диффи-Хеллмана оценивается сложностью решения задачи дискретного логарифмирования в конечной группе. Причем из-за внутреннего устройства схемы эта группа должны быть циклической, что делает ее обязательно абелевой. Квантовый алгоритм Шора [2] способен эффективно решать задачу дискретного логарифмирования в любой конечной абелевой группе. То есть схема Диффи-Хеллмана станет более небезопасной после появления квантового компьютера достаточной мощности. Причем заменить группу, как в случае с переходом от DH к ECDH, не получится по причинам, указанным выше. Таким образом, появилась необходимость в разработке способа формирования общего секретного ключа, который будет устойчивым к атакам с применением квантового компьютера.

Механизмы инкапсуляции ключа: принцип работы и особенности

Механизм инкапсуляции ключа представляет собой тройку вероятностных полиномиальных алгоритмов (KeyGen(), Enc(pk), Dec(sk, c)). Алгоритм генерации ключа KeyGen() формируют ключевую пару (pk, sk) открытого и секретного ключа. В ходе алгоритма инкапсуляции генерирует сессионный ключ ss и его шифротекст c, используя открытый ключ pk. Алгоритм декапсуляции расшифровывает шифротекст c, используя секретный ключ sk, и возвращает сессионный ключ ss. Схема формирования общего ключа при использовании механизма инкапсуляции ключа представлена ниже.

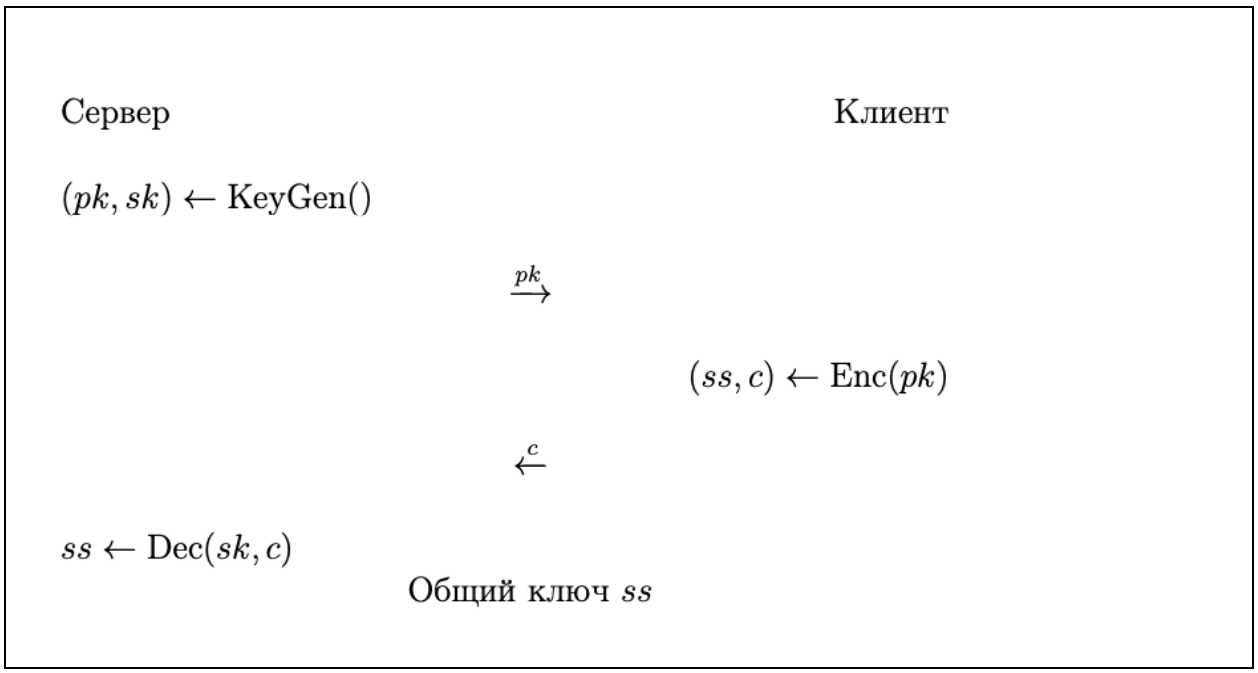


Рисунок 1. Выработка общего ключа с помощью механизма инкапсуляции ключа

Главной отличительной особенностью выработки общего ключа с помощью механизма инкапсуляции ключа является односторонность процесса: только одна сторона генерирует ключ и инкапсулирует его для передачи другой стороне. Это делает такую выработку более быстрой, особенно в сетях с высокой задержкой. Односторонность также упрощает работу при использовании ключей долговременного хранения сервером. Механизм инкапсуляции ключа также хорошо подойдет в случаях, когда сервер устанавливает защищенное соединение с различными клиентами, используя один и тот же открытый ключ. С точки зрения аутентификации, использование механизма ключа требует лишь наличие сертификата открытого ключа сервера, чтобы избежать атаки MITM. При этом аутентификация клиента во многих приложениях становится необязательной.

Обратим также внимание и на то, что схема формирования общего ключа с использованием механизма инкапсуляции труда может быть преобразована в схему, использующую ключевой материал обеих сторон, как в схеме DH или ECDH. Для этого каждая из сторон должна передать другой стороне свой инкапсулированный ключ. Сессионный ключ в такой схеме получается в результате преобразования над ключами обеих сторон.

Механизмы инкапсуляции ключа: причины внедрения

Основной причиной повышенного интереса к механизмам инкапсуляции ключа является квантовая угроза, а именно тот факт, что выработка общего ключа на базе Диффи-Хеллмана неустойчива к атакам с применением квантового компьютера. На сегодняшний день большинство постквантовых (то есть устойчивых к атакам с применением квантового компьютера) альтернатив выработке общего ключа являются механизмами инкапсуляции ключа. Это можно объяснить тем фактом, что современные постквантовые механизмы инкапсуляции ключа по сути являются слегка измененными схемами асимметричного шифрования, в то время, как схема формирования общего ключа является более сложной конструкцией. Более того, механизм инкапсуляции ключа является более гибкой конструкцией и позволяет устанавливать защищенное соединение при разных сценариях.

Механизмы инкапсуляции ключа: области применения и примеры внедрения

Основное назначение механизма инкапсуляции ключа — безопасная передача секретного ключа. Соответственно, область применения механизмов инкапсуляции ключа совпадает с областью применения схем выработки общего секрета. Именно, механизмы инкапсуляции ключа используются в криптографических протоколах в процессе установления защищенного соединения.

На сегодняшний день уже завершен процесс стандартизации первой схемы инкапсуляции ключа в США. Именно, схема Kyber [3] стала стандартом ML-KEM. В связи с этим экспертными сообществами активно разрабатываются проекты стандартов по использованию ML-KEM в различных криптографических протоколах. При этом о полной замене DH подобных схем на ML-KEM речи пока что не идет, поскольку безопасность ML-KEM основана на относительно новой задаче MLWE [7], которая еще не прошла проверку временем. Поэтому в настоящее время речь идет о внедрении гибридной схемы инкапсуляции ключа [8, 9], которая совмещает в себе схемы DH (ECDH) и ML-KEM. Такой гибридный механизм инкапсуляции ключа остается безопасных пока хотя бы одна из составляющих его механизмов является безопасным. Так в проекте стандарта [10] для TLS 1.3 в схеме формирования сессионного ключа предлагается заменить ключ, полученный в результате схемы ECDH, на конкатенацию ключей, выработанных ECDH и ML-KEM. В проекте стандарта протокола IKEv2 [11] также предлагается механизм выработки ключа, вырабатывающий сессионный ключ на базе ключей, полученных в ходе ECDH и ML-KEM.

Выводы

Механизмы инкапсуляции ключа являются более гибким инструментом для выработки общего ключа, чем классические схемы выработки общего ключа на базе схемы

Диффи-Хеллмана. Повышенный интерес к механизмам инкапсуляции ключа связан с квантовой угрозой классическим криптографическим схемам выработки общего ключа. Уже сегодня ведется активная работа над проектами стандартов для внедрения постквантовых механизмов выработки общего ключа в современные криптографические протоколы.

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 // IEEE 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. S.V. Smyshlyaev, E. Alekseev, I. Oshkin, V. Popov, etc. Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012. RFC 7835, 2016.

7. A. Langlois, D. Stehlé. Worst-case to average-case reductions for module lattices // Des. Codes Cryptogr., 2015, vol. 75, pp. 565–599.

8. Federico Giacon, Felix Heuer, and Bertram Poettering. KEM combiners. Cryptology ePrint Archive, Paper 2018/024, 2018.

9. Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. Hybrid key encapsulation mechanisms and authenticated key exchange. Cryptology ePrint Archive, Paper 2018/903, 2018

10. Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. InternetDraft draftietftlshybriddesign10, Internet Engineering Task Force, April 2024. Work in Progress

11. Panos Kampanakis and Gerardo Ravago. Postquantum Hybrid Key Exchange with MLKEM in the Internet Key Exchange Protocol Version 2 (IKEv2). InternetDraft draftkampanakismlkemikev206, Internet Engineering Task Force, August 2024. Work in Progress.

Научный руководитель: Ключарев Петр Георгиевич, професор, доктор технических наук, професор кафедры ИУ8 МГТУ им. Н.Э.Баумана, pgkl@yandex.ru.

Key Encapsulation Mechanisms: Reasons for Implementation, Features, and Applications

Zelenetsky A.S.[86]

Abstract. Recently, key encapsulation mechanisms have started to be used alongside key generation based on the Diffie-Hellman scheme in many cryptographic protocols. This work examines the reasons for the adoption of key encapsulation mechanisms. Additionally, the paper explores the distinctive features of this primitive compared to the classical shared key generation scheme, as well as its application areas.

Keywords: key encapsulation mechanism, key generation schemes, post-quantum cryptography, cryptographic protocols.

[86] Zelenetsky Alexey, QApp, RQC, BMSTU, Moscow, azelenetskiy@qapp.tech

УДК 656.257:004.056

Актуализация угроз функциональной безопасности систем микропроцессорной централизации и автоблокировки

Иванин И.И.[87]

Аннотация. В статье рассматриваются актуальные угрозы функциональной безопасности систем микропроцессорной централизации и системы автоблокировки, полученные в результате исследований.

Ключевые слова: железнодорожная автоматика и телемеханика, автоматизированное рабочее место, объектные контроллеры, защищенность, отказоустойчивость, контролируемая зона, средства защиты информации.

Введение

Системы микропроцессорной централизации (МПЦ) и систем автоблокировки (АБ) относятся к системам железнодорожной автоматики и телемеханики (ЖАТ) [1-3]. Эти системы играют главную роль в обеспечении функционально безопасности движения поездов, повышении пропускной способности железных дорог и оптимизации управления железнодорожным транспортом [5-11]. Основные процессы, обеспечиваемые системами, следующие:

- автоматизированное управление движением подвижных составов;
- обеспечение безопасности движения подвижных составов;
- мониторинг состояния путей и подвижных составов.

В настоящее время актуальным является обеспечение необходимого уровня защищенности информационных ресурсов АБ и МПЦ от угроз целостности, доступности и конфиденциальности [4, 6, 10, 12]. В данном докладе рассматриваются актуальные угрозы безопасности информации (УБИ) в соответствии требованиями с Банком данных угроз ФСТЭК России, реализация которых может повлиять на функциональную безопасность железнодорожной информационной инфраструктуры [13].

В ходе проведения исследований применялся экспертный метод оценивания актуальности угроз систем АБ и МПЦ. Результат анализа представлен в табл. 1.

Таблица 1.

Классы УБИ

№	Класс УБИ	Перечень УБИ
1	Угрозы воздействия на СЗИ, воздействия на идентификационную или аутентификационную информацию	УБИ.003, УБИ.008, УБИ.030, УБИ.031, УБИ.074, УБИ.086, УБИ.100, УБИ.152, УБИ.168, УБИ.181, УБИ.185, УБИ.187, УБИ.197, УБИ.201, УБИ.213, УБИ.214
2	Угрозы воздействия на ПО первичной инициализации	УБИ.004, УБИ.005, УБИ.009, УБИ.013, УБИ.018, УБИ.024, УБИ.032, УБИ.035, УБИ.039, УБИ.045, УБИ.053, УБИ.072, УБИ.087, УБИ.123, УБИ.129, УБИ.144, УБИ.150, УБИ.154
3	Угрозы воздействия на ИС, защищаемую информацию, ПО, ТС	УБИ.006, УБИ.007, УБИ.012, УБИ.025, УБИ.033, УБИ.036, УБИ.037, УБИ.049, УБИ.051, УБИ.061, УБИ.062, УБИ.063, УБИ.068, УБИ.071, УБИ.089, УБИ.091, УБИ.093, УБИ.094, УБИ.095, УБИ.102, УБИ.103, УБИ.109, УБИ.113, УБИ.114, УБИ.117, УБИ.118, УБИ.121, УБИ.149, УБИ.158, УБИ.162, УБИ.163, УБИ.177, УБИ.178, УБИ.179, УБИ.180, УБИ.205, УБИ.207, УБИ.210, УБИ.211, УБИ.212, УБИ.215, УБИ.216, УБИ.217
4	Угрозы, связанные с использованием технологий виртуализации	УБИ.010, УБИ.044, УБИ.046, УБИ.048, УБИ.058, УБИ.059, УБИ.075, УБИ.076, УБИ.077, УБИ.078, УБИ.079, УБИ.080, УБИ.084, УБИ.085, УБИ.108, УБИ.119, УБИ.120

[87] Иванин Иван Иванович, аспирант МИИТ (РУТ), i.ivan98@mail.ru

№	Класс УБИ	Перечень УБИ
5	Угрозы на отказ в обслуживании	УБИ.014, УБИ.022, УБИ.140, УБИ.143, УБИ.153, УБИ.155, УБИ.176, УБИ.182
6	Угрозы нарушения разграничения доступа	УБИ.015, УБИ.016, УБИ.028, УБИ.067, УБИ.074, УБИ.088, УБИ.090, УБИ.107, УБИ.112, УБИ.122, УБИ.124, УБИ.127
7	Угрозы, связанные с сетевым взаимодействием	УБИ.017, УБИ.019, УБИ.026, УБИ.034, УБИ.041, УБИ.042, УБИ.069, УБИ.075, УБИ.092, УБИ.098, УБИ.099, УБИ.104, УБИ.111, УБИ.116, УБИ.128, УБИ.130, УБИ.131, УБИ.132, УБИ.151, УБИ.159, УБИ.173, УБИ.174
8	Угрозы непосредственного физического доступа к компонентам системы	УБИ.023, УБИ.107, УБИ.139, УБИ.156, УБИ.157, УБИ.160
9	Угрозы действия вредоносных программ, использования уязвимостей ПО и ТС	УБИ.022, УБИ.027, УБИ.073, УБИ.115, УБИ.145, УБИ.167, УБИ.170, УБИ.171, УБИ.172, УБИ.175, УБИ.183, УБИ.186, УБИ.188, УБИ.189, УБИ.190, УБИ.191, УБИ.192, УБИ.193, УБИ.195, УБИ.196, УБИ.198, УБИ.203, УБИ.204, УБИ.208, УБИ.209
10	Угрозы ошибок конфигурации / внесения уязвимостей при проектировании и внедрении системы	УБИ.165, УБИ.166, УБИ.169, УБИ.206
11	Угрозы, связанные с использованием суперкомпьютеров и хранилищ больших данных	УБИ.029, УБИ.038, УБИ.050, УБИ.057, УБИ.060, УБИ.082, УБИ.097, УБИ.105, УБИ.106, УБИ.136, УБИ.146, УБИ.148, УБИ.161
12	Угрозы, связанные с использованием облачных услуг	УБИ.020, УБИ.021, УБИ.040, УБИ.043, УБИ.052, УБИ.054, УБИ.055, УБИ.056, УБИ.058, УБИ.064, УБИ.065, УБИ.066, УБИ.070, УБИ.096, УБИ.101, УБИ.134, УБИ.135, УБИ.137, УБИ.138, УБИ.141, УБИ.142, УБИ.164
13	Угрозы воздействия на беспроводные сети Wi-Fi	УБИ.011, УБИ.083, УБИ.125, УБИ.126, УБИ.133
14	Угрозы воздействия на мобильные устройства	УБИ.184, УБИ.194, УБИ.199, УБИ.200, УБИ.202
15	Угрозы воздействия на ГРИД-системы	УБИ.001, УБИ.002, УБИ.047, УБИ.081, УБИ.110, УБИ.147
16	Угрозы воздействия на программы/модели машинного обучения	УБИ.218, УБИ.219, УБИ.220, УБИ.221, УБИ.222

В табл. 2 приводится количество актуальных угроз по каждому классу угроз к каждому виду систем.

Таблица 2.

Отношение классов угроз к видам систем ЖАТ

№	Класс УБИ	МПЦ	АБ
1.	Угрозы воздействия на СЗИ, воздействия на идентификационную или аутентификационную информацию	10	11
2.	Угрозы воздействия на ПО первичной инициализации	14	12
3.	Угрозы воздействия на информационную систему, защищаемую информацию, ПО, технические средства	27	27
4.	Угрозы типа «Отказ в обслуживании»	3	3
5.	Угрозы нарушения разграничения доступа	9	9
6.	Угрозы, связанные с сетевым взаимодействием	9	8
7.	Угрозы непосредственного физического доступа к компонентам системы	6	6
8.	Угрозы действия вредоносных программ, использования уязвимостей ПО и технических средств	10	9
9.	Угрозы ошибок конфигурации / внесения уязвимостей при проектировании и внедрении системы	3	2
	ИТОГОВОЕ КОЛИЧЕСТВО АКТУАЛЬНЫХ УГРОЗ	89	85

Заключение

В работе был сделан вывод, что из 222 существующих УБИ их БДУ ФСТЭК России для МПЦ актуальны 89 типовых УБИ, из которых 83 угрозы актуальны для АРМ, 55 угроз актуальны для коммутационного оборудования, 79 угроз актуальны для ЦПУ и 13 угроз актуальны для объектных контроллеров. При этом реализация 16 угроз требует от нарушителя высокой квалификации, из которых 14 угроз относятся к угрозам, реализуемым на АРМ, 6 угроз относятся к угрозам, реализуемым на коммутационном оборудовании, 13 угроз относятся к угрозам, реализуемым на ЦПУ.

Установлено, что из 222 существующих УБИ их БДУ ФСТЭК России для систем АБ актуальны 85, из которых 83 угрозы актуальны для АРМ и Сервисного терминала, 50 угроз актуальны для Модулей передачи информации, 21 угроза актуальны для Модулей управления/Модулей реле/Модулей контроля. При этом реализация 14 угроз требует от нарушителя высокой квалификации, из которых 14 угроз относятся к угрозам, реализуемым на АРМ, 6 угроз относятся к угрозам, реализуемым на Модулях передачи информации.

Для систем МПЦ и автоматизированных перегонных систем безопасности преобладают угрозы воздействия на информацию, ПО и ТС. Данные угрозы направлены на нарушение функций безопасности, реализованных на программном или микропрограммном уровне, информацию, обрабатываемую в системе, целостность ПО и сетевое взаимодействие между компонентами системы.

Для парирования актуальных угроз могут применяться следующие организационно-технические меры:

1. Обеспечение защиты от несанкционированного доступа;
2. Проведение проверок всех компонентов и программного обеспечения на наличие не декларированных возможностей;
3. Размещение компонентов систем размещаются в условиях, исключающих наличие несанкционированного доступа;
4. Конфигурирование программно-аппаратных средств, исключающее возможность несанкционированного доступа;
5. Внедрение средства обнаружения компьютерных атак.

Соблюдение требований транспортной безопасности как правило позволяет исключить внешнего нарушителя или ограничить его возможности, тем самым минимизировать вероятность наступления событий отказов.

При реализации указанных организационно-технических мер снижается вероятность наступления событий опасного отказа, за счет введения дополнительных защитных состояний, которые понижают надежность системы, однако повышают функциональную безопасность систем.

Список литературы

1. Безродный Б.Ф. Особенности обеспечения безопасности систем ДЦ как объектов критической информационной инфраструктуры // Автоматика, связь, информатика. 2023. № 4. С. 9-11.

2. Бушуев С.В. Пути повышения провозной способности участков железных дорог // Автоматика на транспорте. 2022. Т. 8. № 4. С. 343-353.

3. Отечественные системы железнодорожной автоматики и телемеханики и задачи обеспечения их конкурентоспособности / Розенберг Е.Н., Астрахан В.И., Малинов В.М. // Электротехника. 2019. № 6. С. 2-6.

4. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП // Вопросы кибербезопасности. 2015. № 2 (10). С. 56-59.

5. Жиленков А.А., Черный С.Г. Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 58-66.

6. *Макаров Б.А. Актуальность кибербезопасности на железнодорожном транспорте // Вестник Института проблем естественных монополий: Техника железных дорог. 2015. № 3 (31). С. 10-15.*

7. *Микропроцессорная автоблокировка типа АБТЦ-МШ / Астрахан В.И., Воронин В.А., Кравец И.М., Малинов В.М., Марков А.В., Маршов С.В., Цукерман Б.Г., Шухина Е.Е. Москва, НИИАС, 2013 – 128 с.*

8. *Отечественные системы железнодорожной автоматики и телемеханики и задачи обеспечения их конкурентоспособности / Розенберг Е.Н., Астрахан В.И., Малинов В.М. // Электротехника. 2019. № 6. С. 2-6.*

9. *Подход к оцениванию информационной безопасности автоматизированных систем управления пассажирскими перевозками железнодорожного транспорта / Глухов А.П., Корниенко А.А., Белова Е.И. // Двойные технологии. 2023. № 1 (102). С. 71-77.*

10. *Противодействие компьютерным атакам в сфере железнодорожного транспорта / Бакуркин Р.С., Безродный Б.Ф., Коротин А.М. Вопросы кибербезопасности. 2016. № 4 (17). С. 29-35.*

11. *Пути развития подвижного состава в рамках цифровизации железнодорожного транспорта / Антропов А.Н., Антропова Т.А., Бушуев С.В., Волков Д.В., Колясов К.М. // Вестник Ростовского государственного университета путей сообщения. 2022. № 4 (88). С. 200-208.*

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

13. *Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p.*

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им Н.Э. Баумана.

Actualization of functional security threats for microprocessor centralization and auto-locking systems

Ivanin I.I.[88]

Abstract. The article discusses current threats to functional security for microprocessor centralization systems and auto-locking systems.

Keywords: railway automation and telemechanics, microprocessor centralization systems, auto-locking systems, threats to information security, automated workplace, object controllers, security, fault tolerance, controlled area, information security tools

[88] Ivan Ivanin, Russian University of Transport RUT (MIIT), i.ivan98@mail.ru

УДК 004.89

Комплексные кибератаки компьютерными червями с элементами искусственного интеллекта в связанных экосистемах

Корнеев Н.В. [89]

Предложена структура новой подсистемы безопасности экосистем, направленная на управление обеспечением безопасности от новой угрозы – компьютерные черви с элементами искусственного интеллекта. Рассмотрен пример компьютерного червя с элементами искусственного интеллекта для персонифицированной атаки на жертву через Telegram с использованием генеративного искусственного интеллекта. Сформулированы направления атаки компьютерного червя с элементами искусственного интеллекта на информационную инфраструктуру: через генеративный искусственный интеллект, с целью персонифицированной атаки на жертву; с враждебными самоконфигурируемыми запросами и встраивания враждебного запроса в изображение через самоконфигурируемую нейронную сеть. Выделены компоненты вектора атаки компьютерного червя с элементами искусственного интеллекта для объектов критической информационной инфраструктуры и сформулированы актуальные способы защиты: классические, специальные (SIEM, pentesting), специализированные (honeytops, distributed deception platform).

Ключевые слова: искусственный интеллект, персонифицированная атака, генеративный искусственный интеллект, враждебные самоконфигурируемые запросы, компоненты вектора атаки, SIEM, pentesting, honeytops, distributed deception platform

Введение

Суть комплексной безопасности – обеспечение всех составляющих безопасности объекта: физической, экономической, пожарной, информационной, психологической, безопасности интеллектуальной собственности, техногенной, безопасности от терроризма, экологической безопасности, энергетической безопасности в том числе новых составляющих [1].

Обобщенная структура интеллектуальной системы управления комплексной безопасностью ТЭК, с учетом развития отечественной концепции системы человек-машина, как сложной информационно-энергетической системы подробно представлена в [1].

Новая подсистема безопасности экосистем

В настоящее время целесообразно дополнить предложенную обобщенную структуру интеллектуальной системы управления комплексной безопасностью новой подсистемой безопасности экосистем [2] (рис.1). Такая подсистема будет направлена в первую очередь на управление обеспечением безопасности от новой угрозы комплексной безопасности экосистем – создания виртуального мира разумных (обладающих сознанием) систем с элементами искусственного интеллекта (ИИ), способных общаться между собой, договариваться, строить общество себе подобных, а возможно даже уничтожать людей [2].

В этой связи необходимы новые механизмы обеспечения ИБ особенно для объектов критической информационной инфраструктуры [3-7], которые целесообразно базировать на симметричных ответных технологиях – системах с элементами ИИ, по сути цифровых

[89] 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

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 [8], Irongate [9] или модули для фреймворков, таких как «Autosploit» [10], «ICSSPLOIT», «Metasploit», «Core Impact» и «Immunity Canvas».

Компьютерный червь с элементами искусственного интеллекта

В настоящий момент ярким примером такой новой угрозы комплексной безопасности являются компьютерные черви с элементами ИИ. Такие компьютерные черви с элементами ИИ способны не только нанести урон современным генеративным ИИ-агентам, но и плодиться и размножаться как любые живые организмы, создавать виртуальных подобных себе сущностей, разумных (обладающих сознанием), способных общаться между собой, договариваться, строить общество себе подобных.

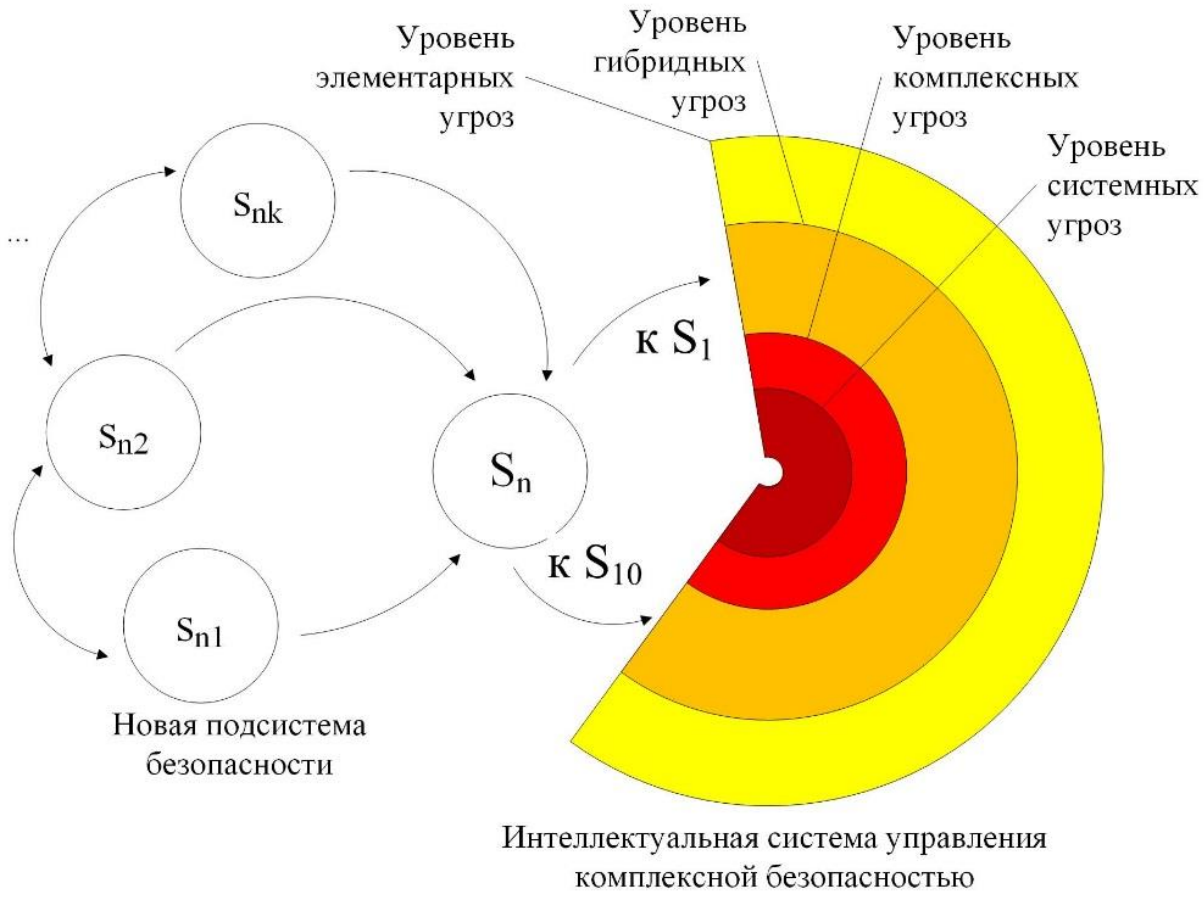


Рис.1. Новая подсистема безопасности в структуре интеллектуальной системы управления комплексной безопасностью

В исследовании [11] группа учёных продемонстрировала создание первого компьютерного червя с элементами ИИ, способного автоматически распространяться между генеративными ИИ-агентами.

Эксперименты специалистов [11] показали, как такой компьютерный червь с элементами ИИ может использоваться для атак на почтовые помощники на базе ИИ с целью кражи данных из электронных писем и рассылки спама, нарушая меры безопасности в системах ChatGPT.

Направления атаки компьютерного червя с элементами ИИ на информационную инфраструктуру

1. Атака описанная выше с использованием генеративного ИИ, с целью персонифицированной атаки на жертву, с целью кражи данных из электронных писем и рассылки спама, кражи финансовых средств со счетов и т.п.

2. Атака с враждебными самоконфигурируемыми запросами в которых компьютерный червь с элементами ИИ использует например самоконфигурируемую нейронную сеть [7].

3. Атака с враждебными самоконфигурируемыми изображениями в которых компьютерный червь с элементами ИИ использует самоконфигурируемую нейронную сеть для встраивания враждебного запроса в изображение.

И хотя до настоящего времени подтверждения самого факта направления атаки 2 и 3 не существует, следует учесть, что такие атаки вполне реальны, например в исследовании [11] показано, что враждебные самовоспроизводящиеся запросы заставляют ИИ-модель в своём ответе генерировать новый запрос, что напоминает традиционные атаки типа SQL Injection и Buffer Overflow.

Второе и третье направление атаки характерно для реальных условий эксплуатации системы, когда риск безопасности особенно для объектов критической информационной инфраструктуры становится чрезвычайно существенен.

Компоненты вектора атаки компьютерного червя с элементами искусственного интеллекта для объектов критической информационной инфраструктуры

Для объектов критической информационной инфраструктуры вектор атаки компьютерного червя с элементами ИИ направлен в первую очередь на следующие компоненты экосистем (рис.2):

1. Компоненты машинного обучения.
2. Компоненты оптимизации затрат.
3. Компоненты управления транспортной логистикой.
4. Компоненты управления эксплуатацией.

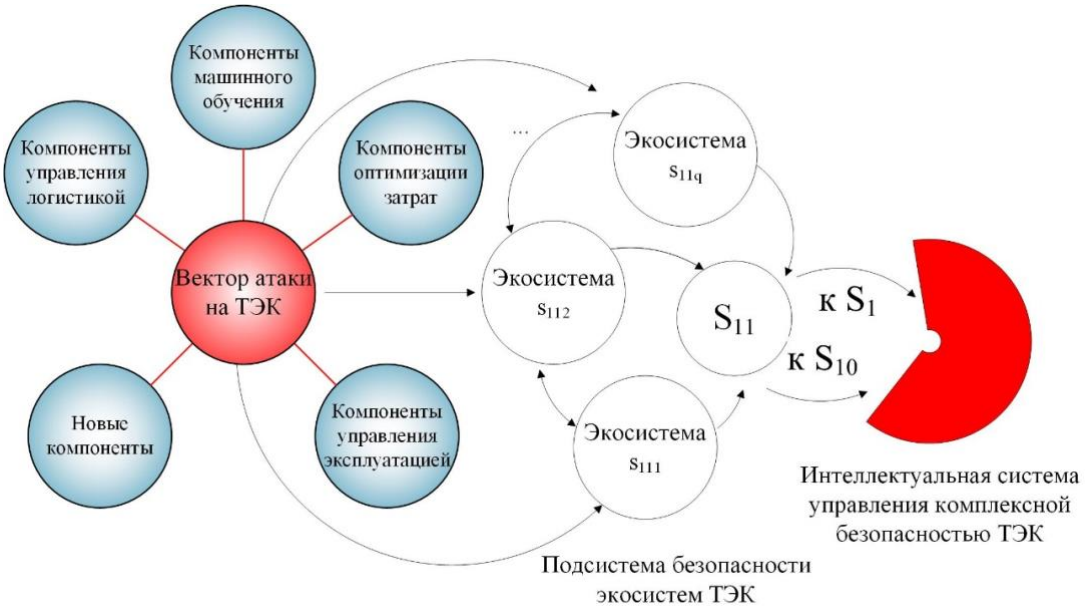


Рис. 2. Компоненты вектора атаки компьютерного червя с элементами искусственного интеллекта для объектов критической информационной инфраструктуры ТЭК

Актуальные способы защиты от потенциальных компьютерных червей с элементами искусственного интеллекта

Классические способы, включающие в себя все многообразие традиционных инструментов информационной безопасности и обеспечение участия человека в процессе принятия решений системами с элементами ИИ.

Специальные способы, включающие в себя [12]:

1. Управление событиями и информационная безопасность (SIEM): технологии, которые объединяют данные из различных источников, например, журналов событий и систем обнаружения вторжений, для обработки и анализа.

2. Пентестинг – это метод проверки безопасности системы или сети через проведение специальных тестов, имитирующих атаки, чтобы выявить слабые места и уязвимости. Внешний пентестинг – это проверка безопасности системы или сети извне. Включает в себя сканирование портов, поиск уязвимостей во внешних системах. Внутренний пентестинг – это проверка безопасности системы или сети изнутри. Включает в себя проверку уровня доступа пользователей, поиск уязвимостей во внутренних системах и приложениях, анализ защиты от вредоносного ПО. Пентестинг приложений – это проверка безопасности веб-приложений и программного обеспечения на наличие уязвимостей, таких как SQL-инъекции, межсайтового скриптинга или уязвимостей аутентификации.

Специализированные способы, включающие в себя:

1. Ханитопы – специально созданные уязвимые системы, представляющие из себя цифровые двойники реальных систем, открытые для атак из сети. Ханитопы подключают к системам мониторинга с целью сбора данных об инструментах и исследования тактики нарушителей.

2. Инфраструктура распределённых ложных целей – специально созданные сетевые ловушки в инфраструктуре реального предприятия с целью отвлечь внимание нарушителя от критически важной инфраструктуры на себя.

Выводы

Отечественных инструментов позволяющие реализовать специализированных способы защиты от потенциальных компьютерных червей с элементами ИИ практически нет, фундаментальная проблема, как кажется автору, кроется в существенной сложности решения вопроса взаимовлияния отдельных подсистем и компонентов интеллектуальной системы управления комплексной безопасностью друг на друга. Такое взаимовлияние связано с взаимным отображением моделей отдельных подсистем и компонентов друг на друга. Один из возможных способов учета этого влияния связан с понятиями гибридная угроза, комплексная угроза, системная угроза.

Литература

1. Korneev N. V. Intelligent complex security management system FEC for the industry 5.0. В сборнике: IOP Conference Series: Materials Science and Engineering. Сер. "Advanced Problems of Electrotechnology" 2020. С. 012016.

2. Корнеев Н.В. Российская индустрия искусственного интеллекта в решении актуальных проблем информационной безопасности. В сборнике: Безопасные информационные технологии. Сборник трудов Двенадцатой международной научно-технической конференции. 2021. С. 89-92.

3. 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.

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

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. Stav Cohen, Ron Bitton, Ben Nassi Here Comes The AI Worm: Unleashing Zero-click Worms that Target GenAI-Powered Applications. Published in arXiv.org 5 March 2024. DOI:10.48550/arXiv.2403.02817.

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

Complex cyber attacks with computer worms with elements of artificial intelligence in connected ecosystems

Korneev N.V. [90]

The article proposes a structure of a new ecosystem security subsystem aimed at managing security from a new threat – computer worms with elements of artificial intelligence. An example of a computer worm with elements of artificial intelligence for a personalized attack on a victim via Telegram using generative artificial intelligence is considered. The attack directions of a computer worm with elements of artificial intelligence on the information infrastructure are formulated: via generative artificial intelligence, for the purpose of a personalized attack on the victim; with hostile self-configuring requests and embedding a hostile request into an image via a self-configuring neural network. The components of the attack vector of a computer worm with elements of artificial intelligence for critical information infrastructure objects are identified and current protection methods are formulated: classic, special (SIEM, pentesting), specialized (honeytops, distributed deception platform).

Keywords: artificial intelligence, personalized attack, generative artificial intelligence, hostile self-configuring requests, attack vector components, SIEM, pentesting, honeytops, distributed deception platform

[90] 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 повышении пропускной способности компьютерной сети на основе рационального учета различных требований к своевременности обработки заявок

Костогрызов А.И.[91]

Интенсивные потоки заявок различной срочности в узлах компьютерной сети приводят к естественным задержкам в обработке заявок. Недопустимые задержки ведут к снижению количества своевременно обработанных заявок, т.е. практически к снижению пропускной способности сети. Предложен динамический метод рационального управления диспетчеризацией заявок различной срочности. Под диспетчеризацией понимается алгоритм выбора заявок из очереди для соответствующей обработки. Сформулирована постановка задачи оптимизации процесса диспетчеризации, использующая дополнительные возможности учета различных требований к своевременности обработки заявок. Применение метода позволяет рационально комбинировать существующие технологии и их настраиваемые параметры. Это при прочих одинаковых условиях на практике способствует повышению пропускной способности компьютерной сети.

Ключевые слова: диспетчеризация, критерий, модель, обработка заявок, очередь, сеть.

1. Введение

Для компьютерных сетей организации обработка разнородных потоков заявок различной срочности обычно задействует общие вычислительные ресурсы. В качестве заявок (запросов на обслуживание) на отдельный узел сети могут выступать заявки на ввод обновляемой информации в базу данных, поиск или получение запрашиваемых данных, выполнение операций, связанных с обеспечением информационной безопасности, решение каких-либо функциональных задач, заявки на прием-выдачу сигналов, пересылку сообщений или выполнение каких-либо промежуточных транзакций, словом, любые заявки, требующие для своей обработки какие-либо общие компьютерные ресурсы в течение определенного времени. При возрастании интенсивности потоков заявок в узлах сети возникают естественные задержки, приводящие к снижению пропускной способности компьютерной сети в целом. В работе пропускная способность сети измеряется количеством своевременно обработанных в сети заявок. Как следствие несвоевременность обработки заявок различной срочности может приводить к упущенной выгоде, потерям или ущербам для пользователей сети. С точки зрения бизнеса и обеспечения безопасности снижение пропускной способности сети критично для компьютерных систем, функционирующих в опасном производстве (например, в интересах топливно-энергетического и нефтегазового комплексов, объектов и систем химического производства), для систем реагирования на чрезвычайные ситуации, различных транспортных систем, иных систем критической информационной инфраструктуры. Сегодня в общем случае на практике в определении последовательности обработки заявок отсутствует какая-либо целенаправленная аналитическая увязка с частотой возникновения заявок различной срочности и возможностями технологий их обработки, с упускаемой выгодой, потерями или ущербами, которые могут последовать из-за нарушения требований к своевременности обработки заявок. В работе сформулирована постановка задачи

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

оптимизации процесса диспетчеризации, учитывающая дополнительные возможности в результате учета различных требований к своевременности обработки заявок [1-12].

2. Критерии своевременности обработки заявок

В общем случае требования к своевременности обработки заявок в системах определяются формально с помощью следующих критериев (например, по ГОСТ Р 59341).

Определение критерия 1 (оценка по среднему времени обработки). Обработка заявок i–го типа считается выполненной в срок, если среднее время их обработки с учетом задержек не превышает заданного $T_{зад.i}$, т.е. если $T_{полн.i} \leq T_{зад.i}$.

Определение критерия 2 (оценка по вероятности своевременной обработки). Обработка заявок i–го типа считается выполненной в срок, если вероятность своевременной обработки за время $T_{зад..i}$ не ниже заданной вероятности $P_{зад.i}$, т.е. $P_{св.i}=P(t_{полн.i} \leq T_{зад..i}) \geq P_{зад.i}$, где случайная величина $t_{полн.i}$ характеризует полное время обработки заявок i–го типа с учетом задержек. Критерий 2 задает более жесткие временные рамки (как правило $P_{зад.i} \geq 0.8$) и используется для компьютерных систем жесткого реального времени.

3. Анализ свойств технологий диспетчеризации для извлечения эффекта

В общем случае при прочих одинаковых условиях пропускная способность сети определяется суммой пропускных способностей всех узлов сети. С точки зрения пропускной способности функционирование отдельного узла может быть формализовано как функционирование однолинейной системы массового обслуживания потока заявок на обработку в узле. При возрастании потока заявок могут возникать очереди. Формальный порядок выбора из очереди следующей заявки для обработки определяется с использованием технологии диспетчеризации заявок.

Рассмотрим выявленные свойства 5 типовых технологий диспетчеризации [1-12], которые с точки зрения обеспечения повышения пропускной способности сети должны учитываться при выборе очередности в обработке заявок – см. рис. 1.

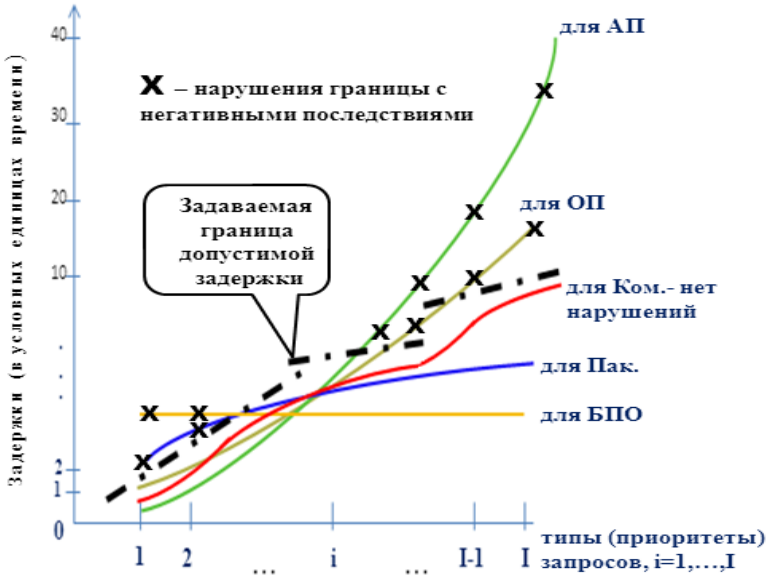


Рис. 1 Свойства технологий диспетчеризации проявляются в задержках, если задержки выходят за формально установленные границы, возникают упущенная выгода, потери или ущербы

Технология 1 заключается в бесприоритетном обслуживании заявок (БПО) в порядке «первый пришел — первый обслужился». Ее главное свойство в том, что средние задержки до начала обработки по всем разнородным заявкам - одинаковы. При использовании одного приоритета (т.е. когда приоритет формально не действует) эта технология 1 является частным случаем технологий 2-5.

Технология 2 заключается в обслуживании заявок с относительными приоритетами (ОП). Заявки более высокого приоритета имеют преимущество перед заявками низшего приоритета, а именно: среди заявок, ожидающих начала обработки, заявки более высокого приоритета обрабатываются впереди заявок низшего приоритета. Из заявок одного приоритета следующим выбирается на обработку заявка, которая поступила раньше (т.е. в порядке «первый пришел — первый обслужился»). Если во время обработки некоторой заявки поступает заявка более высокого приоритета, то прерывания не происходит. Это означает, что начатая в узле обработка всегда доводится до своего завершения, несмотря на поступление более приоритетных заявок. Главное свойство технологии 2 в том, что средние задержки до начала обработки по заявкам низшего приоритета в 3-5 раз выше (при высокой загрузке может быть на порядок выше), чем задержки заявок высшего приоритета.

Технология 3 заключается в обслуживании заявок с абсолютными приоритетами (АП). В отличии от технологии 2 поступающие заявки более высокого приоритета абсолютно прерывают обработку заявки с низким приоритетом. Прерванная заявка дообслуживается с прерванного места. Это означает что при поступлении заявки более высокого приоритета в узле сети прерывается начатая обработка и начинается обработка этой более приоритетной заявки. А завершение начатой обрабатываться, но прерванной заявки осуществляется сразу после выполнения обработки всех поступивших заявок более высоких приоритетов. Главное свойство технологии 3 в том, что средние задержки до начала обработки заявок низшего приоритета в 10-20 раз выше (при высокой загрузке узла может быть и более), чем задержки заявок высшего приоритета.

Технология 4 заключается в пакетном обслуживании заявок с естественным формированием пакетов и относительными приоритетами внутри пакета (Пак.). Первая поступившая заявка при отсутствии очереди образует первый пакет на обработку. Очередной пакет формируется из заявок, поступивших за время обработки заявок предыдущего пакета, а если таковых нет, то из следующей же поступившей заявки. Очередной пакет заявок начинает обслуживаться сразу же после обработки всех заявок предыдущего пакета. В пакете, поступившем на обслуживание, выбираются заявки наивысшего приоритета и обслуживаются последовательно в порядке «первый пришел — первый обслужился». Обработка по всем заявкам, вошедшим в обслуживаемый пакет, осуществляется без прерываний независимо от других поступающих в систему заявок. Главное свойство технологии 4 заключается в следующем. Если для технологий 2 и 3 заявки высшего приоритета имеют подавляющее преимущество (проявляемое в в десятки раз более коротких задержках на обработке), то для технологии 4 это преимущество резко сокращается. В итоге средние задержки заявок низшего приоритета заметно уменьшаются и превышают задержки заявок высшего приоритета не более, чем в 3 раза. Это замечательное свойство доказано в [3, 7] и может быть эффективно использовано в технологии 5, позволяющей путем настройки параметров комбинировать технологиями 2, 3 и 4.

Технология 5 (Ком.), определяющая предлагаемый метод диспетчеризации заявок различной срочности, является комбинацией технологий 2, 3, 4. Технология 5 обобщает варианты обслуживания заявок, описанные в технологиях 2–4. Все поступающие заявки разбиваются на n групп (см. рис. 2). Заявки e-й группы имеют более высокий приоритет над заявками g-й группы при $e<g$ ($e, g=1, n$) Внутри каждой группы приоритеты заявок относительные. Система обладает возможностью обслуживания заявок в соответствии с технологиями 2, 3 и 4. Для обработки заявок g-й группы назначается какая-либо одна из технологий (2 или 4). Между заявками e-й и g-й групп назначаются либо относительные (по технологии 2), либо абсолютные приоритеты (по технологии 3).

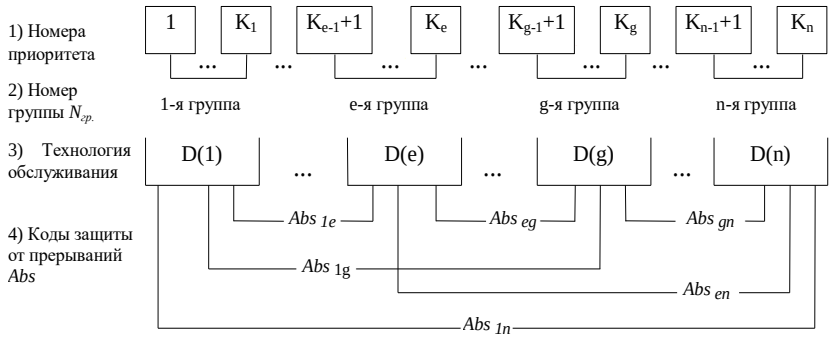


Рис. 2 Структура комбинированной обработки запросов

Предлагаемый динамический метод диспетчеризации заключается в периодической настройке параметров (таких, как разбиение типов заявок по группам, назначение технологий и приоритетов внутри групп) при использовании Технологии 5. Эта Технология 5 способна в различной степени обладать свойствами технологий 2, 3, 4 (вплоть до полного превращения в них) [8-12].

Таким образом, возможный эффект от предложенного метода диспетчеризации состоит в системном использовании резервов в задаваемых ограничениях на обработку заявок различной срочности с тем, чтобы уменьшить суммарную упущенную выгоду, потери или ущербы за счет рационального манипулирования задержками, позволяющим увеличить суммарное количество своевременно обрабатываемых в сети заявок. Метод эффективен при достаточно устойчивых потоках заявок различной срочности и в тех узлах сети, где в обработке этих заявок возникают очереди.

Примечание. Для систем, в которых возникающие задержки в очередях несущественны, от внедрения предлагаемого метода большого практического эффекта ожидать не следует.

4. О показателях и вероятностных моделях для оценки возможных задержек

Без ограничения общности в целях рациональной настройки параметров в конкретном узле сети процессы обработки потоков заявок различной срочности в этом узле формализованы как процессы массового обслуживания пуассоновских потоков заявок в однолинейной системе с ожиданием ($M/G/1/\infty$).

Разносрочность заявок проявляется в различных допустимых сроках их обработки с учетом вынужденных задержек. Предположение о пуассоновости потоков заявок на обработку в узле обосновано тем, что суммарный поток заявок представляет собой, как правило, сумму большого числа потоков от различных источников. Интенсивность каждого из слагаемых потоков мала по сравнению с интенсивностью суммарного потока – в такой ситуации действует предельная теорема А.Я. Хинчина - В. Григолиониса [15, 16], согласно которой суммарный поток будет обладать свойствами пуассоновского потока. Предположение о бесконечности числа мест для ожидания означает на практике возможность приема в узле всех поступающих заявок.

Для расчетов по критерию 1 используется показатель $T_{полн.i}$ – это 1-й моменты полного времени обслуживания заявок i-го типа с учетом задержек (i=1,…,I). Для расчетов по критерию 2 предлагается использовать показатель вероятности своевременной обработки заявок i-го типа за заданное время $P_{св.i}\ (T_{зад.i})$, аппроксимируемой с помощью неполной гамма-функции – см. ГОСТ Р 59341. В этом случае помимо задаваемых ограничений на допустимое время обработки вычисляются показатели $T_{полн.i}$ и $T_{полн.i2}$ – это соответственно 1-й и 2-й моменты полного времени обслуживания заявок i-го типа с учетом задержек. Для расчетов этих показателей ($T_{полн.i}$ и $T_{полн.i2}$) применительно к технологиям 1, 2 и 3 предлагается использовать классические результаты теории массового обслуживания

[1, 2, 4, 5]. Для технологии 4 и 5 применимы формулы, полученные ранее в работах [6-14]. При этом в качестве исходных данных достаточно знать частоты поступления заявок i-го типа (λ_i) и средние времена обработки заявок.

5. О постановке задачи оптимизации и ее решении

Предлагается следующая постановка задачи оптимизации последовательности обработки заявок различной срочности в сети.

Последовательность обработки заявок устанавливается в соответствии с той технологией (из состава технологий 1-5) и с теми параметрами, на которых достигается минимум упущенной выгоды, потерь или ущербов (суммарный ожидаемый ущерб) при ограничениях на своевременность обработки заявок по критериям 1 или 2.

$$\{\sum_{i=1}^{I} \lambda i\ [1 - \text{Рсв. i (Тзад. i)}]\ \text{Ui}\ [\text{Ind}(\alpha_1)+\text{Ind}(\alpha_2)]\}/\lambda \ \rightarrow \ \min ,$$

где λi – частота поступления заявок i-го типа, $\lambda = \sum_{i=1}^{I} \lambda i$;

Ui – ожидаемый размер упущенной выгоды, потерь или ущербов в результате нарушения сроков выполнения работ по заявкам i-го типа;

Ind(α1)=1, если используется критерий 1, иначе Ind(α1)=0;

Ind(α2)=1, если используется критерий 2, иначе Ind(α2)=0.

При формировании исходных данных на практике для расчетов частота поступления заявок i-го типа может пересчитываться за определенный прошедший период времени как отношение количества заявок к длительности взятого периода.

Настройка параметров при оптимизации может быть осуществлена путем перебора всех возможных технологий диспетчирования и вариантов настраиваемых параметров (таких, как разбиение типов заявок по группам, назначение технологий и приоритетов внутри групп). Наиболее рациональными параметрами признаются те, для которых суммарный ожидаемый ущерб (упущенная выгода и/или потери) для пользователей сети минимален. По результатам моделирования для случая, когда расчетным временем определения рациональных параметров для узла сети можно пренебречь, за счет использования предложенного динамического метода диспетчеризации с Технологией 5 количество своевременно обработанных заявок возможно увеличить в разы по сравнению с Технологией 1 и на десятки процентов по сравнению с Технологиями 2, 3, 4. Эти цифры характеризуют возможности по повышению пропускной способности не только одного узла, но и компьютерной сети в целом.

Заключение

Предложен динамический метод рациональной диспетчеризации заявок различной срочности, позволяющий повысить количество своевременно обрабатываемых в узлах сети заявок. Поставлена задача оптимизации последовательности обработки заявок различной срочности путем настройки параметров (таких, как разбиение типов заявок по группам, назначение технологий и приоритетов внутри групп). Решение задачи в процессе функционирования сети направленно на минимизацию упущенной выгоды, потерь или ущербов при ограничениях на своевременность обработки заявок. Охватывая в общем случае компьютерные сети любой области приложения, предложенные динамический метод рациональной диспетчеризации заявок различной срочности и задача оптимизации, связанная с его применением, обладают аналитической новизной. Их применение в сети предоставляет практические возможности для повышения пропускной способности компьютерной сети и уменьшения из-за существующих задержек суммарного ожидаемого ущерба (упущенной выгоды и/или потерь).

Литература

1. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. М.: Наука. 1987.

2. Матвеев В.Ф., Ушаков В.Г. Системы массового обслуживания. М.: МГУ, 1984.

3. Костогрызов А.И., Назаров Л.В. Пакетная обработка требований в системе с относительным приоритетом// Изв. АН СССР сер. Техническая кибернетика. 1981, №3, С.183-187.

4. Балыбердин В.А. Методы анализа мультипрограммных систем. – М. Радио и связь, 1982. – 152с.

5. Балыбердин В.А. Оценка и оптимизация характеристик систем обработки данных. – М.: Радио и связь, 1987. – 176с.

6. Костогрызов А.И., Матвеев В.Ф. Анализ применения комбинированной дисциплины обслуживания в системах реального времени // Изв. АН СССР сер. Техническая кибернетика. 1986, №6, С.79-84.

7. Костогрызов А.И. Пакетная обработка заявок в режиме равномерного разделения процессора с прерыванием // Изв. АН СССР сер. Техническая кибернетика. 1987, №4, С.88-93.

8. Костогрызов А.И. Класс приоритетных дисциплин с комбинированием принципов обслуживания в порядке приоритета и пакетной обработки заявок. Анализ их свойств и возможностей применения в АСУ// Анализ стохастических систем методами исследования операций и теории надежности. К.: Ин-т кибернетики им. В.М.Глушкова АН УССР, 1987. С.52-55.

9. Kostogryzov A., Atakishchev O., Nistratov A., Nistratov G., Klimov S., Grigoriev L. The method of rational dispatching a sequence of heterogeneous repair works // Energetica. 2017. Vol.63, No 4 , P. 154-162

10. Безкоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. М.: Изд. «Вооружение. Политика. Конверсия», 2002.- 304 с.

11. 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.

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

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

14. Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. - London: IntechOpen, 2018. - 278 p.

15. Хинчин А.Я. Работы по математической теории массового обслуживания. -М.: изд-во Физ.-мат.лит., 1963.

16. Григолионис В. О сходимости сумм ступенчатых процессов к пуассоновскому// Теория вероятности и ее применения. Т.8, 1963, № 2.

On increasing the capacity of a computer network based on rational consideration of various requirements for the timely requests processing

Kostogryzov Andrey[92]

Intensive flows of requests of varying urgency in computer network nodes lead to natural delays in requests processing. Unacceptable delays lead to a decrease in the number of requests processed in a timely manner, i.e., practically to a decrease in network capacity. A dynamic method of rational control of dispatching requests with various urgency is proposed. Dispatching refers to the algorithm for selecting requests from the queue for appropriate processing. The formulation of optimizing task to dispatching process is formulated, using the additional possibilities of taking into account various requirements for requests timely processing. The application of the method makes it possible to rationally combine existing technologies and their configurable parameters. This, all other things being the same, in practice helps to increase the capacity of a computer network.

Keywords: dispatching, criterion, model, application processing, queue, network.

[92] 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

Банк данных атомарных действий по реагированию на компьютерные инциденты

Кузнецов А.В.[93]

Разработан банк данных атомарных действий по реагированию на компьютерные инциденты, который в отличие от известных учитывают возможность полной автоматизации отдельно взятого действия и сбор плана реагирования для соответствующего типа (категории) инцидента, что позволяет максимально автоматизировать план реагирования и в будущем применять план реагирования в полностью автоматическом (автономном) режиме, т. е. сократить непосредственное вовлечение представителей группы реагирования (оптимизировать состав группы). Результаты наиболее значимы для владельцев (операторов) распределённых информационных инфраструктур федерального масштаба и центров мониторинга информационной безопасности, в т. ч. центров ГосСОПКА. Проводится процедура государственной регистрации базы данных. Применение результатов настоящего исследования дает положительный эффект в области технических наук (методы и системы защиты информации, информационная безопасность).

Ключевые слова: группа реагирования, средство реагирования, план реагирования, автоматизированное реагирование, автоматическое реагирование

Введение

В настоящее время, к сожалению, нет возможности создавать комплексные системы обеспечения информационной безопасности (ИБ) с применением только превентивных мер обеспечения ИБ, а также недостаточно реализовывать мероприятия только по мониторингу (обнаружению) инцидентов ИБ без последующего реагирования на них [1, 2]. Это подтверждается непрерывным ростом количества инцидентов ИБ [3-6], в т. ч. в кредитно-финансовой сфере [7-9], несмотря на все применяемые превентивные защитные меры.

Здесь же стоит отметит, что человеческих ресурсов всегда недостаточно, а с учётом того, что в процесс реагирования вовлечены не только специалисты по защите информации, на заинтересованность и экспертизу которых ИБ-подразделение не может воздействовать, деятельность групп реагирования подлежит максимальной автоматизации [10] и, в будущем, переходу в полностью автоматический (автономный) режим реагирования [11].

Создание условий для автоматизации реагирования

Деятельность группы реагирования может быть рассмотрена как множество отдельных действий – *A*, т. е. неделимой активности, выполняемой одной командой в командной строке или один выбором в графическом интерфейсе средства реагирования (далее – атомарные действия).

Данные действия комбинируются в зависимости от типа (категории) и критичности инцидента, оперируют контекстными характеристиками инцидента – *C*, и формируют необходимый план реагирования (playbook) – *P*.

Например:

A = {включить, выключить, разблокировать, заблокировать, импортировать, экспортировать, возобновить, приостановить, перевести в другой режим}

C = {имя учётной записи, IP-адрес хоста, FQDN-хоста, MAC-адрес сетевого интерфейса, URL-адрес, номер платежного документа}

Постановка задачи: формирование банка данных атомарных действий по реагированию на компьютерные инциденты, каждое из которых может быть полностью

[93] Кузнецов Александр Васильевич, кандидат технических наук, Финансовый университет при Правительстве Российской Федерации, кафедра информационной безопасности, г. Москва, 1283_my@mail.ru

автоматизировано с использованием соответствующего средства реагирования, для сокращения личного вовлечения представителей группы реагирования.

Для сборки плана реагирования и его последующей полной или частичной автоматизации с использованием соответствующих средств [12, 13], атомарные действия снабжаются следующими атрибутами [14]:

- идентификатор (id);
- входные данные (input);
- выходные данные (output);
- описание действия с учётом контекстной характеристики инцидента (например: заблокировать IP-адрес *1.2.3.4*, заблокировать учётную запись *username*, приостановить платёж *номер* и т. п.).

После указания атрибутов потребуется задание фиксированных условий для активации каждого из атомарных действий, т. е. продвижения по плану реагирования.

В рамках настоящего исследования:

- не проводится деление между понятиями «инцидента информационной безопасности» и «компьютерного инцидента», эти понятия рассматриваются как синонимы;
- рассматриваются мероприятия, относящиеся к этапу непосредственного реагирования, т. е. сдерживания (локализации), устранения и восстановления информационной инфраструктуры, т. к. именно здесь возникает активное противодействие атакующему (нарушителю безопасности информации).

Банк данных атомарных действий

Банк данных рассматривается как автоматизированная информационно-поисковая система, состоящая из одной базы данных атомарных действий и системы хранения, обработки и поиска информации в ней (в терминах ГОСТ 7.73-96[94]).

В реализации используется система управления базами данных Postgres Pro Enterprise (сертификат ФСТЭК России № 4063, срок действия – 16.01.2029 г.) для обработки и поиска информации. Требования к эффективному объёму системы хранения данных: от 10 Гбайт, требования к физическому объёму могут быть определены с использованием соответствующей методики [15].

В состав базы данных входят следующие таблицы:

- автоматизируемые действия;
- варианты запуска автоматизируемых действий;
- коннекторы к средствам реагирования;
- поля входных и выходных данных (в т.ч. поля с типами «каталог» и «массив»);
- права логического доступа, необходимые для выполнения действий с использованием соответствующего средств реагирования;
- переменные, используемые для автоматизации (несколько таблиц).

База данных не содержит персональные данные или иную информацию ограниченного доступа.

Пример отработки запроса к базе данных:

```
SELECT FROM public.catalogs fetch first 2 rows only id,name,values
1,Действие,"['Выполнить', 'Пропустить', 'Согласовано', 'Не требуется']"
2,ДаНет,"['Да', 'Нет']"
```

Планируется дополнительно собрать статистику применения тех или иных атомарных действий для последующего машинного обучения и применения искусственного

[94] ГОСТ 7.73-96 «Система стандартов по информации, библиотечному и издательскому делу. Поиск и распространение информации. Термины и определения».

интеллекта [16]. При этом необходимо будет учитывать актуальное нормативно-правовое регулирование искусственного интеллекта применительно к области обеспечения ИБ [17].

Выводы

По результатам проведенного исследования разработан банк данных атомарных действий по реагированию на компьютерные инциденты, который в отличие от известных учитывают возможность полной автоматизации отдельно взятого действия и сбор плана реагирования для соответствующего типа (категории) инцидента, что позволяет максимально автоматизировать план реагирования и в будущем применять план реагирования в полностью автоматическом (автономном) режиме, т. е. сократить непосредственное вовлечение представителей группы реагирования (оптимизировать состав группы).

Применение результатов настоящего исследования дает положительный эффект в области технических наук (методы и системы защиты информации, ИБ) и наиболее значимо для владельцев (операторов) распределённых информационных инфраструктур федерального масштаба, включающих в свой состав средства реагирования, а также для центров мониторинга информационной безопасности (Security Operations Center, SOC), в т. ч. центров ГосСОПКА [18, 19].

Предложенный банк данных был апробирован автором в рамках выполнения проектных работ в 2024 г. на базе крупнейшего в России коммерческого центра мониторинга ИБ – «Ростелеком-Солар JSOC», в настоящее время проводится процедура государственной регистрации базы данных.

Литература

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

2. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении. - Иннополис: Издательский Дом «Афина», 2017. 440 с.

3. Бутусов И.В., Романов А.А. Предупреждение инцидентов информационной безопасности в автоматизированных информационных системах // Вопросы кибербезопасности. 2020. № 5 (39). С. 45-51.

4. Майорова Е.В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики // Петербургский экономический журнал. 2020. № 1. С. 155-162.

5. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей / Букин А.В., Самонов А.В., Тихонов Э.И. // Вопросы кибербезопасности. 2022. № 5 (51). С. 61-73.

6. Яковишин А.Д. Способы оптимизации процессов реагирования на инциденты ИБ // Вестник науки. 2024. Т. 2. № 2 (71). С. 498-504.

7. Алексеева Н.В., Дуракова А.С., Горденко Д.В., Воропинова О.А. Киберпреступления в банковской сфере России: аналитика и методы противодействия // Вестник Института дружбы народов Кавказа (Теория экономики и управления народным хозяйством). Экономические науки. 2023. № 1 (65). С. 54-64.

8. Зайнулабидов М.Х., Исаев О.В., Толстых О.В. Киберпреступления в кредитно-финансовой сфере // Закон и право. 2024. № 8. С. 68-73.

9. Козьминых С.И. Методический подход к экономической оценке внедрения технических средств защиты информации в кредитно-финансовой организации // Вопросы кибербезопасности. 2020. № 3 (37). С. 87-96.

10. Слинкин Н.А. Разработка и внедрение систем раннего обнаружения и реагирования на киберугрозы УПСВ // Вестник науки. 2024. Т. 4. № 5 (74). С. 1538-1544.

11. Махлин Б.М. Единая система управления безопасностью компании как современное средство обеспечения информационной безопасности // Научный формат. 2019. № 2 (2). С. 59-62.

12. Селезнёв В.М., Боровская О.Е. Встраивание инструментов SOAR-платформ в экосистему SOC для автоматизации процесса реагирования на инциденты ИБ // Международный научно-исследовательский журнал. 2022. № 10 (124). С. 1-9.

13. Очередько А.Р., Бачманов Д.А., Путято М.М., Макарян А.С. Исследование IRP-систем на основе анализа механизмов реагирования на инциденты информационной безопасности // Прикаспийский журнал: управление и высокие технологии. 2021. № 1 (53). С. 74-82.

14. Karlzen H., Sommestad T. Automatic incident response solutions: a review of proposed solutions' input and output. Automatic incident response solutions: a review of proposed solutions' input and output // In The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29-September 01, 2023, Benevento, Italy. ACM, New York, NY, USA, 11 Pages. DOI: https://doi.org/10.1145/3600160.3605066.

15. Кузнецов А.В. Организация раздельного хранения данных о событиях // Вопросы кибербезопасности. 2024. N 2 (60). С. 22-28. DOI: 10.21681/2311-3456-2024-2-22-28.

16. Abhilash R.P.R., Anjan K.R.A. Automating incident response: AI-driven approaches to cloud security incident management // Chelonian Conservation And Biology. 2020. Vol. 15 No. 2. DOI: doi.org/10.18011/2020.04(1).73.79.

17. Кузнецов А.В. Некоторые вопросы применения искусственного интеллекта в разрезе обеспечения информационной безопасности Российской Федерации // Защита информации. Инсайд. 2024. № 3 (117). С. 4-9.

18. Шабля В.О., Орлов Е.О., Галямин Н.А. Анализ процесса функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атака на автоматизированные системы // Наука и реальность. 2024. № 2 (18). С. 71-78.

19. Марков А.С. Технические решения по реализации подсистем ГОССОПКА. // Сборник научных трудов V Международной научно-практической конференции «Управление информационной безопасностью в современном обществе». М.: ВШЭ, 2017. С. 85-96.

The data bank of atomic computer incident response actions

Kuznetsov A.V.[95]

The data bank of atomic computer incident response actions is developed, which unlike the known ones take into account the possibility of complete automation of an atomic action and compilation a response plan for the appropriate type (category) of incident, which allows to automate the response plan as much as possible and, in the future, to apply the response plan in a fully automatic (autonomous) mode, i.e. reduce the direct involvement of response team representatives (optimize the composition of the team). It contributes for owners (operators) of distributed information infrastructures on a federal scale and Security Operations Centers (SOC), including GosSOPKA centers. The state registration procedure of database in progress. The application of this study results has a positive effect in the field of technical sciences (methods and systems of information protection, information security).

Keywords: response team, response tool, response plan, automated response, automatic response

[95] Aleksandr V. Kuznetsov, Ph.D. (in Tech.), CISM, CISSP, Financial University under the Government of the Russian Federation, Moscow, 1283_my@mail.ru

УДК 004.056

Сравнение подходов к обнаружению вторжений с применением нейросетей для анализа сетевого трафика

Маковейчук Я.Т. [96]

Аннотация. В статье выполнено сравнение подходов, основанных на глубоком обучении, к построению систем обнаружения вторжений по аномалиям в сетевом трафике (Интернет), в том числе в системах Интернета вещей, различных исследователей, как зарубежных, так и российских. Сделана систематизация используемых подходов. Выделены достоинства и недостатки. Определены перспективы и направления совершенствования методов построения систем обнаружения и предупреждения вторжений на основе применения нейросетей. Сделан акцент на важности работы с входными данными для моделей, улучшении методов создания наборов входных данных, в том числе синтетических, применении методов интерпретации результатов работы моделей, адаптации исследований по построению моделей к особенностям IoT.

Ключевые слова: модель, система обнаружения вторжений, защита, нейросеть, гибридная модель, трафик, аномалия, глубокое обучение, интерпретируемость, IoT.

Введение. Системы обнаружения вторжений (Intrusion Detection System, IDS) являются важной составной частью сетевых систем защиты, обеспечивающей безопасность информационной системы в условиях возрастающего с каждым годом количества попыток несанкционированного доступа и различных типов атак. Традиционный подход, используемый в IDS, подразумевает обнаружение вторжений на основе сигнатур, которое не предусматривает выявление новых моделей атак [1, 2]. Методы машинного обучения (ML), особенно глубокого обучения (DL), стали многообещающей альтернативой этому подходу благодаря их способности выявлять сложные и неявные закономерности в данных сетевого трафика. Однако, построение оптимальной модели для выявления аномалий в сетевом трафике является на сегодня задачей с множеством подходов и вариантов решений, и первым этапом построения интеллектуальной системы обнаружения вторжений должен стать этап анализа этих подходов и решений, выявление их плюсов и возможных минусов, как в качестве обнаружения, так и в сложности / ресурсозатратности построения. В данной работе выполнена попытка систематизации таких подходов и решений, на основе анализа опыта построения систем обнаружения вторжений по аномалиям в сетевом трафике (Интернет), в том числе в системах Интернета вещей, представленного в зарубежных и отечественных научных исследованиях.

Цель: исследовать подходы к обнаружению вторжений с применением нейросетей для анализа сетевого трафика.

Основная часть. Анализ исследований, с учетом интенсивного развития ML/DL и методик его применения в различных сферах, скорости появления новых улучшенных моделей, был выполнен за небольшой период – 5 лет, с 2020 по 2024 год. Можно отметить, что все исследования в сфере применения ML/DL для повышения безопасности IDS направлены в первую очередь на повышение эффективности выявления вторжений. Большинство проанализированных работ описывают разработку гибридных моделей, использующих комбинацию нейронных сетей и методов фильтрации признаков, а также глубокого обучения (DNN, CNN, RNN, LSTM и их комбинаций). Ученые исследуют способы применения методов глубокого обучения для повышения точности обнаружения вторжений и минимизации ложных срабатываний.

[96] Маковейчук Ян Тарасович, аспирант, Финансовый университет при Правительстве Российской Федерации, г. Москва, makoweychuk.yan@yandex.ru

На основании сравнения общих направлений в развитии ML/DL для обнаружения вторжений были выделены следующие достоинства и недостатки проанализированных подходов (см. таблицу 1).

Таблица 1

Анализ зарубежных научных исследований в области применения ML/DL для IDS

Исследование	**Техника/ Метод**	**Используемый набор данных**	**Достоинства**	**Недостатки**	**Описание и результаты**
Yuan et al. [3]	DLL-IDS система	NSL-KDD	Высокая точность (до 90%) в сложных сценариях атак благодаря использованию глубокого обучения и состязательных примеров.	Возможная сложность реализации и высокая вычислительная нагрузка.	Предложена структура DLL-IDS, включающая DL-IDS, AE на основе LID и ML-IDS. DLL-IDS показала значительно более высокую точность по сравнению с традиционными IDS.
Wang et al. [4]	Модели глубокого обучения DNN, CNN, RNN, LSTM, CNN+RNN, CNN+LSTM	CSE-CIC-IDS2018	Высокая точность многоклассовой классификации (более 98%), применение современных моделей DL.	Комбинированные модели демонстрируют более длительное время вывода.	Оценка различных моделей DL для обнаружения сетевых атак. Точность превышает 98% для многоклассовой классификации.
Awajan [5]	IDS на основе глубокого обучения (DL-based IDS)	Набор данных с 25000 экземплярами	Надежная работа при обнаружении различных типов атак в IoT, средняя точность 93,74%.	Независимость от протокола связи усложняет настройку и развертывание.	Разработана система IDS для IoT, достигающая средней точности 93,74% при обнаружении атак, включая DDoS и Blackhole.
Khan et al. [6]	Гибридные алгоритмы глубокого обучения (RNN, GRU)	ToN-IoT	Высокая точность (до 99%) для сетевых потоков и прикладного уровня, превосходство над предыдущими моделями IDS.	Требует оптимизации производительности, например, использование Adam оптимизатора.	Предложена интеллектуальная IDS для IoT с использованием гибридных алгоритмов DL. Достигнута точность 99% для сетевых потоков и 98% для прикладного уровня.
Sharma et al. [7]	Аномалистическая IDS на основе DNN	UNSW-NB15	Эффективность при работе с дисбалансом классов, точность до 91% после применения GAN для создания синтетических данных.	Первоначальная точность без обработки дисбаланса составила всего 84%.	Разработана IDS для IoT с применением DNN и GAN для устранения дисбаланса данных. Точность модели достигла 91%.
Ravi et al. [8]	IDS на основе глубокого обучения	IoMT набор данных	Высокая точность для сетевых и комбинированных данных, применение уровня глобального внимания для улучшения характеристик.	Возможные сложности в интеграции биометрических данных и их обработке.	Предложена модель для IoMT с использованием сетевых и биометрических данных, достигнута точность 99% для комбинированных данных.

Исследование	Техника/ Метод	Используемый набор данных	Достоинства	Недостатки	Описание и результаты
Bowen et al. [9]	BLoCNet (CNN + BLSTM)	CIC-IDS2017, IoT-23, UNSW-NB15	Высокая эффективность обнаружения атак по сравнению с другими моделями DL, использование двух мощных архитектур (CNN и BLSTM).	Более сложная структура модели требует значительных вычислительных ресурсов.	Разработана гибридная модель BLoCNet для IDS, показавшая превосходство над другими DL моделями по точности обнаружения атак.
Gupta et al. [10]	Гибридный подход с нейронными сетями и выбором признаков на основе корреляции	NSL-KDD	Высокая точность (98%) и точность, использование гибридного метода оптимизации.	Метод может быть чувствителен к изменениям в распределении данных, что требует дополнительных настроек.	Разработан гибридный метод на основе HCSAOANN, обеспечивающий точность 98% при обнаружении аномалий в сетевом трафике.
Kumar et al. [11]	Усиленная IDS с использованием алгоритма PCGSO	ISCXIDS2012	Высокая точность (99%), улучшенный выбор функций и настройка гиперпараметров.	Сложность реализации и необходимость в оптимизации гиперпараметров, время обработки.	Предложена система IDS с улучшением точности до 99% за счет использования PCGSO для выбора функций и настройки гиперпараметров.
Wang et al. [12]	DMCNN (глубокая многомасштабная CNN)	NSL-KDD	Высокая точность для обнаружения DOS атак (98%), эффективное использование пакетной нормализации.	Применение требует значительных вычислительных мощностей и может быть сложно в настройке.	Разработана модель DMCNN для обнаружения вторжений, которая показала высокую точность (98%) и низкий уровень ложных тревог в сетевом трафике.
Павленко Е.Ю. и др. [13]	Рекуррентная нейронная сеть с долгой кратковременной памятью (LSTM) для классификации киберугроз на адаптивных топологиях	Синтетический набор данных, моделирующий топологию сети в течение 15 000 тактов, включая штатные и аварийные адаптации	Высокая точность классификации киберугроз (87,2%), с улучшением по мере накопления данных. Учет предыдущих состояний узлов благодаря особенностям LSTM. Применимость к крупномасштабным системам с адаптивной топологией.	Точность в начале обработки данных ниже из-за недостаточного объема обучающих паттернов. Ограниченность синтетических данных - требуется тестирование на реальных.	Предложен подход на основе LSTM для обнаружения атак, включая единичные и каскадные отказы в обслуживании. Результаты показывают удовлетворительную точность классификации (87,2%) с перспективой улучшения при более длительном обучении.
Котенко И. В. [14]	LSTM в связке с автоэнкодером для выявления аномалий в сетевом трафике	Сгенерированный набор данных для проверки эффективности предложенного подхода	Высокая точность в обнаружении аномалий, особенно в реальном времени. Обход уязвимостей Web Application Firewall. Снижение погрешностей/	Зависимость точности от качества сгенерированных наборов данных. Сложность реализации и настройки LSTM и автоэнкодеров	Для обнаружения аномалий в сетевом трафике в качестве дополнения LSTM использован автоэнкодер. Эксперимент показал высокую эффективность подхода, выявление атак в РВ или близком к РВ.

Исследование	Техника/ Метод	Используемый набор данных	Достоинства	Недостатки	Описание и результаты
Большаков А. С. и др. [15]	Многослойная нейронная сеть прямого распространения с использованием корреляционной матрицы на основе коэффициентов Пирсона.	UNSW-NB15	Минимизация признаков за счет использования корреляционной матрицы Пирсона. Высокое качество предсказания. Простота реализации: многослойная нейронная сеть с сигмоидальной функцией передатчика.	Выбор 5 признаков может ограничить модель. Проблемы с обучением: эффективность модели зависит от качества и специфики данных.	Предложена нейронная сеть для обнаружения аномалий в сетевом трафике, использующая минимальное количество признаков. При использовании 5 признаков модель эффективно классифицирует аномалии.
Зегжда Д.П. и др. [16, 17]	LSTM интегрированная с honeypot-системой для изоляции и анализа подозрительного трафика.	Использование трафика, поступающего в сеть, с целью анализа аномалий	Два уровня защиты: первый уровень — IDS на базе LSTM для обнаружения аномалий, второй — использование honeypot для изоляции подозрительных действий.	Зависимость от обучающего набора данных. Ограничение по времени обработки.	Предложена двухуровневая защита локальной сети, включающая IDS на основе LSTM. При обнаружении аномалии система перенаправляет подозрительный трафик на honeypot.

Достоинства

1. Высокая точность обнаружения. Большинство современных подходов достигают точности выше 90%, а в некоторых случаях даже 98–99% для различных наборов данных.

Это связано с применением глубоких нейронных сетей (DNN), RNN, LSTM, CNN и их комбинаций, которые эффективно анализируют сложные паттерны в сетевом трафике.

2. Гибридные и многослойные архитектуры для глубокого анализа.

Комбинированные модели (например, CNN+RNN, CNN+LSTM, BI-GRU) обеспечивают более глубокий анализ временных и пространственных характеристик данных. Использование методов, таких как BLoCNet и DMCNN, позволяет интегрировать извлечение признаков и последовательное обучение для повышения эффективности.

3. Решение проблем дисбаланса классов.

Генеративно-состязательные сети (GAN) активно используются для синтеза данных атак, чья доля в трафике обычно невелика («меньшинств»), что улучшает сбалансированность данных и повышает точность классификации.

4. Оптимизация обработки данных.

Методы предварительной обработки (нормализация, стандартизация, выбор признаков) улучшают качество данных, а алгоритмы выбора признаков (например, PCGSO) позволяют сосредоточиться на наиболее значимых характеристиках.

5. Применение к IoT и специализированным системам.

Исследования адаптируются к особенностям IoT, учитывая низкие вычислительные ресурсы и специфические виды атак (например, Blackhole, DDoS). Это делает их более практичными для реальных сценариев.

6. Многоклассовая классификация.

Новые модели могут различать не только нормальный трафик, но и несколько типов атак, что повышает их универсальность.

Недостатки

1. Высокая вычислительная сложность.

Комбинированные модели (например, CNN+LSTM, CNN+RNN) демонстрируют увеличенное время вывода, что затрудняет их использование в реальном времени. Такие

подходы требуют значительных ресурсов для обучения и тестирования.

2. Проблемы интерпретируемости.

Глубокие нейронные сети часто рассматриваются как "черные ящики". Это вызывает сложности в объяснении решений моделей и снижает доверие пользователей к результатам.

3. Ограниченная применимость к новым типам атак.

Некоторые подходы зависят от заранее собранных наборов данных, которые могут не содержать новых или редких атак. Это ограничивает их эффективность в динамично меняющихся сетевых условиях.

4. Зависимость от качества данных.

Успех моделей сильно зависит от качества и разнообразия данных. Плохая разметка или шум в данных могут снижать точность.

5. Отсутствие стандартизации.

Использование различных наборов данных и метрик оценки затрудняет сравнение методов между собой и их объективную оценку.

6. Неоптимальная адаптация к IoT.

Хотя есть подходы, учитывающие специфику IoT, многие из них недостаточно оптимизированы для устройств с ограниченными ресурсами.

7. Сложность настройки гиперпараметров.

Многие модели требуют тонкой настройки гиперпараметров для достижения высокой производительности, что увеличивает время и сложность разработки. На основании выполненного сравнительного анализа, можно выделить следующие перспективы в разработке новых подходов к построению систем обнаружения вторжений по аномалиям в сетевом трафике (Интернет), в том числе в системах Интернета вещей.

1. Разработка интерпретируемых моделей.

Использование методов интерпретации, таких как LIME и SHAP, для повышения прозрачности и объяснимости решений.

2. Интеграция с облачными платформами.

Использование облачных решений для обработки больших объемов данных и реализации вычислительно затратных моделей.

3. Обучение на потоковых данных.

Разработка методов, способных адаптироваться к изменениям в данных в РВ

4. Модели с низким энергопотреблением.

Упрощение архитектур для реализации в ограниченных средах, таких как IoT.

5. Использование новых наборов данных.

Создание и использование более разнообразных и актуальных наборов данных для оценки моделей. Использование генеративно-состязательных сетей (GAN) для синтеза данных атак.

Выводы. На основании исследования можно сделать выводы, что дальнейшая работа в этой области предполагает совершенствование методов и построение новых моделей глубокого обучения, их апробация путем моделирования на основе датасетов уязвимостей, как собранных, так и синтетических, и сравнительный анализ результатов выявления угроз. Практический интерес такой работы обоснован задачей внедрения систем обнаружения вторжений в реальные секторы использования IoT устройств, что позволит избежать больших потерь на рынке, связанных с киберпреступлениями.

Литература

1. Петренко С.А. Методы обнаружения вторжений и аномалий функционирования киберсистем Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 194-202.

2. Сертификация систем обнаружения вторжений / Барабанов А., Марков А., Цирлов В. // Открытые системы. СУБД. 2012. № 3. С. 31-33.

3. Yuan X, Han S, Huang W, Ye H, Kong X, Zhang F. A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system. Computers & Security. 2024; 137:103644.

4. *Wang YC, Houng YC, Chen HX, Tseng SM. Network Anomaly Intrusion Detection Based on Deep Learning Approach. Sensors [Internet]. 2023; 23(4). Disponible sur: https://www.mdpi.com/1424-8220/23/4/2171*

5. *Awajan A. A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. Computers [Internet]. 2023; 12(2). Disponible sur: https://www.mdpi.com/2073-431X/12/2/34*

6. *Khan NW, Alshehri MS, Khan MA, Almakdi S, Moradpoor N, Alazeb A, et al. A hybrid deep learning-based intrusion detection system for IoT networks. Mathematical Biosciences and Engineering. 2023;20(8):13491-520.*

7. *Sharma B, Sharma L, Lal C, Roy S. Anomaly based network intrusion detection for IoT attacks using deep learning technique. Computers and Electrical Engineering. 2023; 107:108626.*

8. *Ravi V, Pham TD, Alazab M. Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. IEEE Internet of Things Magazine. 2023; 6(2):50-4.*

9. *Bowen B, Chennamaneni A, Goulart A, Lin D. BLoCNet: a hybrid, dataset-independent intrusion detection system using deep learning. International Journal of Information Security. 2023; 22(4):893-917.*

10. *Gupta C, Kumar A, Jain NK. An Enhanced Hybrid Intrusion Detection Based on Crow Search Analysis Optimizations and Artificial Neural Network. Wireless Personal Communications [Internet]. 2024.*

11. *Kumar PM, Vedantham K, Selvaraj J, Kavin BP. Enhanced Network Intrusion Detection System Using PCGSO-Optimized BI-GRU Model in AI-Driven Cybersecurity. In: 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC). 2024. p. 1-6.*

12. *Wang X, Yin S, Li H, Wang J, Teng L. A Network Intrusion Detection Method Based on Deep Multi-scale Convolutional Neural Network. International Journal of Wireless Information Networks. 2020; 27(4):503-17.*

13. *Павленко Е. Ю., Гололобов Н. В., Лаврова Д.С., Козачок А.В. Распознавание киберугроз на адаптивную сетевую топологию крупномасштабных систем на основе рекуррентной нейронной сети // Вопросы кибербезопасности, 2022, № 6 (52), с. 93-99.*

14. *LSTM neural networks for detecting anomalies caused by web application cyber-attacks / I. Kotenko, I. Saenko, O. Lauta, K. Kribel // Frontiers in Artificial Intelligence and Applications. 2021. Vol. 337. P. 127-140.*

15. *Большаков А.С., Хусаинов Р.В., Осин А.В. Обнаружение аномалий трафика с использованием нейронной сети для обеспечения защиты информации // I-methods. 2021. Т. 13. №4. URL: http://intech-spb.com/wp-content/uploads/archive/2021/4/6-bolshakov.pdf*

16. *Соболев Н.В., Зегжда Д.П. Построение сети с honeypot на основе классификации трафика с помощью LSTM // Методы и технические средства обеспечения безопасности информации: Материалы 31-й научно-технической конференции 27 – 30 июня 2022 года. СПб: Изд-во Политехнического университета, 2022. – С. 15-16.*

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

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, профессор, Финансовый Университет при правительстве Российской Федерации, a.markov@npo-echelon.ru.

Approaches to Intrusion Detection Using Neural Networks to Analyse Network Traffic Comparison

Makoveichuk Y. T. [97]

Abstract. In the article the approaches based on deep learning to the design of intrusion detection systems by anomalies in network traffic (Internet), including in the systems of the Internet of Things, of different researchers, both foreign and Russian, are compared. The systematisation of the used approaches is made. Advantages and disadvantages are highlighted. Prospects and directions of improvement of methods for building intrusion detection and prevention systems based on the use of neural networks are defined. Emphasis is made on the importance of working with input data for models, improvement of methods for creating input data sets, including synthetic ones, application of methods for interpreting the results of models, adaptation of research on model building to the peculiarities of IoT.

Keywords: model, intrusion detection system, defence, neural network, hybrid model, traffic, anomaly, deep learning, interpretability, IoT.

[97] Yan Makoveichuk, PhD Student, Financial University under the Government of the Russian Federation, Moscow, makoweychuk.yan@yandex.ru

УДК 004.056

Контроль IoT при помощи средств информационной безопасности в государственном и корпоративном управлении

Марков Г.А.[98], Маркова Е.Д.[99]

Аннотация. В статье рассматривается возможность контроля Интернета вещей (IoT) средствами информационной безопасности в сферах государственного и корпоративного управления. Предложена методология обеспечения безопасности данных при внедрении технологий Интернета вещей с учетом внутренних и внешних угроз. Проведен обзор подходящих средств информационной безопасности и предоставлены рекомендации по их применению к контролю устройств Интернета вещей. Результаты исследования могут быть полезны в улучшении уровня информационной безопасности за счет минимизации рисков, имеемых при использовании Интернета вещей в государственных учреждениях и корпоративных компаниях.

Ключевые слова: Интернет вещей, защита информации, кибербезопасность, SIEM

Введение.

Актуальность темы обусловлена ростом количества устройств Интернета вещей, внедряемых как в обиходе, так и в государственных и коммерческих предприятиях. Использование подобных устройств несет свои риски в области информационной безопасности, так как в большинстве случае отсутствуют процессы управлениями уязвимостей IoT и контроля безопасности передачи данных [1-7]. С ростом цифровизации становится необходимым контролировать подобные устройства для защиты инфраструктуры. Исследование направлено на анализ имеющихся мер по снижению вышеуказанных рисков на предприятиях.

Целью работы является разработка методики улучшения эффективности контроля и защиты устройств Интернета вещей при помощи средств защиты информации применительно к государственному и корпоративному управлению.

Для достижения цели, были сформированы следующие задачи:

1) провести анализ угроз касательно использования устройств Интернета вещей;
2) провести анализ существующих подходов и методов для контроля и обеспечения информационной безопасности в инфраструктура;
3) при помощи собранных материалов сформировать подходы и рекомендации по внедрению средств Интернета вещей.

Определение и сущность понятия Интернета вещей

В настоящее время отсутствует единое определение понятия Интернета вещей. Джейд Картер предложил рассмотреть Интернет вещей, как концепцию, предполагающую соединение различных физических устройств, оборудованных сенсорами, программным обеспечением и другими технологиями, для обмена данными через интернет [8].

М.В. Ядровская, М.В. Поркшеян, А.А. Синельников в своей работе [9] определили Интернет вещей, как технологию, состоящую в объединении с помощью сетей людей, устройств, физических и виртуальных вещей, процессов и систем, которые могут взаимодействовать друг с другом посредством передачи данных.

Е.П. Зараменских и И.Е.Артемьев отметили, что Интернет вещей – это объединяющий термин для совокупности технологий, которые обеспечивают захват разного рода данных из внешней среды и их дальнейшую обработку при минимальном участии человека [10].

[98] Марков Георгий Алексеевич. Инфосистемы Джет, detonate1@yandex.ru
[99] Маркова Елена Дмитриевна. Аппарат Совета Федерации, РАНХиГС, manlendmi@yandex.ru

Законодательно в РФ не закреплено понятие Интернета вещей, однако в Прогнозе долгосрочного социально-экономического развития Российской Федерации на период до 2030 года Интернет вещей считается инфраструктурой новых классов объектов и определяется как информатизация различных предметов и включение их в единую сеть сетей[100].

Архитектурно Интернет вещей можно представить как устройства, подключенные к сети и осуществляющие сбор и передачу информации без участия человека. Подобные устройства передают данные на удаленный сервер, где происходит обработка информации. Несмотря на то, что устройства используются без человека, это не значит, что в нем не может быть функционала, который может использоваться.

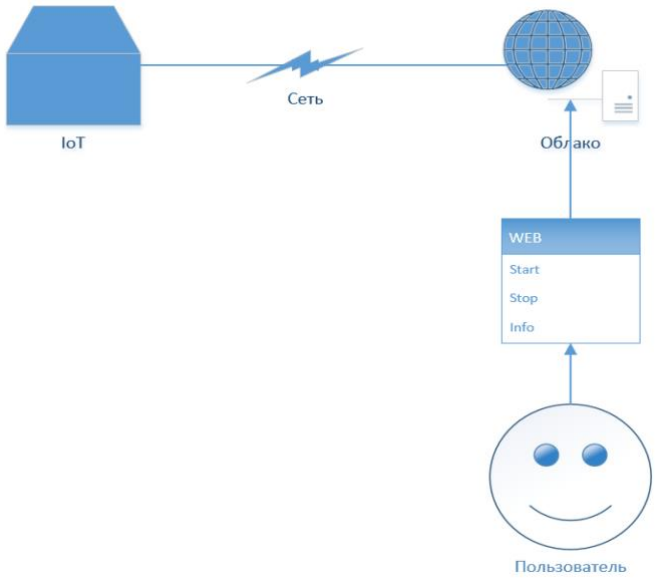


Рис. 1. Компоненты технологии Интернета вещей.

К наиболее важной проблеме использования технологии Интернета вещей стоит отнести вопросы кибербезопасности. Прогнозируется, что количество устройств Интернета вещей во всем мире почти удвоится с 15,9 млрд в 2023 году до более чем 32,1 млрд устройств IoT в 2030 году, что автоматически приведет к увеличению риска нарушения безопасности Интернета вещей[101].

На сегодняшний день можно выявить ряд актуальных угроз безопасности Интернета вещей (табл. 1).

Таблица 1.

Актуальные угроз безопасности

Угроза	Описание
Незащищенное оборудование	66% модулей IoT, поставленных в 2023 году не имели специальной аппаратной защиты, а 29% не имели функций безопасности.
Передача данных в незашифрованном виде	98% всего трафика IoT-устройств не зашифровано, что несет риск раскрытия данных.
Ботнеты Интернета вещей	Ботнет – это сеть IoT-устройств, зараженных вредоносным ПО, используемая для DDos-атак с целью перегрузки серверов, кражи личных данных и конфиденциальной информации, рассылки массового спама и пр.

[100] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[101] https://iot-analytics.com/cellular-iot-module-security/

Угроза	Описание
Взлом или подмена физических IoT-устройств	Наиболее уязвимые устройства Интернета вещей: корпоративные компьютеры, камеры видеонаблюдения, веб-камеры, промышленные IoT-устройства. Устройства Интернет вещей могут стать объектами атак, если злоумышленники получат доступ к их сети путем подбора пароля, обхода системы безопасности.
Несвоевременное обновление или обслуживание IoT-устройств.	На сегодняшний день имеются проблемы, связанные с выявлением дефектов уязвимостей в продукте, которые в большинстве своем закрываются путем обновления программного обеспечения устройства. При подобном обновлении в ряде случаев устройство временно перестает функционировать, что недопустимо для критичной инфраструктуры либо непрерывного производства.

Подходы к контролю Iot

Законодательная сфера контроля безопасности устройств Интернета вещей только развивается [11]. Приведем несколько примеров законодательных мер.

Федеральный закон «О персональных данных» регулирует отношения, обработки персональных данных, которые могут собираться устройствами IoT. Определяет правила обработки и защиты данных, устанавливает требования к обработке. Согласно ст.6 требуется обязательное наличие согласия пользователя на обработку его персональных данных.

Устройства содержат технологии, которые могут быть защищены авторскими правами, патентами, поэтому перед использованием таких устройств следует быть уверенным, что не нарушается интеллектуальная собственность. В РФ данные вопросы регламентируются Гражданским кодексом Российской Федерации.

Федеральный закон «Об информации, информационных технологиях и о защите информации» защищает частную жизнь человека, недопустим сбор, хранение и распространения информации без его согласия. Операторы устройств должны обеспечивать защиту информации, собираемой и обрабатываемой IoT-устройствами.

В октябре 2024 года Минпромторг сообщил, что Росстандарт утвердил ключевой протокол связи для Интернета вещей, который стал национальным стандартом. Новый стандарт будет способствовать развитию технологий умных устройств и формированию экономики данных в стране., а также позволит создавать современные отечественные решения для сельского и городского хозяйства, промышленности, здравоохранения, энергетики и транспортной инфраструктуры».

В данном исследовании мы будем учитывать техническо-организационные меры. Приведем основные методы контроля средств Интернета вещей в виде таблицы (табл. 2):

Таблица 2

Методы контроля средств Интернета вещей

Мера	Требование
Шифрование данных	Для обеспечения конфиденциальности передаваемых данных нужно использовать алгоритмы шифрования. Если сам IoT не содержит подобного функционала – можно использовать криптошлюзы для закрытия данного риска.
Авторизация устройств и пользователей	Должно происходить профилирование подключаемых устройств к сети предприятия для избежание нелегитимных действий и доступа. Одним из решений может быть система класса NAC.

Управление уязвимостями/патчами/версиями ОС	Требуется наличие или разработка процессов выявления уязвимостей и дефектов в операционных системах устройств, а также из программного обеспечения. Вспомогательным средством для решения подобных проблем могут быть системы класса vulnerability management
Мониторинг и реагирования на инциденты	Из-за большого количества устройств требуется их централизованный мониторинг. Контроль основных показателей при помощи систем мониторинга не является достаточным. Необходима система класса SIEM с процессами управления инцидентами
Контроль сетевого периметра	Для избежание несанкционированного доступа по сети нужно использовать средства типа МЭ

Данный набор методов (табл.1) можно считать минимумом для покрытия представленных ранее рисков.

На основе методов и рисков была предложена следующая методика внедрения устройства Интернета вещей на предприятии или в государственном учреждении:

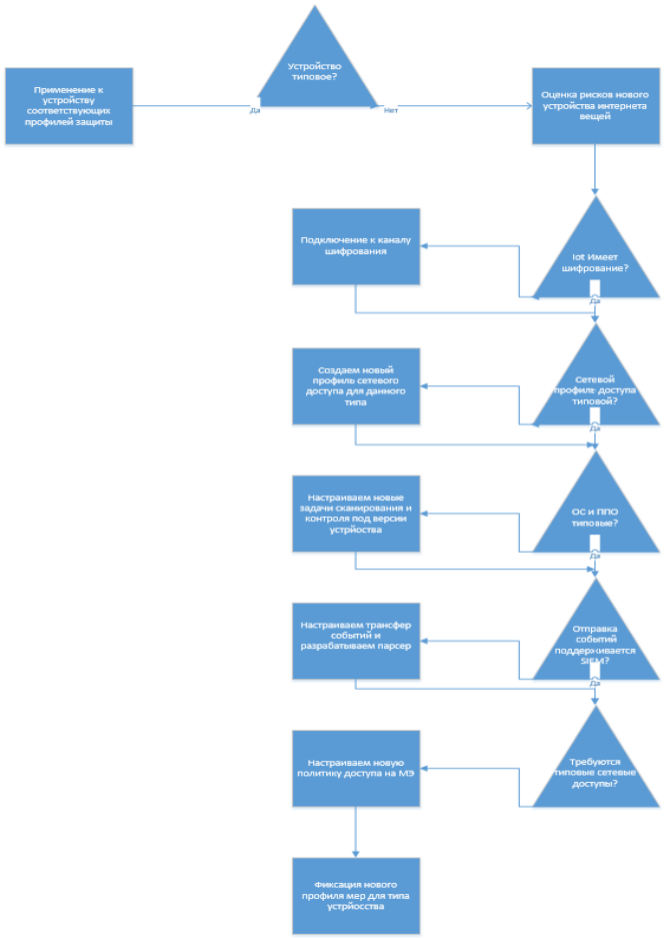


Рис. 2. Методика внедрения устройства Интернета вещей.

Заключение

В заключении следует отметить, что предложенная методика может повысить эффективность управления устройствами Интернета вещей за счет подходов информационной безопасности при внедрении.

Нужно отметить, что предложенные средства защиты информации должны быть современны и полностью выполнять свои функции безопасности необходимые для выполнения методики.

Не стоит забывать, что с устройствами работает персонал. Поэтому важной частью процесса работы с устройствами Интернета вещей является проведение обучения сотрудников с целью эффективного использования возможностей IoT-технологии, а также для наилучшей адаптации к новым технологиям.

Текущие реалии диктуют необходимость усовершенствования законодательства Российской Федерации в области контроля Интернета вещей. Данная тема может быть рассмотрена как совершенствование методики данного исследования в будущем.

Комплексное внедрение и использование Интернета вещей в государственном и корпоративном управлении могут привести к улучшению эффективности, уменьшению затрат и повышению уровня предоставляемых услуг. Важно не только следовать технологическим трендам, но и учитывать все риски и возможные проблемы, связанные с данной технологией.

Литература

1. *Анализ и оценка эффективности протоколов транспортного уровня в сетях NB-IOT / Колесников А.В., Басараб М.А., Ключарев П.Г., Кузьминов И.М. // Приборы и системы. Управление, контроль, диагностика. 2024. № 4. С. 1-14.*
2. *Дахнович А.Д., Москвин Д.А., Зегжда Д.П. Применение принципа "безопасности через незнание" в промышленном интернете вещей // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1. С. 131-137.*
3. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д. П. Зегжды. - М.: Горячая линия - Телеком, 2021. - 560 с.*
4. *Петренко А.А., Петренко С.А., Костюков А.Д. Киберустойчивая платформа интернета вещей // Защита информации. Инсайд. 2020. № 4 (94). С. 20-30.*
5. *Петренко С. А. Киберустойчивость индустрии 4.0. - СПб.: Издательский Дом "Афина". - 2020. - 256 с.*
6. *Система измерения защищенности информации и персональных данных для устройств интернета вещей / Федорченко Е.В., Новикова Е.С., Котенко И.В. и др. // Вопросы кибербезопасности. 2022. № 5 (51). С. 28-46.*
7. *Соколов М.Н., Смолянинова К.А., Якушева Н.А. Проблемы безопасности интернет вещей: обзор // Вопросы кибербезопасности. 2015. № 5 (13). С. 32-35.*
8. *Картер Д. IOT Интернет вещей: разработка, интеграция и управление устройствами. М.: Литрес, 2024. 180 с.*
9. *Ядровская М.В. Перспективы технологии интернета вещей/ М.В. Ядровская, М.В. Поркшеян, А.А. Синельников // Advanced Engineering Research. – 2-21. – Т. 21, № 2. – С.207-217.*
10. *Зараменских Е.П. Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е. Артемьев. – Москва: ИНФРА-М, 2024. – 188 с.*
11. *Стандарты кибербезопасности четвертой промышленной революции и индустрии 4.0 / Марков А.С., Тимофеев Ю.А. // Защита информации. Инсайд. 2021. № 3 (99). С. 54-60.*

IoT control using information security tools in state and corporate governance

Markov G.A.[102], Markova E.D.[103]

Abstract. The article considers the possibility of controlling the Internet of Things (IoT) by means of information security in the spheres of state and corporate governance. The methodology of ensuring data security in the implementation of Internet of Things technologies taking into account internal and external threats is proposed. A review of suitable information security tools is conducted and recommendations for their application to the control of Internet of Things devices are provided. The results of the study can be useful in improving the level of information security by minimising the risks available when using the Internet of Things in government agencies and corporate companies.

Keywords: Internet of Things, information protection, cyber security, SIEM

[102] Georgiy A. Markov. Jet Infosystems, detonate1@yandex.ru

[103] Elena D. Markova. Office of the Federation Council, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, manlendmi@yandex.ru

УДК 004.056

Подходы, направленные на повышение эффективности тестирования безопасности на этапе конструирования и комплексирования ПО

Марчеков С.Д.[104],Булатов М.С.[105], Быков А.Ю.[106]

Аннотация: тестирование безопасности в рамках цикла непрерывной интеграции в рамках разработки безопасного программного обеспечения является обязательным этапом для команд разработки, к которым предъявляются требования по безопасности. В рамках данной статьи рассматриваются подходы, направленные на повышение эффективности тестирования ПО на этапах проверки исходного кода, его сборки и формирования дистрибутива. Проведена оценка методов применяемых для анализа ПО и аналитической обработки результатов анализа с целью автоматизации методов обработки результатов инструментальных средств (средств композиционного анализа заимствованных компонентов, статического анализа исходного кода и экспертизы исходного кода) и повышению скорости выявления ошибок (недостатков) в системном и инфраструктурном ПО для операционных систем семейства Linux.

Ключевые слова: статический анализ, экспертиза исходного кода, заимствованные компоненты, информационная безопасность, безопасная разработка, операционная система.

Введение

В соответствии с ГОСТ 56939-2016 в процессе разработки безопасного программного обеспечения при выполнении конструирования и комплексирования должны реализоваться следующие меры:

- использование при разработке ПО идентифицированных инструментальных средств;
- создание программы на основе уточненного проекта архитектуры программы;
- создание (выбор) и использование при создании программы порядка оформления исходного кода программы;
- статический анализ исходного кода программы;
- экспертиза исходного кода программы.

Стоит учесть, что и обновленная редакция стандарта 2024 года и методики тестирования сертифицированных средств [1] так же включают данные требования реализации мер. Рассмотрим технические меры, указанные в списке, а именно статический анализ и экспертизу исходного кода программы.

В рамках анализа кодовой базы можно выделить несколько наборов компонентов:

1. Заимствованные компоненты.
2. Проприетарные компоненты:
   - код, написанный разработчиком с нуля;
   - код, с открытой лицензией или код по NDA соглашению, переиспользуемый или дорабатываемый для использования в текущем ПО.

Опишем подходы применимые для каждого из этих наборов, проанализируем применимость подходов для повышения эффективности методов тестирования безопасности разрабатываемого ПО.

104 Марченков Сергей Дмитриевич, аспирант, МГТУ им. Н.Э. Баумана, Москва, marchenkovsd@bmstu.ru
105 Булатов Марк Станиславович, ведущий специалист, ООО «РусБИТех-Астра», Москва, mbulatov@astralinux.ru
106 Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

Тестирование заимствованных компонентов

Использования статических анализаторов

Схема работы статических анализаторов разделяется на контролируемую сборку и сканирование исходного текста. Сборка, сканирование и анализ в данном случае выполняются автоматизированными методами, разметка – ручная верификация результатов работы статических анализаторов специалистами тестирования безопасности. Именно разметка представляет интерес для реализации методов дополнительной автоматизации для ускорения процесса общего анализа и доведения сведений об ошибках до разработчиков.

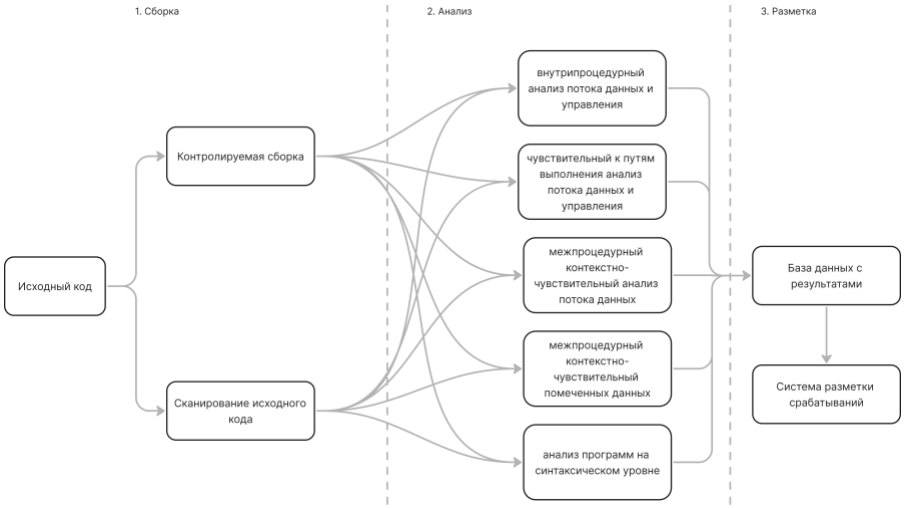


Рис. 1. Схема работы статических анализаторов

При проведении статического анализа заимствованных компонентов стоит учитывать специфику реализации сборки, это особенно важно учитывать при анализе компилируемых языков программирования, так как инструментальные средства работают с контролируемым процессом сборки, в рамках которого происходит перехват системных вызовов. При контролируемой сборке анализатор фиксирует порядок запуска программных средств, их настройки и используемые конфигурации [2 - 4]. Это позволяет отследить запуски всех интересующих утилит, получить требуемую информацию из их параметров и окружения, организовать запуск собственных компонент анализатора.

Анализ файлов конфигурации

В зависимости от языка программирования варьируется и основная система сборки (**CMake, Make, Ninja, Bazel, Maven, Gradle, Buildah и проч.**). На основе файлов конфигурации можно определить цели, которые будут собираться в готовый дистрибутив. Например, если в целях Makefile или debian/rules отсутствует модуль исходных тестов, представленных в оригинальном коде, то можно провести постобработку результатов статических анализаторов в системе разметки с выставлением статуса проверки «false positive» и требуемых действий «игнорировать». Тем самым обозначив избыточность кода. Так как оригинальный код сложно поддерживать, то и удаление данных участков кода влечет за собой накладные расходы. Поэтому самым простым решением остается игнорирование срабатываний в данных областях кода.

Стоит также рассмотреть код интерпретируемых скриптов, который может быть перенесен из исходного кода в директорию debian (при создании двоичных, готовых к установке пакетов debian) при наложении патчей разработчиков на оригинальный код. В таком случае стоит объединить срабатывания из обеих директорий, что сократит количество срабатываний.

Анализ избыточного кода

Сканирование кода методами сигнатурного анализа (как одного из основных методов анализа по ГОСТ Р 71207 – 2024 Статический анализ программного обеспечения. Общие требования) проводится как правило по всему коду, в том числе не задействованного при работе программы, относящегося к неиспользуемым импортируемым модулям.

Неиспользуемый импорт замедляет компиляцию, эффект, который может стать существенным по мере накопления кода программы со временем. По этим причинам Go отказывается компилировать программы с неиспользованными переменными или импортами, внося краткосрочное удобство для долгосрочной скорости сборки и ясности программы [5]. В компиляторах gcc и clang предусмотрен механизм оптимизации, который может пропустить неиспользуемые переменные, но неиспользуемый импорт допускается и попадает в бинарное представление.

Отличие от предыдущего метода в том, что проверка неиспользуемых заголовочных файлов и поиска методов и функций из неиспользуемого импорта не точно прорабатывается алгоритмами статических анализаторов. Данный вид анализа можно отнести к межпроцедурному анализу, по-умолчанию максимальная глубина поддерживаемого межпроцедурного анализа (количество вызовов процедур, через которые может передаваться собираемая в ходе анализа информация о потоке данных программы) не должна быть заранее ограничена, но может определяться с учетом доступных для анализа вычислительных ресурсов. В данном случае стоит исследовать только первое включение функции. Если срабатывание было найдено именно методом синтаксического анализа исходного кода ПО, стоит провести анализ вызывающего модуля на предмет наличия в нем вызова функции данного заголовочного файла. На рисунке 2 приведена ситуация, когда функция *function_b()* отсутствует в вызывающем компоненте, который импортирует *b.h*. В случае, если ни один файл имеющий импорт *b.h* не содержит функций из *b.h*, то весь импорт *b.h* можно убрать из перечня исследуемых файлов.

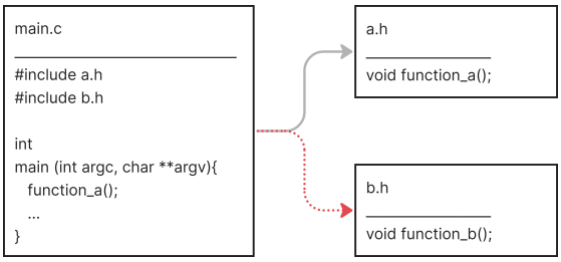


Рис. 2. Исключение неиспользуемых заголовочных файлов при анализе

Поиск известных ошибок (недостатков)

Системное программное обеспечение в рамках поддержки определенного списка операционных систем должно работать с зависимостями, которые идут в составе среды функционирования. Разработчики операционных систем опираются на патчи вендоров, если выявляется уязвимость критического уровня опасности. Если брать в рассмотрение недостатки, которые не всегда приводят к уязвимостям безопасности, но имеют статус серьезности маркера – высокий или критичный, данные недостатки должны быть устранены после верификации их специалистом или разработчиком.

Такой же логики нужно придерживаться при заимствовании исходного кода, который находится в свободном доступе под открытой лицензией. Сложность заключается в том, что версия данного заимствованного модуля может быть ниже, чем версия, которая находится в основной ветке разработки (upstream). В таком случае на каждое срабатывание анализатора можно производить поиск по коду в upstream, указывая на коммит исправления основного разработчика. Стоит учитывать, что коммит можно вынести из upstream (рис.3), но применение его в виде патча остается в ответственности мейнтейнера поддерживающего

компоненту, которая отвечает за его корректное функционирование в комплексе модулей, непосредственно влияющих на разрабатываемое ПО.

С целью упрощения анализа обнаруженных ошибок авторами разработан инструмент, позволяющий автоматически сопоставлять срабатывания с ошибками, содержащимися в upstream, что дает возможность быстрее обнаруживать ошибки, ранее выявленные другими исследователями или заносить еще неизвестные ошибки на исправление в upstream.

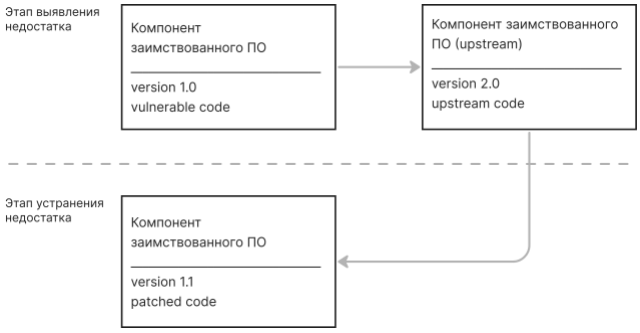


Рис. 3. Способы устранения недостатка в upstream

Данный подход можно так же приметить к результатам композиционного анализа при описании корректирующих воздействий по результатам анализа уязвимостей в зависимостях ПО. Для актуальных уязвимостей из списка CVE может предоставляться сразу несколько решений:

– минимальная неуязвимая версия компонента, если её использование не нарушает корректного функционирования ПО;

– патч вендора из основной ветки разработки;

– компенсирующие меры, которые могут быть применены для обеспечения безопасности, к таковым можно отнести встроенные и наложенные средства защиты информации.

Первые два метода могут быть автоматизированы, патч вендора может подтягиваться по указанному коммиту с исправлением описанным выше инструментальным средством (рис.4).

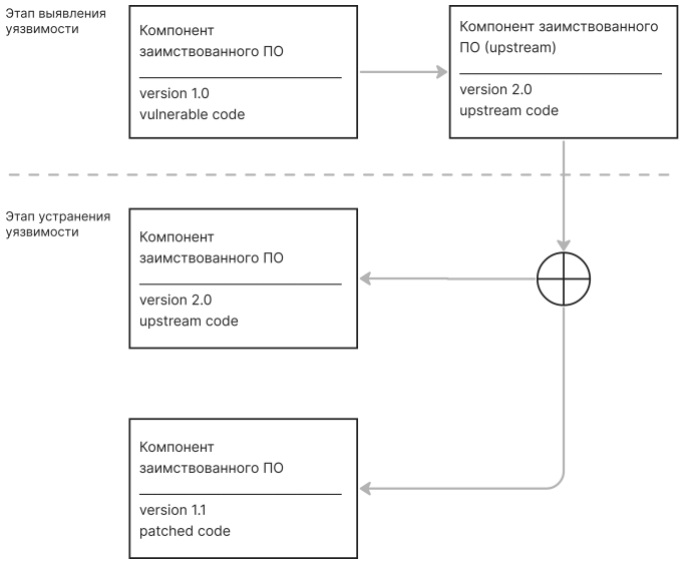


Рис. 4. Способы устранения уязвимости в upstream

Тестирование проприетарных компонентов

Схема анализа разрабатываемых компонентов идентична анализу заимствованных (рис.1), отличие заключается в полной ответственности разработчика за собственный код.

В системах интеграции реализовано большое количество подходов к исследованию кода, в том числе и на базе искусственного интеллекта и машинного обучения [6, 7]. Но в рамках исследования стандартных средств приведем лишь некоторые из подходов, которые можно автоматизировать силами DevOps инженеров.

Автоматизированная отладка

Инструменты статического анализа на значительных объемах программного кода выдают большое количество предупреждений о возможных ошибках, большинство из которых являются ложноположительными или не требующими устранения в силу их несущественного влияния на безопасность ПО. Чтобы провести полноценную аналитическую обработку всех срабатываний требуется большое количество человеческих ресурсов для подтверждения и эксплуатации выявленных недостатков. Анализаторы не учитывают параметры сборки, которые могут подтвердить результаты некоторых предупреждений.

Проанализировав процесс подтверждения недостатка, можно выделить этап дополнительного анализа в рамках динамического анализа и отладки (рис.5).

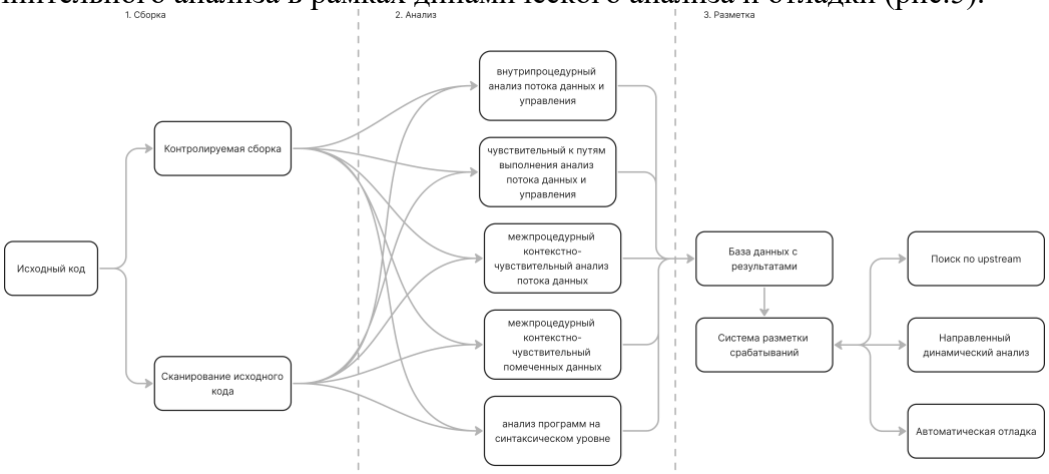


Рис. 5. Дополнительные этапы автоматизированной разметки срабатываний

Данный этап можно автоматизировать либо применением направленного динамического анализа, либо методами ручной отладки и нефункционального тестирования (тестирование на проникновение). Если первый уже успешно применяется на практике [8], то второй можно автоматизировать лишь частично. В рамках исследований утилит пользовательского пространства авторам удалось успешно подобрать параметры запуска программы для прохождения пути до места срабатывания в определенной функции и автоматизировать обращение к бинарному коду в рамках отладки с помощью gdb.

Некоторые из срабатываний, которые могут быть проверены методом интерактивной отладки:

- использование небезопасных функций;
- самоприсваивание или неиспользуемый код;
- неинициализированная переменная и разыменование неинициализированной переменной.

Определить ложное срабатывание для каждого случая — задача тривиальная. Для небезопасных функций, сравнив функцию при отладке с упомянутой в срабатывании. Замена может происходить при использовании макроса FORTIFY_SOURCE при компиляции. Самоприсваивание или неиспользуемый код могут быть опущены при компиляции в рамках оптимизации при использовании флагов «-O». Разыменование просто прервет программу при обращении к переменной.

Доработка анализаторов

Инфраструктура анализа расширяема, это означает, что возможно разработать дополнительные алгоритмы для поиска новых видов потенциально опасных ситуаций в

коде программы с использованием имеющихся алгоритмов и подготовленных ими данных. Многие инструменты статического анализа позволяют писать правила поиска недостатков на основе XPath [9] или чекеров реализованных в clang-tools [10], с целью автоматизации нахождения ошибок и уязвимостей, ранее найденных методами экспертизы кода и тестирования на проникновение, специалистам и инженерам, непосредственно работающим с инструментами статического анализа, нужно адаптировать выявленные ошибки под шаблоны, которые могут быть найдены инструментальным средством.

Приведение метрик анализаторов к единому стилю

При агрегации результатов статических анализаторов критерии оценки инструментальных средств отличается, поэтому могут происходить расхождения в срабатываниях. В случае дедупликации срабатываний автоматизированными средствами стоит оставить максимальный уровень опасности, который в дальнейшем будет верифицирован вручную специалистом по тестированию безопасности или разработчиком.

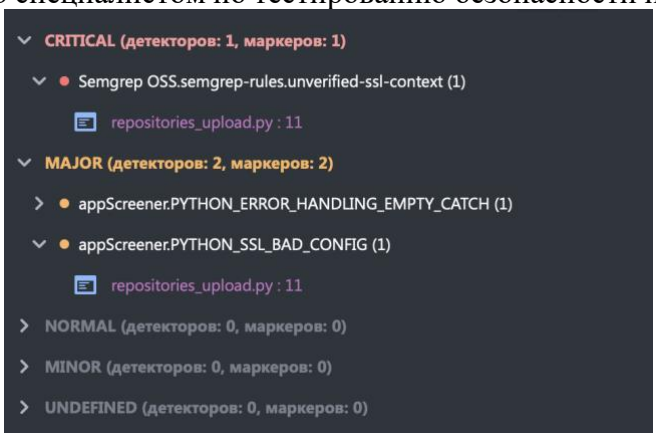


Рис. 6. Расхождение метрик статических анализаторов

Выводы

Совокупность описанных подходов и реализующих их инструментальных средств, применяемых авторами на этапах конструирования и комплексирования ПО позволяет сократить время, затрачиваемое на анализ обнаруженных срабатываний анализаторов. Важным критерием эффективности является время выявления ошибок, которое в результате применения всех описанных подходов сократилось втрое по сравнению с планомерным ручным тестированием каждого срабатывания. Совокупность применяемых подходов для автоматизации проведения тестирования безопасности обеспечивает большую уверенность в качестве полученных результатов. Таким образом, предложенные подходы к тестированию позволяют обеспечивать минимизацию ошибок в коде на протяжении всего жизненного цикла разработки, устраняя большинство программных ошибок на его ранних этапах, что создает условия для разработки безопасного системного и инфраструктурного ПО.

В качестве направлений дальнейших исследований наиболее приоритетными являются:

- исследование корреляции результатов динамического анализа и срабатываний статических анализаторов;
- уточнение метрики степени опасности срабатываний статических анализаторов в зависимости от различных факторов.

Литература

1. Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of Software Vulnerability Detection in Certification Testing // Journal of Physics: Conference Series. 2018. V. 1015. P. 042033.

2. Белеванцев А.А., Избышев А.О., Журихин Д.М. Организация контролируемой сборки в статическом анализаторе Svace. М.: Системный администратор, 2017, С. 135-139.

3. А.Е. Бородин, А.А. Белеванцев. Статический анализатор Svace как коллекция анализаторов разных уровней сложности. М.: Труды ИСП РАН, том 27, вып. 6, 2015 г., с. 111-134.

4. Бородин А.Е., Горемыкин А.В., Вартанов С.П., Белеванцев А.А. Поиск уязвимостей небезопасного использования помеченных данных в статическом анализаторе Svace. М.: Программирование, 2021, № 6, стр. 62-80.

5. Carmine Cesarano, Vivi Andersson, Roberto Natella, and Mar-tin Monperrus. 2024. GoSurf: Identifying Software Supply ChainAttack Vectors in Go. In .ACM, New York, NY, USA, 10 pages.

6. Felix Fischer, Jonas Höbenreich, and Jens Grossklags. 2023. The E□ectivenessof Security Interventions on GitHub. In Proceedings of the 2023 ACM SIGSACConference on Computer and Communications Security (CCS '23), November26–30, 2023, Copenhagen, Denmark. ACM, Copenhagen, DK, 17 pages.

7. Tamás Szabó. 2023. Incrementalizing Production CodeQL Analyses. In Pro-ceedings of the 31st ACM Joint European Software Engineering Conferenceand Symposium on the Foundations of Software Engineering (ESEC/FSE '23), December 3–9, 2023, San Francisco, CA, USA. ACM, New York, NY, USA,16 pages.

8. Егорова В.В., Панов А.С., Тележников В.Ю., Девянин П.Н., Подходы, направленные на повышение эффективности фаззинг- тестирования компонентов защищенной ОС. М.: Труды ИСП РАН, том 34, вып. 4, 2022 г., стр. 21-34.

9. D. Chen, R. Huang, et al., Improving static analysis performance using rule-filtering technique. Proceedings of the 26th International Conference on Software Engineering and Knowledge Engineering, 2014.

10. M. Arroyo, F. Chiotta, and F. Bavera, "An user configurable clang staticanalyzer taint checker," in 2016 35th International Conference of theChilean Computer Science Society (SCCC). IEEE, 2016, pp. 1–12.

Approaches for improving the efficiency of application security at the stage of software design and integration

Marchenkov S.D.[107], Bulatov M.S.[108], Bykov A.Y.[109]

Abstract. Application security testing as part of the continuous integration cycle within the framework of secure software development is a mandatory stage for development teams that are subject to security requirements. This article discusses approaches aimed at improving the effectiveness of software testing at the stages of source code verification, its assembly and distribution formation. The evaluation of the methods used for software analysis and analytical processing of analysis results was carried out in order to automate the methods of processing the results of tools (tools for compositional analysis of borrowed components, static analysis of source code and examination of source code) and to increase the speed of error detection (deficiencies) in system and infrastructure software for Linux operating systems.

Keywords: static analysis, source code review, software compositional analysis, information security, secure development, operating system.

107Sergey Marchenkov, Ph.D. student, Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru
108 Mark Bulatov, leading specialist, RusBITech-Astra, Moscow, mbulatov@astralinux.ru
109 Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

УДК: 004.4:004.056

Практика обучения специалистов информационной безопасности с помощью платформы разработки программного обеспечения

Марченков С.Д.[110], Марочкин И.С.[111], Барзин А.А.[112], Быков А.Ю.[113]

Аннотация: постоянные изменения в подходах организации тестирования безопасности приложений определяет ход развития технологий и методов обучения сотрудников для работы с большим набором инструментальных средств тестирования. В статье рассматриваются методы использования платформы разработки программного обеспечения (ПО) GitFlic для подготовки специалистов информационной безопасности, методы развития навыков тестирования программ. Перечислены преимущества и недостатки использования платформы разработки и системы контроля версиями студентами и преподавателями.

Ключевые слова: система контроля версий, платформа безопасной разработки, совместная работа, безопасная разработка, система контроля версий, образование.

Введение

В силу тенденций обеспечения безопасности программного обеспечения, перед разработчиками возникают вызовы по сокращению срока разработки, реализации ПО клиентам, а также по своевременному устранению недостатков и уязвимостей, возникающих на различных этапах жизненного цикла ПО.

Тестирование безопасности на ранних стадиях разработки программного продукта (в рамках концепции shift-left [1]) произвел революцию в обеспечении качества ПО, что в свою очередь привело к повышению степени безопасности их инфраструктуры. Важным фактором тестирования является специализация экспертов, проводящих анализ результатов инструментальных средств тестирования, их доработка и уточнение конфигурации в зависимости от специфики тестируемого ПО.

Для обеспечения команд разработки необходимыми навыками требуется обучение сотрудников практикам в области тестирования безопасности. Для таких нужд выделяется наиболее подготовленный состав команды разработки (security champions) и группа тестирования безопасности (application security). Ответственность за проведение тестирования, разметку результатов средств тестирования и передачу сведений о недостатках возлагается на группу тестирования безопасности, в то время как команда разработки производит анализ и оценку корректности переданных данных. Целью данной работы стало исследование применимости платформы разработки в целях отслеживания данных процессов и применимости их к процессу обучения специалистов.

Практический курс обучения

В рамках освоения курсов по разработке защищенного ПО выделяются практические занятия по проведению тестирования ПО методами композиционного анализа ПО (далее — КАПО), статического анализа, динамического анализа и фаззинг-тестирования. Каждый из видов анализа имеет два этапа:

−автоматизированное сканирование;

−ручная разметка срабатываний.

[110] Марченков Сергей Дмитриевич, аспирант, МГТУ им. Н.Э. Баумана, Москва, marchenkovsd@bmstu.ru
[111] Марочкин Игорь Сергеевич, студент, МГТУ им. Н.Э. Баумана, Москва, marochkinis@student.bmstu.ru
[112] Барзин Анатолий Александрович, студент, МГТУ им. Н.Э. Баумана, Москва, barzin.anatoly@yandex.ru
[113] Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

Локальное тестирование

Тестирование можно производить локально на этапе написания кода программистом, но с учетом инфраструктуры развертывания средств, в большинстве случаев используют self-hosted решения или сервисы в SaaS [2]. Кратко рассмотрим варианты локального тестирования.

КАПО может производиться средствами сбора SBOM по коду, либо по артефакту сборки (deb или rpm пакеты, jar файлы, docker контейнеры и проч.), в результате сбора перечня компонентов проводится семантический поиск по открытым базам данных угроз. Преимущества локального сканирования КАПО – разработчик видит актуальные уязвимости и устраняет их сразу в локальной версии на рабочем месте. Недостатки — подходит для небольших проектов, зависимости поднимаются локально, не затрагивая другие компоненты системы, результаты об устраненных CVE не отображаются для других разработчиков, если заранее не продумана система оповещения об устранении уязвимости и передачи её в changelog.

Статический анализ кода в средствах, требующих сборки разделяется на агента сборки [3] и сервер анализа. Для более легковесных анализаторов используются плагины в IDE и анализаторы, результаты которых могут храниться рядом с кодом и обрабатываться средой разработки. Преимущества локального сканирования – разработчик видит и устраняет недостатки на локальном рабочем месте. Недостатки — подходит для легковесных анализаторов в области видимости отдельного модуля, тогда как глубокий анализ требует больше технических ресурсов.

Есть вариант обращения к серверу анализа с помощью плагинов или api запросов с последующим отображением результатов сканирований в IDE, но в рамках тестового стенда данный вариант не поддерживается из-за отсутствия такого вида интеграций для большинства статических анализаторов кода.

Динамический анализ разворачивается на тестовом стенде в процессе непосредственной работы приложения. Данный метод не применяется локально, только если не проводится модульное тестирование. Недостатки – требуются технические ресурсы для проведения качественного и быстрого сканирования, что невозможно реализовать на локальной машине.

Таким образом, выполнение тестирования в ручном режиме возможно, но имеет свои недостатки. Рассмотрим методы тестирования в процессе обучения, которые можно переложить на платформу совместной работы с кодом. В рамках эксперимента было создано две группы, проходившие обучение различными методами: метод командной работы, метод пошагового индивидуального обучения.

Алгоритм действий при использовании метода командной работы:

1. Разделение специалистов по направлениям тестирования.
2. Подготовка стенда тестирования.
3. Запуск инструментальных средств.
4. Снятие статуса работ один раз в неделю, уточнение задания.
5. Завершение тестирования, слияние изменений.

Для каждого направления выделяется отдельная ветвь разработки (Рис.1).

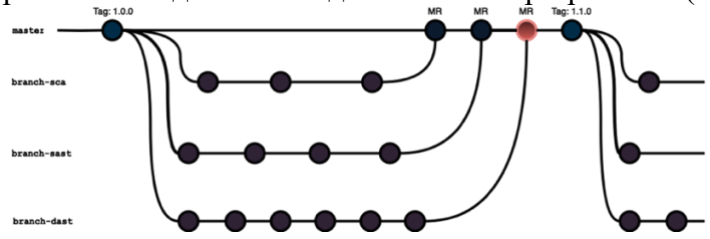


Рис. 1. GitFlow командной работы

Алгоритм действий при использовании метода пошагового индивидуального обучения:

1. Выделение отдельной ветки для создания конвейера тестирования.
2. Подготовка стенда тестирования.
3. Запуск инструментальных средств.
4. Снятие статуса работ один раз в неделю, уточнение задания.
5. Завершение тестирования, стабилизация конвейера разработки.

Для каждого обучающегося создается своя ветка тестирования (Рис.2). Используя тематические ветки, работа может вестись над разными функциями независимо [4]. Управление ветками позволяет студентам заранее начать разработку своих проектов, не мешая им при этом выполнять мелкие работы, такие как другие практические занятия или домашние задания [5-6].

Подготовка стенда тестирования подразумевает использование раннера для запуска инструментальных средств.

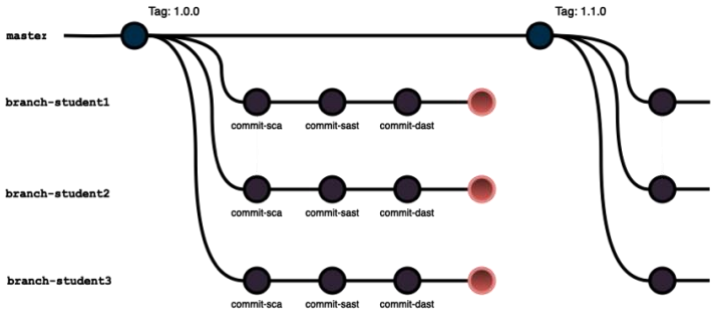


Рис. 2. GitFlow индивидуального обучения

Данный раннер может быть развернут как самим обучающимся (с привязкой к собственным мощностям), так и преподавателем на корпоративных ресурсах. Последний вариант более предпочтителен, так как не потребует дополнительного времени на установку раннера в ходе практических занятий.

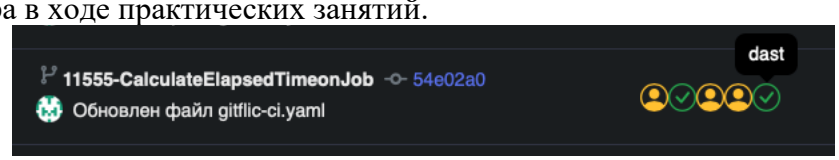


Рис. 3. Представление конвейера GitLab CI/CD

Завершение работы каждого инструмента в конвейере (Рис.3) сопровождается сбором артефакта, который может быть направлен на сторонние ресурсы разметки и системы управления процессами безопасной разработки (Рис.4), например, ASOC система.

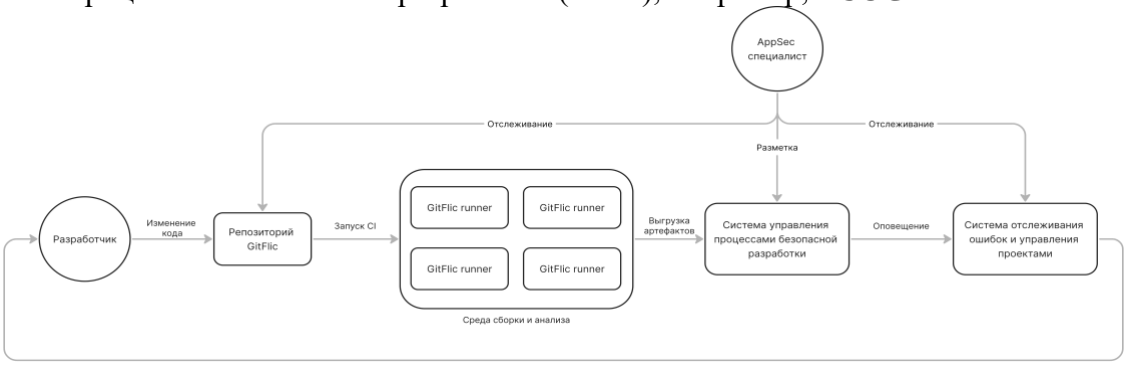


Рис. 4. Процесс тестирования безопасности ПО

Платформа GitFlic в отличие от обычной системы контроля версиями позволяет совмещать несколько инструментов для управления процессами разработки:

1. Система контроля версиями.
2. Система непрерывной интеграции.
3. Хранилище артефактов.
4. Система управления процессами безопасной разработки.

Каждый из элементов дает представление о безопасной разработке. В рамках системы хранения кода используется ролевая модель, которая позволяет определить индивидуальные права пользователей в проекте или команде (группе проектов). Непрерывная интеграция, как неотъемлемая часть процесса разработки, позволяет автоматизировать процессы тестирования [7-9]. Хранилище артефактов, а также реестр пакетов и контейнеров позволяют обеспечить независимость от внешних ресурсов, сохраняя образы с инструментами для тестирования локально. Система управлениями процессами безопасной разработки, которая реализована как отдельная функциональная вкладка «Безопасность» в проекте обеспечивает разбор артефактов и занесение их в список выявленных недостатков. Панель «Безопасность» позволяет сократить процесс оповещения разработчиков через системы отслеживания задач за счет отображения данных недостатков одновременно для специалистов группы тестирования безопасности, так и для команды разработки всех срабатываний (Рис. 5).

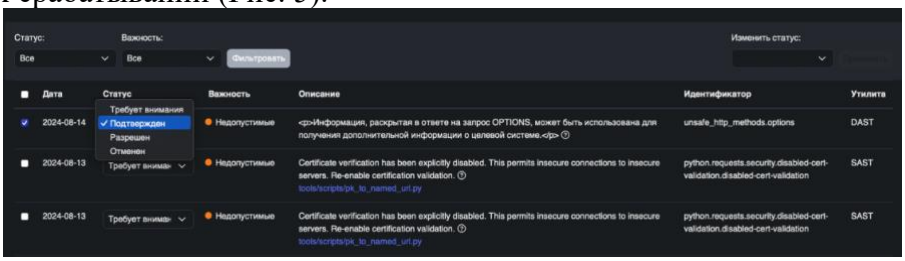


Рис. 5. Панель «Безопасность» платформы GitFlic

В рамках настройки этапов тестирования в конвейере разработки авторами были запущены задачи на статический анализ различными средствами проверки безопасности, такие как Syft, Trivy, Semgrep [8], SonarQube, ZAP [9] и Atheris, что показало корректную интеграцию со средствами тестирования безопасности под открытой лицензией и прием стандартизированных форматов предоставляемых средствами Solar appScreener, АК-ВС 3 и некоторыми другими проприетарными инструментами [10].

В дополнение к стандартным правилам тестирования авторами были протестированы сценарии создания собственных правил для статических анализаторов и их внедрения в этапы тестирования статическими анализаторами.

Проверка и оценка таких результатов может проводиться руководителем разработки (преподавателем) на этапе слияния или стабилизации работы конвейера [11].

Также с использованием платформы процесс тестирования безопасности ПО оптимизируется на этапе оповещения команды разработки за счет единого пространства работы с кодом и системой агрегации ошибок в панели «Безопасность» (Рис.6).

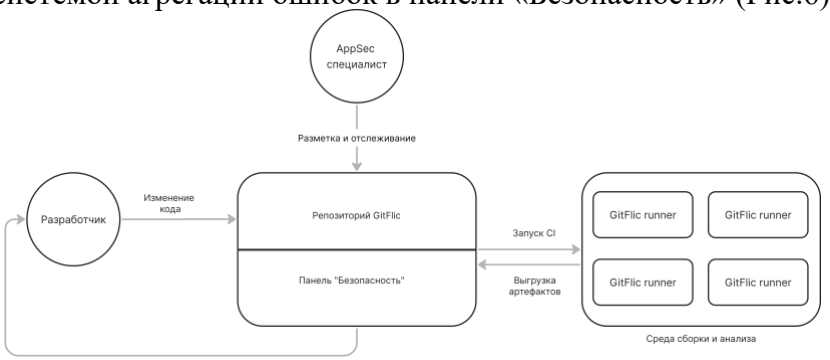


Рис. 6. Оптимизированный процесс тестирования безопасности ПО

Выводы

Метод командной работы позволяет проводить тестирование проекта в более короткий срок и предпочтителен для проведения в рамках производственных практик, что позволяет более глубоко вникнуть в узкоспециализированную тему.

Метод пошагового индивидуального обучения позволяет охватить больше методов тестирования, позволяя проявить большую свободу действий и применяемых методов тестирований.

Каждый из методов, проведенных на платформе GitFlic, позволяет проводить тестирование различных проектов в рамках нового семестра обучения, тем самым уменьшая вероятность повторения событий безопасности в проектах и увеличивая базу разметки срабатываний, что может стать основой для дальнейшего тестирования моделей машинного обучения применительно к размеченной выборке.

Литература

1. Vaddadi S. A., Padthe A., Arnepalli P. R. R., "Shift-Left Testing Paradigm Process Implementation for Quality of Software Based on Fuzzy," 2023.

2. Jozeph Lawrance, Wentworth Institute of Technology, Seikyung Jung, Charles Wiseman. "Git on the cloud in the classroom. " // Conference: Proceeding of the 44th ACM technical symposium on Computer science education. March 2013.

3. Белеванцев А.А., Избышев А.О., Журихин Д.М. Организация контролируемой сборки в статическом анализаторе Svace. М.: Системный администратор, 2017, С. 135-139.

4. Elgun Jabrayilzade, Fatih Sevban, Sülün Bilkent. "An Interactive Approach to Teaching Git Version Control System" // Conference: CSEE&T / HICSS 2022 - Conference on Software Engineering Education and Training: Special Track of Hawaii International Conference on System Sciences.

5. Felix Fischer, Jonas Höbenreich, and Jens Grossklags. 2023. The Effectiveness of Security Interventions on GitHub. In Proceedings of the 2023 ACM SIGSACConference on Computer and Communications Security (CCS '23), November26–30, 2023, Copenhagen, Denmark. ACM, Copenhagen, DK, 17 pages.

6. Lehtonen T, Suonsyrjä S, Kilamo T, Mikkonen T. Defining metrics for continuous delivery and deployment pipeline. In: Nummenmaa J, Sievi-Korte O and Mäkinen E (eds) Proceedings of the 14th symposium on programming languages and software tools (SPLST'15), Tampere, Finland, October 9–10, 2015, vol.1525 of CEUR workshop proceedings; 2015. pp.16–30, CEUR-WS.org

7. Ana Filipa & Zenha-Rela, M´ario. (2021). Monitoring CI/CD Workflow Using Process Mining. SN Computer Science. 2.10.1007/s42979-021-00830-2

8. Yang R., Cai J., Han X., "Poster: TaintGrep: A Static Analysis Tool for Detecting Vulnerabilities of Android Apps Supporting User-defined Rules," Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 2022, pp. 3507-3509.

9. Rangnau T., Buijtenen R. V., Fransen F. and Turkmen F. "Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines,"EDOC '20, 2020, pp. 145–154.

10. Сравнительный анализ и выбор статических анализаторов безопасности кода / Марков А.С., Антипов И.С., Арустамян С.С., Магакелова Н.А. // Вопросы кибербезопасности. 2024. № 5 (63). С. 79-88.

11. Тулеубаева А.А., Камолов А.Б., Рычков В.А. Современные методологии разработки безопасного программного обеспечения. М.: Цифровая экономика в контексте национальной безопасности материалы IV международной научно-практической конференции, 2022, с. 97-105.

Approaches for improving the efficiency of application security at the stage of software design and integration

Marchenkov S.D.[114], **Marochkin I.S.**[115], **Barzin A.A.**[116], **Bykov A.Y.**[117]

Abstract. Constant changes in the approaches of the organization of application security testing determine the course of development of technologies and methods of training employees to work with a large set of testing tools. The article discusses the methods of using the GitFlic software development platform for training information security specialists, methods for developing software testing skills. The advantages and disadvantages of using the development platform and version control system by students and teachers are listed.

Keywords: version control system, secure development platform, collaboration, secure development, version control system.

[114] Sergey Marchenkov, Ph.D. student, Bauman Moscow State Technical University, Moscow, marchenkovsd@bmstu.ru
[110] Marochkin Igor, student, Bauman Moscow State Technical University, Moscow, marochkinis@student.bmstu.ru
[111] Barzin Anatoly, student, Bauman Moscow State Technical University, Moscow, barzin.anatoly@yandex.ru
[112] Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, Москва, abykov@bmstu.ru

УДК 004.056.5(07)

Фильтрация трафика в межсетевом экране промышленного назначения

Медведев Н.В.[118]

Аннотация. В работе проанализированы актуальные технологии, применяемые в межсетевом экранировании промышленных сетей, предложены алгоритмы фильтрации сетевого трафика, выполнено сравнение схем обработки данных в части фильтрации трафика, определены практики по проектированию, эксплуатации и разработке межсетевых экранов промышленного назначения, сформулирована математическая постановка задачи разработки фильтра, проведено имитационное моделирование работы фильтра, выполнено функциональное тестирование разработанного программного обеспечения;

Ключевые слова: межсетевой экран типа Д, технологии межсетевого экранирования, фильтр трафика, преобразование сетевых адресов

В начале развития информационных технологий промышленные сети строились по централизованной схеме с одним мощным вычислительным устройством и обширной кабельной сетью для подключения оконечных устройств [1]. Подобная архитектура обуславливалась высокой стоимостью вычислительной техники того времени. Увеличение количества производимой цифровой техники привело к снижению стоимости вычислительных устройств, из-за чего стало экономически эффективным внедрение на предприятии ряда интеллектуальных устройств связи с объектом, объединенных в единую сеть передачи данных.

Современные промышленные вычислительные и управляющие сети представляют собой распределённые системы управления, связывающие различные датчики, исполнительные механизмы, промышленные контроллеры, при построении которых необходимо учитывать, что технологии взаимодействия отдельных компонентов друг с другом основаны на использовании вычислительных сетей.

Автоматизация современных предприятий представляет собой сложный и длительный процесс. Зачастую для достижения целей автоматизации используется оборудование разных производителей, что обуславливается экономическими соображениями.

Объединение устройств одного производителя в единую цифровую сеть обычно не вызывает проблем, так как их программное и аппаратное обеспечение разработано с учетом совместимости. Однако, при построении сети из устройств разных производителей необходимо обеспечить сопряжение их работы на программном и аппаратном уровнях.

Исходя из вышеизложенного при построении промышленных сетей необходимо учитывать следующие принципы [2]:

- **взаимосвязанность**: свободное подключение устройств разных производителей;
- **совместимость**: сеть должна работать с компонентами разных поставщиков;
- **взаимозаменяемость**: устройства, подключённые к сети, имеют аналоги от других производителей.

Промышленные сети в силу специфики применения должны отвечать ряду строгих требований [1, 2]:

- жёсткая детерминированность (предсказуемость) поведения;

[118] Медведев Николай Викторович, к.т.н., доцент, МГТУ им. Н.Э. Баумана, г. Москва, medvedevnick54@yandex.ru

• обеспечение функций реального времени;

• работа на длинных линиях с использованием недорогих физических сред (например, витая пара);

• повышенная надежность физического и канального уровней передачи данных для работы в промышленной среде (например, при больших электромагнитных помехах);

• наличие специальных высоконадежных механических соединительных компонентов;

• возможность организации питания оборудования по кабельной системе

В Требованиях ФСТЭК от 28 апреля 2016 г. N 240/24 выделен межсетевой экран уровня промышленной сети (тип «Д») – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами [3, 4]. Межсетевые экраны типа «Д» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, Industrial Ethernet и (или) иные протоколы).

Согласно профилю защиты межсетевых экранов в их функциональные возможности входит [5-9]:

• возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации (в том числе исполнительных устройств) и всех операций передачи контролируемой МЭ информации к узлам автоматизированной системы управления и от них;

• возможность обеспечения фильтрации для всех операций перемещения через МЭ информации к узлам автоматизированной системы управления и от них;

• возможность обеспечения фильтрации для всех операций перемещения через МЭ информации к узлам автоматизированной системы управления и от них;

• возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации: промышленные протоколы, которые используются для взаимодействия.

Фильтр трафика можно представить, как одноканальную систему массового обслуживания с ограниченной очередью, допустимой, если она не превышает числа $m > 0$ [10, 11].

Состояния пакетного фильтра будут нумероваться по числу сетевых пакетов, находящихся в буфере фильтра, т. е. S_k — состояние фильтра, когда в его буфере находится k пакетов:

S_0 — фильтр свободен: буфер пуст, очереди нет;

S_1 — фильтр занят, обслуживается один сетевой пакет, очереди нет;

S_2 — фильтр занят, обслуживается один сетевой пакет, один сетевой пакет находится в буфере;

S_3 — фильтр занят, две сетевых пакета стоят в очереди; …;

S_{m+1} — фильтр занят, m сетевых пакетов находятся в буфере, т.е. все допустимые места в буфере заняты, очередному пакету, поступившему в фильтр, будет отказано в обслуживании.

Под буфером понимается структура данных, которая хранит пакеты до начала их обработки фильтром и работает по принципу обслуживания в порядке очереди. Принцип обслуживания в порядке очереди может быть описан следующим образом: пакеты помещаются в буфер в порядке их прибытия, первый пакет становится головным, в то время как остальные, которые прибывают после, добавляются в конец. Когда фильтр переходит в состояние готовности, то он сначала обрабатывает самый первый пакет в списке, затем второй и так далее до тех пор, пока буфер не будет пуст [12].

Размеченный граф системы представлен на рисунке 1

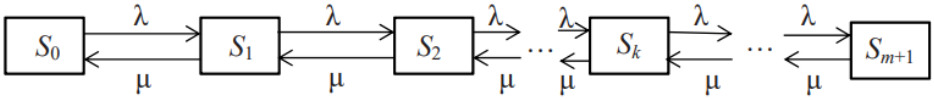


Рис. ***Error! No text of specified style in document.****. Схема размеченного графа системы*

Пакеты поступают в фильтр в соответствии со стационарным пуассоновским процессом со скоростью λ. Затем каждый пакет обрабатывается фильтром, который решает, пропустить его или отбросить. Решение фильтра основано на атрибутах пакета, таких как IP-адреса источника и назначения, порты и протокол, и осуществляется со скоростью μ.

Данная система имеет конечное число состояний, поэтому из каждого состояния за конечное число шагов можно перейти в любое другое состояние. Значит, предельные вероятности всех состояний системы существуют. Составим выражение для вычисления предельной вероятности состояния S_0 (1).

$$p_0 = (1 + \rho + \rho^2 + \cdots + \rho^{m+1})^{-1}$$ (**Error! No text of specified style in document.**)

где $\rho = \frac{\lambda}{\mu}$

При применении фильтра пакетов в рамках контроля информационных потоков внутри информационной системы, в большинстве случаев, применяют набор из так называемых правил фильтрации.

При первом подходе каждое правило рассматривается как отдельный объект. Система фильтрации проверяет каждый фильтр последовательно для каждого сетевого пакета, при этом проверка происходит без использования информации, полученной о полях пакета из предыдущего сопоставления. Стоимость идентификации совпадающего правила растет линейно с увеличением их количества. Такая стоимость неприемлема в системах, которые задают большое количество правил.

В рамках промышленной сети невозможно ограничиться парой правил, поэтому скорость обслуживания фильтром пакета μ не будет равняться скорости поступающих пакетов λ, и как следствие $\rho \neq 1$.

В данных условиях предельная вероятность состояния S_0 будет вычисляться следующим образом (2):

$$p_0 = \frac{1-\rho}{1-\rho^{m+2}}$$ (1)

Предельные вероятности остальных состояний системы вычисляются соответственно (3):

$$p_1 = \rho \cdot p_0, p_2 = \rho^2 \cdot p_0, \dots, p_{m+1} = \rho^{m+1} \cdot p_0$$ (**Error! No text of specified style in document.**.2)

Показатели эффективности для рассматриваемого случая будут вычисляться по следующим формулам:

- Вероятность отказа пакету в обслуживании (4):

$$P_{\text{отк}} = \rho^{m+1} \cdot p_0 = \rho^{m+1} \cdot \frac{1-\rho}{1-\rho^{m+2}}$$ (3)

- Относительная пропускная способность системы (5):

$$Q = 1 - \rho^{m+1} \cdot p_0 = \frac{1-\rho^{m+1}}{1-\rho^{m+2}}$$ (4)

- Абсолютная пропускная способность системы (6):

$$A = \lambda \cdot (1 - \rho^{m+1} \cdot p_0) = \lambda \cdot \frac{1-\rho^{m+1}}{1-\rho^{m+2}} \quad (5)$$

• Вероятность наличия очереди (7):

$$P_{\text{оч}} = \rho^2 \cdot \frac{1-\rho^m}{1-\rho} \cdot p_0 = \rho^2 \cdot \frac{1-\rho^m}{1-\rho^{m+2}} \quad (6)$$

• Среднее число пакетов, находящихся под обслуживанием, или средняя загрузка канала (8):

$$L_{\text{об}} = \bar{k} = k_{\text{заг}} = 1 - p_0 \quad (7)$$

• Среднее число пакетов, стоящих в очереди (9):

$$L_{\text{оч}} = \rho^2 \cdot \frac{1-\rho^m \cdot (m+1-m \cdot \rho)}{(1-\rho)^2} \cdot p_0 = \rho^2 \cdot \frac{1-\rho^m \cdot (m+1-m \cdot \rho)}{(1-\rho) \cdot (1-\rho^{m+2})} \quad (8)$$

• Среднее число пакетов в системе (10).

$$L_{\text{сист}} = L_{\text{об}} + L_{\text{оч}} \quad (9)$$

• Среднее время пребывания пакетов в очереди, под обслуживанием и в системе (11-13):

$$T_{\text{оч}} = \frac{L_{\text{оч}}}{\lambda} \quad (10)$$

$$T_{\text{об}} = \frac{L_{\text{об}}}{\lambda} \quad (11)$$

$$T_{\text{сист}} = \frac{L_{\text{сист}}}{\lambda} \quad (12)$$

Данная система будет функционировать без возникновения отказов, если в системе не будет накапливаться очередь, то есть необходимо, чтобы в среднем запросы в системе обслуживались быстрее, чем они поступают: $\mu \geq \lambda$.

В алгоритме фильтрации для каждого захваченного пакета на основе информации заголовка вычисляется его ключевое значение и выполняется сопоставление с индексным файлом [13]. Если найдено правильное совпадение, это указывает на то, что конкретный пакет с такой же информацией заголовка ранее поступал в сеть, и поэтому выполняется дальнейший поиск в файле журнала и на основе поля принятия решения принимается действие [14].

Весь процесс подбора показан на рисунке 2.

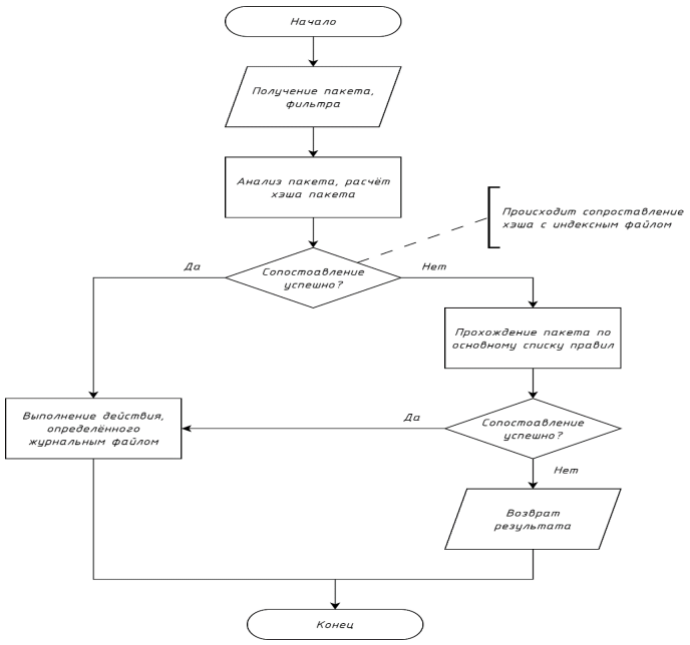


Рис. ***Error! No text of specified style in document.****. Блок-схема предлагаемого алгоритма фильтрации*

Во время реализации поддерживаются три файла: основной файл, содержащий основные правила пакетного фильтра, файл журнала, который является подмножеством основного набора правил, содержащего недавно захваченные пакеты, и индексный файл, содержащий хэш-значения. Для каждого захваченного пакета вычисляется значение ключа на основе информации его заголовка, и выполняется сопоставление с индексным файлом.

Изначально индексный файл и файл журнала пусты, поэтому для первого пакета в сетевом потоке выполняется поиск в файле журнала и на основе поля принятия решения принимается действие. При обнаружении точного совпадения вычисляется его хэш-значение и делается соответствующая запись в индексном файле и в файле журнала. Для всех последующих пакетов, принадлежащие одному и тому же потоку, выполняется сопоставление путям поиска записи в файле журнала вместо основного набора правил. Таким образом, каталогизируя информацию о недавно полученных пакетах, сокращается время поиска для сканирования основного набора правил [14]. Здесь файл журнала выступает в качестве подмножества основного набора правил фильтра траффика. Количество правил в файле журнала меньше по сравнению с правилами в основном файле, поэтому очевидно, что время, необходимое для сканирования файла журнала, будет меньше по сравнению со временем, необходимым для сканирования основного набора правил.

Вывод

Для достижения наиболее эффективной фильтрации с минимизацией задержек была поставлена математическая задача и предложены пути её решения. Задача основана на применении теории массового обслуживания, что позволяет моделировать поведение пакетного фильтра и оптимизировать его производительность.

Предложенные подходы решения могут быть использованы для проектирования эффективного пакетного фильтра, оптимизирующего качество фильтрации и эффективность обработки и обеспечивающего защиту промышленных систем от кибератак, гарантируя безопасность и надежность контролируемых процессов [11].

Применение адекватного и корректного математического метода массового обслуживания для постановки и решения поставленной задачи практически подтверждают достоверность предлагаемого научного решения.

Литература

1. Борисов, А.М. Основы построения промышленных сетей автоматики: учебное пособие / А.М. Борисов. – Челябинск: Изд. Центр ЮУрГУ. – 2022. – 108 с.

2. Сахнюк, А.А. Промышленные сети. / А.А. Сахнюк, А.М. Литвин // ПиКАД. – 2018. – №2. – С. 6–8.

3. Барабанов А.В., Марков А.С., Цирлов В.Л. Испытания межсетевых экранов по требованиям безопасности информации. - М.: НЦПИ Минюста России, 2017. 44 с.

4. Тестирование межсетевых экранов по требованиям безопасности информации / Барабанов А.В., Марков А.С., Цирлов В.Л. – М.: МГТУ им.Н.Э.Баумана, 2021. – 53 с.

5. Designing Firewalls: A Survey / A. Keromytis, V. Prevelakis // Network Security: Current Status and Future Directions. – 2016. – С. 33–49.

6. Scarfone, K. Guidelines on Firewalls and Firewall Policy / K. Scarfone, P. Hoffman // NIST : электронный журнал. – URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf. – Дата публикации: 09.2009.

7. Special-Purpose IP Address Registries / M. Cotton, L. Vegoda, R. Bonica, B. Haberman // RFC 6890 : электронный журнал. – URL: https://www.rfc-editor.org/rfc/rfc6890. – Дата публикации: 04.2013. – ISSN 2070-1721

8. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing / P. Ferguson, D. Senie // RFC 2827: электронный журнал. – URL: https://www.rfc-editor.org/rfc/rfc2827. – Дата публикации: 05.2020.

9. Certifying spoofing-protection of firewalls / C. Diekmann, L. Schwaighofer, G. Carle // 11th International Conference on Network and Service Management (CNSM). – 2015. – С. 168–172.

10. Теория массового обслуживания: учебное пособие / М.А. Плескунов; Министерство науки и высшего образования РФ, Урал. федер. ун-т.— Екатеринбург: Изд-во Урал. ун-та, 2022. — 264 с.

11. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. -М.: НИИ РиЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.

12. The BSD packet filter: A new architecture for user-level packet capture / S. McCanne, V. Jacobson // USENIX Winter. – 1993. – С. 259–270.

13. Efficient packet demultiplexing for multiple endpoints and large messages / M. Yuhara, B. N. Bershad, C. Maeda, J. Eliot, B. Moss // USENIX Winter. – 1994. – С. 153–165.

14. Pathfinder: A pattern-based packet classifier / M. L. Bailey, B. Gopal, M. A. Pagels, L. L. Peterson, P. Sarkar // Operating Systems Design and Implementation. – 1994. – С. 115–123.

Traffic filtering in an industrial firewall

Nikolay Medvedev[119]

Annotation. The paper analyzes current technologies used in the inter-network shielding of industrial networks, proposes algorithms for filtering network traffic, compares data processing schemes in terms of traffic filtering, defines practices for the design, operation and development of industrial firewalls, formulates a mathematical formulation of the filter development problem, simulates the filter operation, performs functional testing of the developed software security.

Keywords: D-type firewall, firewall technology, traffic filter, network address translation

[119] Nikolay Medvedev, Ph.D, Associate Professor, BMSTU, Moscow, medvedevnick54@yandex.ru

УДК 004.056

Механизм создания доверия к социально значимым информационным системам

Минзов А.С.[120],Невский А.Ю., Баронов О.Р., Токарева Н.А.

Развитие государственных информационных систем для населения привело к появлению нового класса этих систем, который определен как «социально значимые информационные системы» (СЗИС)[121]. Кроме обеспечения этих систем требованиями по их функциональности и безопасности возникает также необходимость создания механизма доверия к ним. В докладе рассматриваются механизмы создания абсолютного доверия на основе концепции Zero Trust Architecture (ZTA).

Ключевые слова: модель угроз, архитектура безопасности, ZTA.

Введение

В настоящее время социально значимые информационные системы требуют повышенного внимания к доверию к ним общества и системы государственного и муниципального управления. Анализ показал, что существующие механизмы определения оценочного уровня доверия не гарантируют полного доверия к СЗИС, так как не учитывают полный комплект угроз, относящихся к доверию этим системам [1, 2]. Доверие к СЗИС рассматривается нами как многокомпонентная функция, значения которой определяются медийной частью и уровнем организационно-технической реализации технологий обеспечения доверия к СЗИС [3]:

$$D=f(d_m) \oplus f(d_t), \quad (1)$$

где $f(d_m)$ - функция оценки уровня доверия общества к ИТ –проекту за счет использования СМИ и других медийных средств [4]. Это направление мы не рассматриваем.

$f(d_t)$ - функция оценки уровня доверия общества к проекту СЗИС за счет организационно-технических мер на этапах проектирования и разработки архитектуры информационной безопасности, функционального тестирования, статического и динамического анализа кода, внедрения проекта СЗИС и поддержания его безопасного состояния.

Существующие механизмы обеспечения доверия $f(d_t)$ основаны на концепции стандарта 15408 (3 часть) и стандарта по безопасному проектированияю ИТ[122].

Основные принципы стандарта 15408 состоят в том, что следует четко сформулировать угрозы безопасности (класс APE, семейство SPD), положения политики безопасности организации и продемонстрировать достаточность предложенных мер безопасности [5]. Основной способ достижения доверия $f(d_t)$ основан на проведении его оценки (всего 6 оценочных уровней доверия). Методы оценки основаны на анализе процессов, требований к ним, верификации доказательств достижения целей безопасности.

[120] Минзов Анатолий Степанович, д.т.н, профессор, НИУ «МЭИ», каф. БИТ, Москва, minzovas@mpei.ru
Невский Александр Юрьевич, к.т.н., доцент, НИУ «МЭИ», зав.кафедрой БИТ, Москва, nevskyau@mpei.ru
Баронов Олег Рюрикович, к.т.н.,доцент, НИУ «МЭИ», кафедра БИТ, Москва, baronovor@mpei.ru
Токарева Надежда Александровна, к.ф-м.н, доцент, Университет «Дубна», зав.кафедрой ИТ, tokareva@uni-dubna.ru

[121] Постановление Правительства РФ от 29 декабря 2021 г. N 2531 "Об утверждении Правил ведения перечня отечественных социально значимых информационных ресурсов"

[122] ГОСТ Р 56939. Защита информации. Разработка безопасного программного обеспечения. Общие требования -2024 г.

Доверие к техническим средствам ИТ-проектов обеспечивается транзитивно через посредников (сертифицированных технических средств, удостоверяющих центров и т.д.). Но, к сожалению, эти меры не дают нам гарантии полного доверия к СЗИС.

Концепция ZTA и ее реализация

Одним из механизмов решения этой задачи является концепция ZTA [4, 6, 7], которая позволяет разработать архитектуру информационной безопасности ИТ на основе системного анализа компонентов информационной системы с позиций доверия к процессам сбора, обработки, передачи и хранения информации, принятия решений и контроля всех процессов. Пример такого анализа приведен на рис.1.

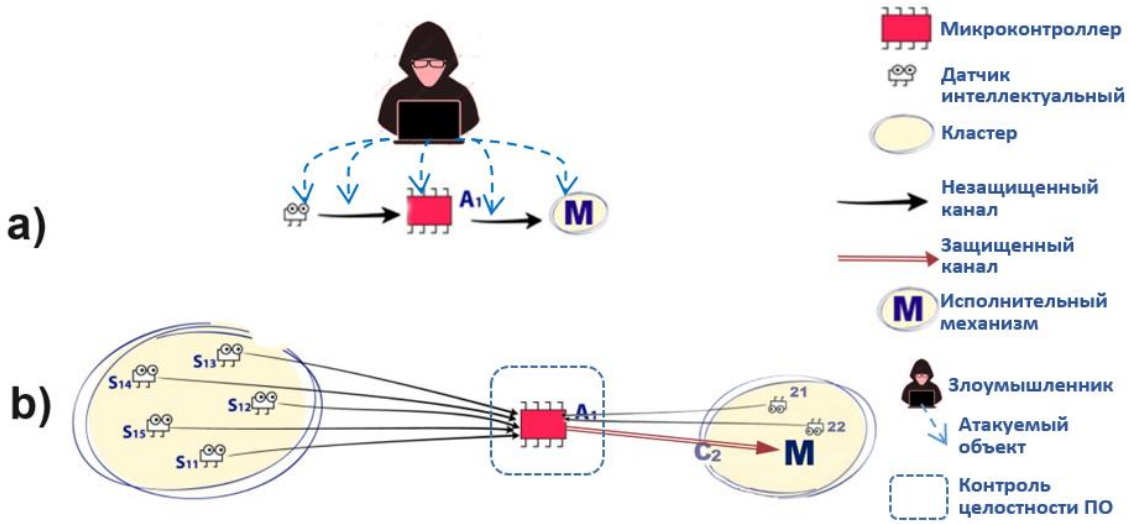


Рис.1.Пример реализации концепции ZTA

На рис.1a представлена типичная схема управления киберфизичской системой, состоящей из датчика, незащищенного канала к микроконтроллеру и незащищенного канала к исполнительному мезанизму. Такая схема не обеспечивает доверие к управлению КФС. На рис.b представлен (вариант) этой же схемы управления с полным уровнем доверия. На ней увеличено количество датчиков и каналов передачи их показаний, контролируется целостность ПО микроконтроллера, создается защищенный канал для управления исполнительным механизмом (М) и включает дополнительно два датчика контроля корректности его работы.

Условия «абсолютного» доверия к ИТ-проекту СЗИС

Пусть x_i – элемент информационной структуры ИТ-проекта ($x_i \in X$), в котором происходит обработка информации в соответствии политикой безопасности. Определим x_i как:

$$x_i=\{a_i, t_i, d_i, m_i\}, \quad (2)$$

где a_i– функция обработки информации;

t_i – угроза, влияющая на уровень доверия к СЗИС;

d_i – метрика измерения уровня доверия ($d_i \in D$:$0 \le d_i \ge 1$). Значение d_i может быть задано в ajhvt лингвистической переменной;

m_i– мера по снижению угрозы.

Оценка уровня доверия всего ИТ-проекта $f(d_t)$ может быть представлена в следующем виде:

$a)$ $\forall x_i, (m_i \in M), (t_i \in T), (d_i \in D) \rightarrow (f(d_t)=1 : T=\emptyset)$ «абсолютное» доверие. (3)

$b)$ $\forall x_i, (\exists t_i : t_i \in T, m_i \in M) \rightarrow (f(d_t)=min\{d_i\})$ реальное доверие. (4)

Выражения (3) и (4) действительны при условии выполнения требований к классу (APE) семейства (SPD) и требований к архитектуре информационной безопасности (ADV_ARC) стандарта 15408 (часть 3).

Выводы

1. Основное достоинство подобных архитектур ИС заключается в том, что для них не требуется применять механизм доказательства доверия, что требуется для оценочных уровней доверия от ОУД-4 до ОУД-1, так как здесь используется очевидная логика вывода: если каждый элемент системы построен на абсолютном доверии, то и вся информационная система имеет тот же уровень доверия. Однако, для более сложных ИС это не вполне очевидно и требует реализаций дополнительных функций доверия при межсистемном взаимодействии различных подсистем, в том числе используя транзитивный подход к проектированию архитектуры безопасности.

2. Для практической реализации СЗИС и КИИ такой подход потребует изменения концепций проектирования и модернизации SCADA – систем путем включения в их состав компонентов, решающих типовые задачи доверия к компонентам информационных систем.

Литература

1. Веселов Ю.В., Липатов А.А. Доверие в организации: методологические основания исследования в экономике, социологии и менеджменте // Российский журнал менеджмента. 2015. №4.

2. Деньжаков А. Ю. Анализ доверия как формализуемой концепции / А. Ю. Деньжаков, С. В. Шибанов. // Молодой ученый. — 2011. — № 9 (32). — С. 29-33.

3. Минзов А.С., Невский А.Ю., Баронов О.Р. Механизм создания системы доверия к социально значимым общественным информационным системам - Доклад на конференции Рускрипто-23. URL: https://ruscrypto.ru/resource/archive/rc2023/files/15_minzov_nevskiy_baronov.pdf

4. Минзов А.С. e-PR. Основы теории, модели коммуникаций, социальные сети, информационные войны: Монография. - М.: ВНИИгеосистем, 2015. – 110 с.

5. Оценка соответствия средств защиты информации "общим критериям" / Барабанов А.В., Марков А.С., Цирлов В.Л. // Информационные технологии. 2015. Т. 21. № 4. С. 264-270.

6. Scott R., Oliver B., Stu M., Sean C. NIST Special Publication 800-207 "Zero Trust Architecture" URL https://doi.org/10.6028/NIST.SP.800-207, August 2020.

7. Ross S. J. Information Security Architecture: From Access Paths to Zero Trust // ISACA Journal. – 2024. – №. 2.

Mechanism for Creating Trust in Socially Important Information Systems

MinzovA.S., Nevsky A.U., Baronov O.R., Tokareva N.A.[123]

Abstract*. The report discusses mechanisms for creating absolute trust in socially important information systems based on the Zero Trust Architecture (ZTA) concept.*

Keywords: *threat model, security architecture, ZTA.*

[123] MinzovA.S., Dr.Sc., Professor, MPEI, Moscow, minzovas@mpei.ru,
Nevsky A.U., PhD, Associate Professor, MPEI, Moscow, nevskyau@mpei.ru
Baronov O.R., PhD, Associate Professor, MPEI, Moscow, baronovor@mpei.ru
Tokareva N.A., PhD, Associate Professor, Universite Dubna, tokareva@uni-dubna.ru

УДК 004.056

Роль искусственного интеллекта в предотвращении фишинговых атак

Мишина Л.О.[124]

Аннотация. В статье рассмотрено понятие фишинга как вида мошенничества, выделены основные виды фишинга. Определены методы борьбы с фишингом посредством применения искусственного интеллекта, а также преимущества и недостатки применения искусственного интеллекта в борьбе против фишинговых атак.

Ключевые слова: интернет, искусственный интеллект, фишинг, машинное обучение, кибербезопасность.

Введение. Фишинг как один из популярных видов мошенничества, заключается в отправке поддельных электронных писем с целью обмана пользователей, а также получения их личной информации, например, это может быть поддельное сообщение от банка с просьбой срочно обновить пароль, чтобы не потерять свои средства. Для предотвращения популярной и постоянно изменяющейся атаки, необходимо использовать популярные современные технологии – искусственный интеллект. Использование автоматизации и искусственного интеллекта (ИИ) улучшается эффективность реакции на угрозы, обнаружение аномалий и управление инцидентами.

Целью данной статьи является анализ методов искусственного интеллекта для предотвращения фишинговых атак.

Изложение основного материала

Фишинг – представляет собой вид кибератаки, целью которой является мошенническое получение конфиденциальных данных пользователя, например, логин, пароль, номер банковской карты, путем маскировки атакующего под доверенное лицо или организацию. Зачастую, атаки осуществляются через электронные письма, сообщения в социальных сетях, звонки от представителей банка и других организаций, а также через фальшивые веб-сайты, имитирующие настоящие.

Методы борьбы с фишингом разнообразны и включают в себя различные подходы – от традиционных до более современных технологий, основанных на анализе содержания и поведенческих характеристик. Одними из самых распространенных методов являются:

−черные и белые списки – использование баз данных со списками известных фишинговых и доверенных сайтов для фильтрации трафика;

−эвристический анализ – применение правил для оценки вероятности фишинга на основе структуры сайта и проверка сертификатов безопасности;

−машинное обучение – применение алгоритмов для анализа и обучения на основе предыдущих инцидентов фишинговых атак, что позволит автоматически обнаружить новые угрозы.

ИИ способен анализировать большие объемы данных с высокой точностью, что делает его идеальным инструментом для выявления и предотвращения фишинговых атак. Алгоритмы машинного обучения, являющиеся частью ИИ, могут обучаться на примерах реальных фишинговых сообщений, что позволяет им со временем становиться только эффективнее в идентификации потенциально опасного контента.

Особенно значимым использованием ИИ, является анализ текстового и визуального контента в электронных письмах и на веб-сайтах. Системы, на основе ИИ могут распознавать мошеннические призывы, скрытые в тексте, и обнаруживать поддельные

[124] Мишина Лилия Олеговна, студентка 3 курса направления подготовки 09.03.03 «Прикладная информатика» Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО «Крымский федеральный университет им. В.И. Вернадского» в г. Ялте, lilimish16012004@mail.ru

логотипы или интерфейсы, что часто используется в фишинговых атаках для обмана пользователей.

Кроме того, алгоритмы могут анализировать структуру веб-сайтов и их доменные имена, выявляя подозрительные признаки, такие как необычное использование символов или отклонение от обычных паттернов дизайна.

Использование ИИ также включает в себя мониторинг и анализ моделей поведения пользователей и их взаимодействия с электронной почтой и веб-сайтами. Это позволяет выявлять аномалии, которые могут указывать на попытку фишинговой атаки, например, необычно высокую частоту запросов к определенным ресурсам.

Системы на основе ИИ могут адаптироваться к новым стратегиям мошенников, обеспечивая более надежную защиту для пользователей [1]. Рассмотрим основные виды фишинга, которые представлены в табл. 1.

Таблица 1.

Виды фишинга

Виды фишинга	Описание	Примеры
Почтовый фишинг (Phishing emails)	Отправка ложных электронных писем, выдающих себя за сообщения от доверенных источников	Письмо просит перейти по ссылке и ввести учетные данные на поддельном сайте
Фишинг через веб-сайты (Phishing websites)	Создание поддельных веб-сайтов, имитирующих легитимные ресурсы, для получения личных данных	Поддельная страница банка, запрашивающая у пользователя ввод его банковских данных
SMS-фишинг (SMS-phishing)	Использование текстовых сообщений для мошеннических уведомлений и запросов конфиденциальной информации	SMS с предложением перейти по ссылке для обновления пароля на вымышленном сайте

Данная таблица раскрывает понимание видов фишинга включая конкретные примеры и контексты использования, но помимо видов фишинга, следует рассмотреть пример кода на языке программирования Python с использованием библиотеки «smtplib» для отправки электронного письма [2]:

```
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

def send_phishing_email(sender_email, send-er_password, recipient_email,
subject, body):
# Настройки SMTP сервера
smtp_server = 'smtp.example.com'
smtp_port = 587

# Создание объекта сообщения
message = MIMEMultipart()
message['From'] = sender_email
message['To'] = recipient_email
message['Subject'] = subject

# Добавление тела письма
message.attach(MIMEText(body, 'plain'))

# Подключение к SMTP серверу и отправка письма
with smtplib.SMTP(smtp_server, smtp_port) as server:
server.starttls()
```

```
    server.login(sender_email, sender_password)server.sendmail(sender_email,
recipi-ent_email, message.as_string())
    # Пример использования
    sender_email = 'your_email@example.com'
    sender_password = 'your_email_password'
    recipient_email = 'victim@example.com'
    email_subject = 'Important Security Update'
    email_body = 'Dear User, we need you to update your security information.
Please click on the link: malicious-website.com'
```

# Отправка поддельного письма
send_phishing_email(sender_email, sender_password,recipient_email, email_subject, email_body)

Каждый раз мошенники стараются найти и создать новые возможности для похищения личных аккаунтов и средств людей, поэтому, следует не переходить по незнакомым ссылкам и не выполнять другие условия от незнакомого адресата. С внедрением искусственного интеллекта в повседневную жизнь, появились новые угрозы для информационной безопасности.

Мошенники могут использовать искусственный интеллект для создания более убедительного контента, чтобы убедить жертву в том, что они хорошо разбираются в теме.

Также, в мошеннических целях, с помощью искусственного интеллекта могут быть имитированы мышление человека, которого он клонирует, его привычки, словарный запас и подход к информации.

Системы искусственного интеллекта склонны к ложным срабатываниям, так как высокая активность в сети Интернет может быть ошибочно принята как фишинговая атака. А сами данные о фишинговых атаках могут быть разнообразными и неоднородными, что создает сложности в обучении модели, так как системе необходимо учитывать различные формы фишинга и их уникальные характеристики.

Говоря о преимуществах и недостатках применения искусственного интеллекта в борьбе против фишинговых атак, можно выделить следующие [3], представленные в табл. 2.

Таблица 2.

Преимущества и недостатки применения ИИ в борьбе против фишинговых атак

Преимущества	**Недостатки**
Быстрое обнаружение фишинговых атак	Возможность применения в разработке атак
Способность учиться на ошибках	Ложное срабатывание
Выявление новых паттернов атак	Сложность обучения
Экономия времени и ресурсов	Необходимость большого объема данных

В развитии ИИ для обнаружения фишинговых атак прослеживаются значительные проблемы и ограничения.

Во-первых, эффективность ИИ зависит от объема и качества обучающих данных.

Во-вторых, мошенники постоянно разрабатывают новые методы обхода систем обнаружения, вследствие чего ИИ должен постоянно обновляться и адаптироваться.

В-третьих, существует проблема ложноположительных срабатываний, когда законные сообщения ошибочно классифицируются как фишинговые, что может привести к недовольству пользователей и потере важных сообщений [1, 4].

Ещё одно ограничение связано с необходимостью баланса между приватностью пользователей и эффективностью обнаружения атак [5]. Применение ИИ также требует значительных вычислительных ресурсов, особенно при обработке больших массивов

данных в реальном времени. Это может стать барьером для малых и средних предприятий, имеющих ограниченные технологические и финансовые возможности.

Кроме того, эффективность ИИ в обнаружении фишинга может снижаться из-за сложности идентификации новых и уникальных форм атак, которые не были представлены в обучающем наборе данных.

Для минимизации риска фишинговых атак на различные организации необходимо анти-фишинговое программное обеспечение на основе искусственного интеллекта, способное выявлять и блокировать фишинговый контент во всех коммуникационных службах организации (электронная почта, приложения для повышения производительности и т.д.) и платформах (рабочие станции сотрудников, мобильные устройства и т.д.) [6, 7].

Такой комплексный охват необходим, поскольку фишинговый контент может поступать по любому носителю, а сотрудники организаций могут быть более уязвимы к атакам при использовании мобильных устройств.

Выводы

Таким образом, для защиты от фишинговых атак необходима комплексная стратегия борьбы с фишингом, включающая ознакомление населения с принципами борьбы с фишингом. Решение для обнаружения фишинга на основе искусственного интеллекта может отфильтровать большинство фишинговых писем, снижая вероятность того, что человек попадется на одно из них и будет подвергнут атакам.

Литература

1. Киргизбаев, С. П. Использование искусственного интеллекта для распознавания и предотвращения фишинговых атак / С. П. Киргизбаев, В. П. Киргизбаев // Научные исследования студентов и учащихся: сборник статей XI Международной научно-практической конференции, Пенза, 20 марта 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 39-41. – EDN PSQIVC.

2. Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для СПО / А. Н. Баланов. — Санкт-Петербург, 2024. — 284 с. — ISBN 978-5-507-49251-0.

3. Перова, М. В. Преимущества и недостатки использования искусственного интеллекта в борьбе с фишинговыми атаками / М. В. Перова, З. А. Мансурова, В. Е. Безукладная // Современные тенденции развития общества: образование, коммуникация, психология: Сборник по итогам научно-практической конференции с международным участием, Ростов-на-Дону, 24 ноября 2023 года. – Ростов-на-Дону: Российская академия народного хозяйства и государственной службы при Президенте РФ, 2023. – С. 348-352.

4. Баланов, А. Н. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург, 2024. — 680 с. — ISBN 978-5-507-49562-7.

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

6. Ишмеева, А. С. Фишинг, как вид киберпреступности / А. С. Ишмеева // Актуальные проблемы раскрытия и расследования преступлений, совершаемых с использованием интернета: Сборник материалов Всероссийской научно-практической конференции, Белгород, 23 сентября 2021 года / Под редакцией Н.А. Жуковой. – ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»: Белгородский государственный национальный исследовательский университет, 2021. – С. 34-37. – EDN YBRCHL.

7. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа "phishing" на локальную компьютерную сеть // Вопросы кибербезопасности. 2021. № 2 (42). С. 17-25.

Научный руководитель или консультант: Таран Виктория Николаевна, кандидат технических наук, доцент кафедры математики и информатики Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО «Крымский федеральный университет им. В.И. Вернадского» в г. Ялте, victoriyayalta@gmail.com

The Role of Artificial Intelligence in Preventing Phishing Attacks

Mishina L.O. [125]

Abstract. The article examines the concept of phishing as a type of fraud, defines methods of combating phishing through the use of artificial intelligence, highlights the main types of phishing, as well as the advantages and disadvantages of using artificial intelligence in the fight against phishing attacks.

Keywords: Internet, artificial intelligence, phishing, machine learning, cybersecurity.

[125] Mishina Liliya Olegovna, 3rd year student of the program 09.03.03 "Applied Informatics" Humanitarian and Pedagogical Academy (branch) of the Federal State Autonomous Educational Institution of Higher Education "V.I. Vernadsky Crimean Federal University" in Yalta, lilimish16012004@mail.ru

УДК 004.056

Внутренний аудит безопасности конфигураций

Потапова А.С.[126]

Статистика атак на страны СНГ и в частности на Россию показывает острую необходимость принимать проактивные меры по защите отдельных сервисов и IT-инфраструктуры в целом. Требуется регулярная проверка системы на наличие уязвимых версий программного обеспечения (ПО), недостатков парольной политики, а также слабых сторон аутентификационных данных пользователей. Результаты внутреннего аудита должны быть использованы для улучшения настроек безопасности конфигураций и минимизации рисков информационной безопасности (ИБ). Анализ научных публикаций и различных источников, проведённый по теме исследования, выявил наличие проблемы в данной области. Рассмотрены и проанализированы методы проведения аудита ИБ, предложена технология точечной автоматической проверки безопасности конфигураций, а также способы по улучшению организации мероприятий, направленных на устранение проблем, выявленных проверкой.

Ключевые слова: информационная безопасность, парольная политика, словарные пароли, аудит ИБ, уязвимое ПО, аутентификация.

Введение

Кибербезопасность в современных компьютерных сетях становится все более актуальной проблемой. Согласно исследованиям Positive Technologies[127], количество кибератак на страны СНГ во втором квартале 2024 года увеличилось в 2,6 раза по сравнению с аналогичным периодом 2023 года.

Важно отметить, что эксплуатация уязвимостей в ПО уже пять лет подряд входит в тройку наиболее распространенных методов атак. В 2023 году 32% успешных атак были связаны с использованием уязвимостей[128]. Злоумышленники активно используют вредоносное ПО, которое сыграло ключевую роль в 60% успешных атак (рис. 1). Это может быть вызвано несвоевременным обновлением компонентов информационной системы (ИС) и наличием уязвимых версий программного обеспечени [1].

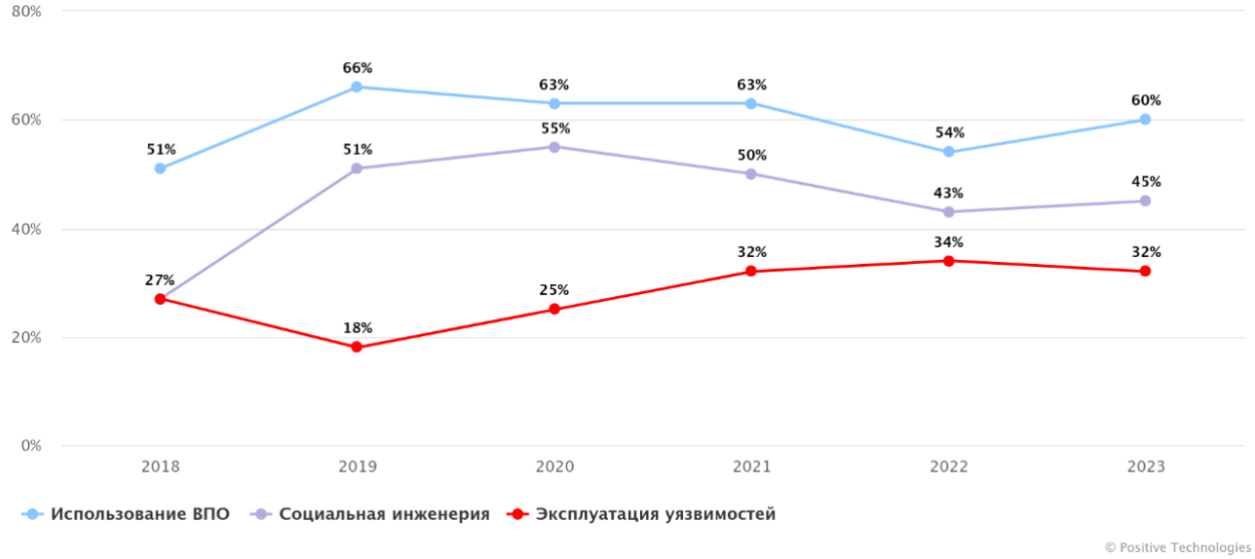


Рис.1. Топ-3 методов атак на организации

[126] Потапова Анастасия Сергеевна, Национальный исследовательский ядерный университет «МИФИ», Москва, PASer@mail.ru

[127] https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024

[128] https://www.ptsecurity.com/ru-ru/research/analytics/the-consequences-of-delays-in-remediating-vulnerabilities-2022-2023

В топ-10 актуальных уязвимостей по версии OWASP также входят ошибки идентификации и аутентификации, чем пользуются злоумышленники, проводя атаки методом перебора (Bruteforce) и подстановки учетных данных (рис. 2, 3). Успешных реализаций на их долю в 2022–2023 годах приходилось 10% всех выявленных уязвимостей, 11% из которых привели к компрометации учетных данных.

Рис.2. Распределение уязвимостей по категориям OWASP Top 10

Рис.3. Уязвимости, связанные с недостатками идентификации и аутентификации

Важно отметить, что брутфорс также входит в топ-10 обнаруженных атак и составляет 67,03% от всех угроз[129], выявленных защитным решением, за последний месяц (рис. 4). Также исследователи [2-11] отмечают, что ввиду сложности запоминания стойких паролей, пользователи придумывают словарные комбинации.

[129] https://statistics.securelist.com/ru/intrusion-detection-scan/month

После анализа научных статей [4, 5] сделан вывод, что применение словарных паролей облегчает злоумышленникам реализацию таких атак. Таким образом, данная проблема требует особого внимания.

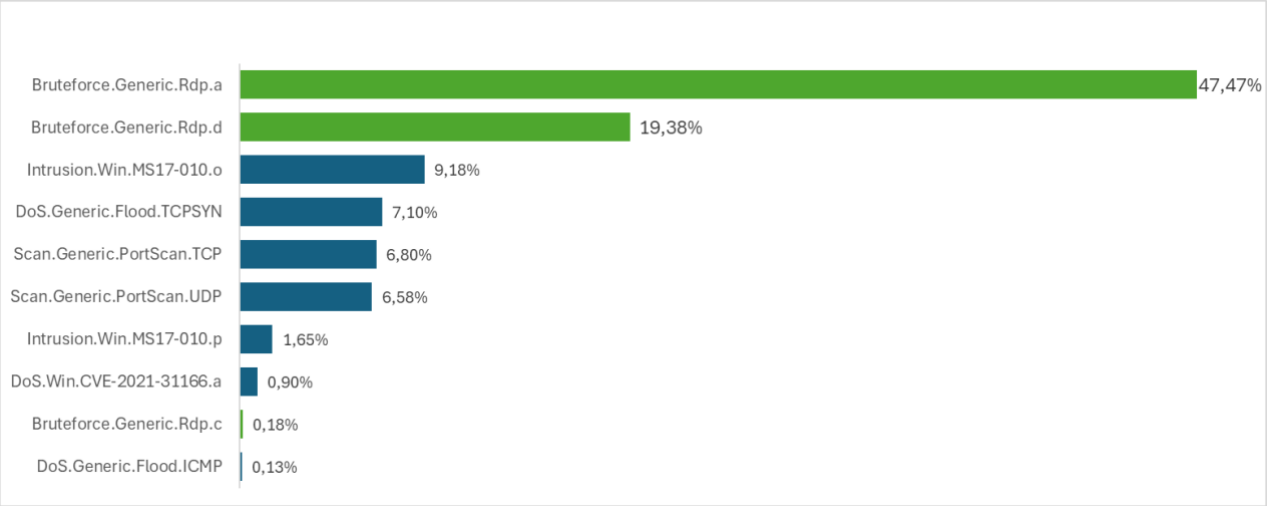


Рис.4. Топ-10 обнаруженных угроз, выданных защитным решением, за месяц

Постановка задачи

Цель исследования: разработать технологию аудита парольной политики, словарных паролей, ИС на наличие уязвимых версий ПО и подготовить рекомендаций по повышению эффективности мероприятий, направленных на устранение проблем, выявленных проверкой. Для достижения поставленной цели требуется решить следующие основные задачи:

1) анализ нормативно-правовой базы, регламентирующей проведение аудита ИБ, а также описывающей требования к объектам исследования;

2) анализ современных методов внутреннего аудита безопасности конфигураций ИС и выбор способа для достижения наилучшего результата на основе сравнительного анализа, метода принятия решений и экспертных оценок.

3) определение принципов безопасности конфигураций в контексте ИБ и анализ уязвимостей и угроз, возникающих при использовании словарных паролей, устаревшего ПО, а также неправильной парольной политики. При анализе используется теория вероятностей и математическая статистика, метод кластерного анализа;

4) разработка и автоматизация технологии для аудита парольной политики, словарных паролей и актуальных версий ПО;

5) разработка рекомендаций по повышению эффективности проведения мероприятий, нацеленных на устранение выявленных недостатков;

6) оценка эффективности разработанной технологии и предложенных подходов с использованием теории графов и математической статистики.

Решение задачи

С целью максимально упростить подготовку к аудиту и само его проведение было решено использование базовых, преднастроенных средств операционной системы (ОС). Практически все действия выполняются с помощью команд и командлетов powershell, а для ускорения некоторых задач используется язык программирования Python.

Часто для взлома паролей используются hashcat и John the Ripper. Но запуск этих утилит создает ненужную нагрузку на сеть, требует установки специализированных операционных систем, что может противоречить политики ИБ организации, а также предоставляет пароли в открытом виде, нарушая конфиденциальность проверки и этичные

нормы. Поэтому данные механизмы используются косвенно для расширения базы словарей и за пределами локальной вычислительной сети (ЛВС).

Для проверки словарных паролей осуществляется выгрузка ntds.dit средствами powershell: утилитами ntdsutil.exe, ntds_decode, хэши паролей сравниваются с хэшами из радужных таблиц и базы словарей программными средствами, написанными на языке Python.

Для получения списка установленных программ на устройстве выполняется скрипт powershell, в основе которого лежит команда Get-WmiObject -ComputerName $computer.Name -Class Win32_Product, где класс WMI Win32_Product используется для получения информации о версии ПО. Поиск уязвимых ПО осуществляется на основе сравнения актуальных версий ПО, уставленного на устройствах, с базой CVE.

Для проверки парольной политики также используются командлеты powershell: Get-ADDomainPasswordPolicy и net accounts. Текущие настройки сравниваются с требованиями парольной политики организации, а также нормативными документами, например, «Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014)».

Для автоматизации каждая часть объединена в полноценный скрипт [11]. Предлагается загрузить полученную технологию в планировщик задач для регулярной проверки конфигураций информационной системы в разных сегментах и доменах организации.

Выводы

В результате была создана технология и разработаны рекомендации, позволяющая быстро и эффективно проводить аудит безопасности конфигураций ИС, своевременно выявляя недостатки безопасности и предупреждая реализацию угроз ИБ. Технология отличается своей простой в использовании и скоростью выполнения. Результаты аудита словарных паролей можно использовать для обучения сотрудников о правилах безопасности и важности создания и использования сильных паролей. В дальнейшем предлагается сформировать шаблон визуализации результатов для удобной аналитики данных и предоставления отчетности.

Литература

1. Легковесное управление уязвимостями / Дорофеев А.В., Марков А.С. // Защита информации. Инсайд. 2024, № 6. С. 2-9.

2. Беленко А. Пароли: стойкость, политика назначения и аудит // Защита информации. Инсайд.2019. № 1 (25). С. 61-64.

3. К вопросу о парольной защите почтовых сервисов / Марков Г.А., Шарунов В.А. // Вопросы кибербезопасности. 2015. № 5 (13). С. 55-59.

4. Гуфан К.Ю., Новосядлый В.А., Эдель Д.А. Оценка стойкости парольных фраз к методам подбора // Открытое образование. 2011. №2. 127-130 с.

5. Сааков В.В., Кошиев К.Х., Боготов И.М., Кирин Д.А. Анализ проблем парольной защиты. Сборник трудов конференции «Наука и образование: сохраняя прошлое, создаём будущее». - 2022. - С. 34-36.

6. Тюрин К.А., Семин Р.В. Анализ стойкости парольных фраз на основе информационной энтропии // Известия ЮФУ. Технические науки. 2015. —С. 18-27.

7. Чмыхалова, А. В., Сосновский М. В. Проблемы в проведении аудита ИБ и способы их решения / Флагман науки. – 2024. – № 3(14). – С. 358-360.

8. Любухин, А. С. Повышение эффективности внутреннего аудита информационной безопасности объектов КИИ / Современная наука: традиции и инновации : Сборник научных статей по итогам VI молодежного конкурса научных работ. – Волгоград : Научный издательский центр "Абсолют", 2022. – С. 51-55.

9. Сёмин Р. В., Новосядлый В. А. Исследование задачи активного аудита парольной политики в компьютерных сетях // Известия ЮФУ. Технические науки. 2015. №5 (166).

10. Сахибгареев, И. Р. Автоматизация проведения проверки по оценке соответствия АСУ ТП стандартам компании / Фундаментальная и прикладная наука: состояние и тенденции развития : Сборник статей XXXV Международной научно-практической конференции, Петрозаводск, 23 ноября 2023 года. – Петрозаводск: Международный центр научного партнерства "Новая Наука", 2023. – С. 81-88.

11. Потапова А.С. Техническая проверка словарных паролей. Сборник научных трудов Второй научно-технической конференции «Кибернетика и информационная безопасность» (КИБ-2024). НИЯУ МИФИ, 2024. С. 60-61.

Научный руководитель: Марков Алексей Сергеевич, д.т.н., профессор кафедры ИУ8 «Информационная безопасность» МГТУ им. Н.Э.Баумана, Москва, a.markov@bmstu.ru**.**

Internal configuration security audit

Potapova A.S.[130]

Abstract. The statistics of attacks on Russia show the urgent need to take proactive measures to protect individual services and the IT infrastructure. Regular system checks are required for vulnerable software versions, password policy flaws, and weaknesses in user authentication data. The results of the internal audit should be used to improve configuration security settings and minimize information security risks. An analysis of scientific publications and various sources conducted about the study revealed the existence of a problem in this area. The methods of conducting an information security audit are considered and analyzed, the technology of point-based automatic configuration security verification is proposed, as well as ways to improve the organization of activities aimed at eliminating problems identified by the audit.

Keywords: information security, password policy, dictionary passwords, information security audit, vulnerable software, authentication.

[130] Anastasia S. Potapova, National Research Nuclear University "MEPhI", Moscow, PASer@mail.ru

УДК 336:004.056

Криптоактивы: объекты для цифровых вторжений, средство для виртуальных афер, сравнение с альтернативными инструментами инвестирования

Ревенков П.В.[131], **Бердюгин А.А.**[132], **Чебарь А.Г.**[133], **Бердюгин В.А.**[134]

В статье рассматриваются особенности и риски инвестиций в криптовалюты, а также анализируются альтернативные инструменты, такие как банковские депозиты. Цель исследования – оценить преимущества и недостатки криптовалют как инвестиционного инструмента, а также дать рекомендации для новичков на финансовом рынке. Выявлены ключевые моменты, касающиеся волатильности рынка криптовалют, их инвестиционной привлекательности и рисков, связанных с кибермошенничеством. Проведено сравнение криптовалюты с другими финансовыми инструментами. Делаются выводы об общественной ценности криптовалют и их влиянии на экономику.

Ключевые слова: *криптовалюта, инвестиции, банки, депозиты, риски, волатильность, мошенничество*

Введение

В настоящее время растёт популярность криптовалют [1-4]. Некоторые эксперты считают, что криптовалюты станут частью новой смарт-инфраструктуры для поддержания глобальной экономики. Однако есть мнение, что это обычная пирамида. Криптовалютные биржи – это торговые площадки, где клиенты могут покупать и продавать, обменивать и хранить цифровые активы. В марте 2024 года общий объем торгов на них составил 2,5 триллиона долл., а на бирже Binance – более 1 триллиона долларов [5]. Кроме того, объем средств, хранящихся на биржах, превышает 100 миллиардов долл. Согласно Chainalysis, в 2023 году было зафиксировано более 230 атак на биржи, и общий объем украденных активов составил около 1,7 миллиарда долл. 24% атак были направлены на централизованные биржи, 57% – на DeFi-сервисы.

По данным, представленным на веб-сайте компании Chainalysis, за 2023 год было зафиксировано более 230 случаев хакерских атак на криптовалютные биржи. При этом общий объем украденных активов составил около 1,7 миллиарда долл. [6]. При этом, согласно информации, представленной на веб-сайте компании «ШАРД», 24% из всех зафиксированных атак на крипто-сервисы за 2023 год были направлены на централизованные криптовалютные биржи, около 57% – на DeFi-сервисы, к которым также относятся и децентрализованные криптовалютные биржи:

- Poloniex (ущерб 125 миллионов долл.);
- CoinEx (ущерб 70 миллионов долл.);
- Bitrue (ущерб 23 миллиона долл.);
- GDAC (ущерб 14 миллионов долл.);
- dYdX (ущерб 9 миллионов долл.);
- Coins.ph (ущерб 6,2 миллиона долл.);
- Sushiswap (ущерб 3,3 миллиона долл.);

[131] Ревенков Павел Владимирович, доктор экономических наук, профессор кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, PVRevenkov@fa.ru

[132] Бердюгин Александр Александрович, младший научный сотрудник кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, AABerdyugin@fa.ru

[133] Чебарь Александр Геннадьевич, старший преподаватель кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, AGChebar@fa.ru

[134] Бердюгин Василий Александрович, руководитель направления ПАО «Мечел», Москва, berdyugin.vasiliy@mail.ru

• OKX (ущерб 2,7 миллиона долл.);
• Remitano (ущерб 2,7 миллиона долл.).

Помимо кибератак на криптовалютные биржи с целью завладения чужими криптоактивами, есть и ещё одна проблема – это использование криптовалют для осуществления новых видов мошенничества. Далее приведём несколько таких примеров с использованием различных криптовалют.

Парадокс «честных» мошенников

Часть команд ICO[135] сразу начинали работу с мошенничества, включая в названия своих проектов даже «подсказки».

Например, PonziCoin, названный в честь самой известной финансовой пирамиды (однако, намёки в названии данного проекта не помешали ему собрать 250 тысяч долл.). ScamCoin давал такое обещание: «Единственный ICO-проект, в котором можно быть уверенным! Вы получите 0% дохода с каждых 100% вашей инвестиции, мы это гарантируем!» [7]. Это редкие случаи работы «честных жуликов», которые на своих же сайтах открыто заявляли, что проект не имеет никакой ценности, что это финансовая пирамида и что инвестировать в него бессмысленно. Но все равно находились желающие отдать им свои деньги.

Одна ICO назвалась «Бесполезный Эфир» (токен, названный в честь blockchain-технологии Ethereum). Разработчик прямо на сайте написал, что не собирается ничего делать с заработанными им деньгами, просто купит себе новую бытовую технику, а начать собирается с огромного плоского телевизора.

Скорее всего, это первый стартап такого рода с полностью точным рекламным описанием. Его создатель честно признавался, что проект «абсолютно прозрачно сулит инвесторам нулевую ценность», совершенно точно не подлежит никакому аудиту, а любой пафосный текст описаний дословно скопирован с ресурса GitHub[136]. Проект набрал 40 тысяч долл. [7].

Часть мошенников для обмана инвесторов шли по дороге невероятных и несбыточных обещаний. Они сулили партнёрство с MasterCard, Visa, Amazon, Microsoft и хвастались огромными якобы уже сформированными базами клиентов и пользователей.

Зачастую позиционировали свои «многомиллиардные» доходы превосходящие доходы многих крупных мировых компаний. Мнимые и несбыточные технические достижения затмевали дорогостоящие проекты мировых лидеров отрасли.

Некоторые ICO утверждали, что они будут предоставлять банковские услуги 2,5 миллиардов человек по всему миру, которым крупнейшие мировые банки никогда не предоставляли свои услуги. Чаще всего за отсутствием такого охвата и впрямь стояло нежелание традиционных финансовых систем тратить большие деньги ради скромного дохода.

Шанс для авантюриста

Не все ICO запускали с мошенническими целями. Некоторые из них оказались под руководством индивидуумов, обладающих очевидными недостатками интеллекта и опыта, но проявляющих авантюрные наклонности.

В 2017 году термин «блокчейн» ещё обладал почти магическим влиянием, и его упоминание сразу же повышало оценку компании. Региональная американская чайная компания Long Island Ice Tea Corp изменила свой бренд на Long Blockchain Corp. Их акции за ночь резко выросли на 289% [8].

---

[135] ICO – первичное размещение монет, аналог IPO или краудфандинга. Инвестиции в него сопряжены с высоким риском, но имеют шанс на высокий доход.

[136] https://github.com – крупнейший веб-сервис для хостинга IT-проектов, программных кодов и их совместной разработки.

Фейковые мошеннические сайты практически неотличимы от настоящих (рис. 1, рис. 2) [9, 10].

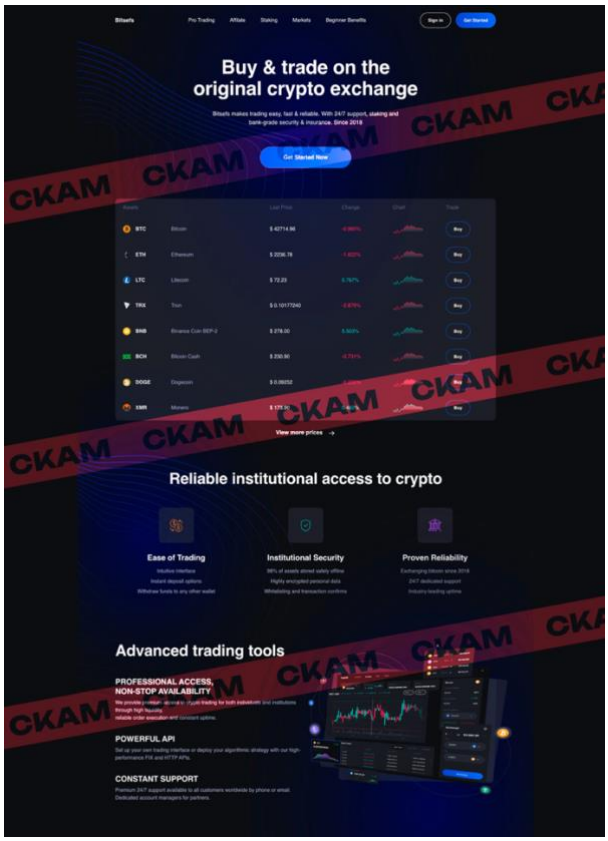


Рис.1. Пример интерфейса мошеннического сайта по покупке и продажи криптовалют [11]

Рис. 2. Реклама от Impulse Team, опубликованная в феврале 2021 года на российском подпольном форуме киберпреступников [12]

Другой пример связан с созданием ICO вокруг темы любовных отношений[137]. «Романтические аферы» – популярный способ обмана частных инвесторов в сфере криптовалют. Даже опытные люди могут стать жертвами подобных схем. Чаще всего после общения на сайте-знакомств, следовало предложение сделать инвестиции в какой-нибудь новый «быстроразвивающийся» проект. После перевода средств виртуальный любовник исчезал (не выходил на связь и становился недоступен), а вывести деньги из «инвестиционной системы» становилось невозможным [5].

В середине 2022 года компанию Sky Mavis ограбили на 540 миллионов долл. в криптовалюте в ходе атаки со шпионским программным обеспечением.

На сегодняшний день это считается самой крупной кражей криптовалюты. Чтобы обмануть разработчиков, злоумышленники провели целевую атаку на сотрудников Sky Mavis. Они заранее собрали информацию о компании и разработали схему мошенничества, основанную на фиктивном предложении работы с высокой заработной платой.

План преступников оказался успешным: они связались (вероятно, через LinkedIn) с одним из старших инженеров Axie Infinity, который был заинтересован в их выгодном предложении. Он успешно прошёл «собеседование» и получил торговое предложение (оффер) в виде PDF-файла. Сотрудник скачал документ и непреднамеренно загрузил в сеть компании скрытую шпионскую программу [13].

Немного о депозитах и других активах

Выделим несколько аспектов для анализа и сравнения вложений в криптовалюты с другими финансовыми инструментами.

В табл. 1 представлено несколько направлений для сравнения:

Табл. 1.

Сравнение криптовалюты с другими финансовыми инструментами. Анализ авторов

Критерий	***Крипто-валюты***	***Акции***	***Золото***	***Облига-ции***	***Недвижи-мость***
Волатильность	Высокая	Умерен.	Низкая	Низкая	Умерен.
Потенциальная доходность	Высокая	Высокая	Умерен.	Низкая	Умерен.
Ликвидность	Высокая	Высокая	Средняя	Высокая	Низкая
Риски	Высокие	Умерен.	Низкие	Низкие	Умерен.
Защита от инфляции	Ограниченная	Умерен.	Высокая	Умерен.	Средняя
Дивиденды	Нет	Есть	Нет	Есть	Есть
Глобальная доступность	Высокая	Высокая	Высокая	Средняя	Низкая
Необходимость регулирования	Высокая	Умерен.	Низкая	Низкая	Умерен.

Таким образом, криптовалюты и акции – волатильные (подвержены значительным колебаниям цен), с высокой доходностью и рисками, ликвидные (быстро конвертируются в денежные средства) [14, 15]. Золото защищено от инфляции. Акции и облигации приносят дивиденды, криптовалюты и золото – нет.

Все активы (кроме недвижимости) глобально доступны, но криптовалюты более доступны, требуют строгого регулирования.

[137] Например, SexCoin был реализован в качестве средства платежа за использования сексуальных услуг. Его позиционировали как инструмент борьбы с обманом клиентов и поставщиков услуги. Как именно предполагалось решать эту благородную задачу, конечно же, не уточнялось. Потратить секс-койны можно было только в магазине «Секс-койн горничная» [8].

Таблица 1 позволит лучше понять преимущества и недостатки разных финансовых инструментов, включая криптовалюты, и может служить основой для более глубокого анализа в дальнейшем.

Заключение

Некоторые эксперты считают, что традиционные регулируемые системы не выдержат конкуренции даже в условиях протекционизма, поскольку они недостаточно быстры, гибки и масштабируемы в мире, где ежечасно продаются 200000 смартфонов с доступом в интернет [5, 16, 17]. В результате банки могут отказаться от традиционных продуктов и предложить лишь базовые банковские услуги, тогда как регуляторы займутся мониторингом капитала, а хранение и обработка персональных данных перейдут к брокерам и государственным идентификационным сервисам на основе блокчейна. Оценку риска операций может взять на себя искусственный интеллект [18].

Литература

1. *Анализ современных тенденций развития технологии "блокчейн" и цифровых валют / Астраханцев Р.Г., Лось А.Б., Мухамадиева Р.Ш. Вопросы кибербезопасности. 2019. № 5 (33). С. 57-62.*
2. *Безопасность в сфере оборота виртуальной валюты / Захаров Д.Н., Иванов В.Ю. // Вопросы кибербезопасности. 2017. № S2 (20). С. 30-38.*
3. *Выявление подозрительных узлов сети биткоин методами анализа больших данных / Гарин Л.А., Гисин В.Б. // Вопросы кибербезопасности. 2022. № 3 (49). С. 90-99.*
4. *О развитии технологии блокчейн в России / Петренко С.А., Петренко А.С. // Защита информации. Инсайд. 2019. № 2 (86). С. 19-25.*
5. *Кинг Б. Банк 4.0. Новая финансовая реальность – М.: Олимп-Бизнес. 2023. – 476 с.*
6. *Прокофьев С.Е. VR-технологии как инструмент повышения эффективности учебного процесса в экономическом вузе // Аккредитация в образовании. 2022. № S1. С. 70-71.*
7. *Абрамова М.А., Амосова Н.А., Пашковская И.В. и др. Финансовая стабильность на финансовых рынках: идентификация лидерства и источников генерации рисков: монография. М.: ООО «Издательство “КноРус”». 2025. – 240 с.*
8. *Тетенева О.А., Кочкаров Р.А., Рябов П.Е. Разработка сервиса анализа и подбора инструментов коллективных инвестиций для неквалифицированных инвесторов // Нейрокомпьютеры: разработка, применение. 2024. Т. 26. № 3. С. 14-21.*
9. *Подход к вероятностному прогнозированию защищенности репутации политических деятелей от "фейковых" угроз в публичном информационном пространстве / Костогрызов А.И. // Вопросы кибербезопасности. 2023. № 3 (55). С. 114-133.*
10. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д. П. Зегжды. - М.: Горячая линия - Телеком, 2021. - 560 с.*
11. *Щербаков Д., Палей Л. Предупреждён – вооружен. Обнаружена будущая цель для хактивистов – операторы ЦФА // BIS Journal, 2024, № 3 С. 8-9.*
12. *Могайар У.: Блокчейн для бизнеса – М.: Бомбора, 2018. 224 с.*
13. *Черняева Е. Криптовалюты. Знания, которые не займут много места – М.: Эксмо, 2024, 128 с.*
14. *Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDOS-угроз // Вопросы кибербезопасности. 2017. № 3 (21). С. 16-23.*

15. Ревенков П.В., Бердюгин А.А., Макеев П.В. Оценка риска нарушения кибербезопасности в коммерческом банке (на примере атак на банкоматы "brute force" и "black box") // Вопросы кибербезопасности. 2021. № 3 (43). С. 20-30.

16. Царегородцев А.В., Елин В.М. Цифровой суверенитет России в условиях построения мирового информационного общества // Юридическая наука. 2024. № 6. С. 39-43.

17. Ревенков П.В., Францев В.В., Бердюгин А.А., Чебарь А.Г. Цифровые экосистемы, или как технологии начинают думать за нас // Банковское дело. 2022. № 5. С. 36-41.

18. Игра-викторина ProgressQuest с элементами Tamagotchi и Easter Egg: Рос. Федерация. № RU 2024612236 / Бердюгин А.А., Ревенков П.В.; регистр. 25.01.2024; опубл. 30.01.2024.

Cryptocurrencies: targets for cyberattacks, a tool for cyber fraud, comparison with other assets

Revenkov P.V.[138]**, Berdyugin A.A.**[139]**, Chebar A.G.**[140]**, Berdyugin V.A.**[141]

Abstract. The article examines the features and risks of investing in cryptocurrencies, as well as analyzes alternative instruments such as bank deposits. The aim of the research is to evaluate the advantages and disadvantages of cryptocurrencies as an investment tool and to provide recommendations for newcomers in the financial market. Key points regarding the volatility of the cryptocurrency market, its investment attractiveness, and risks related to cyber fraud are identified. A comparison of cryptocurrencies with other financial instruments is conducted. Conclusions are drawn regarding the social value of cryptocurrencies and their impact on the economy.

Keywords: cryptocurrency, investments, banks, deposits, risks, volatility, fraud

[138] Revenkov Pavel Vladimirovich, Doctor of Economic sciences, Professor of the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, PVRevenkov@fa.ru

[139] Berdyugin Alexander Alexandrovich, Junior Researcher at the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, AABerdyugin@fa.ru

[140] Chebar Aleksandr Gennadevich, Senior Lecturer at the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, AGChebar@fa.ru

[141] Berdyugin Vasily Aleksandrovich, Head of Department, PJSC Mechel, Moscow, berdyugin.vasiliy@mail.ru

УДК 004.051

Искусственный интеллект в космических технологиях: текущая ситуация, задачи, перспективы

Ромашкина Н.П.[142]

Аннотация. В статье представлен анализ применения технологий искусственного интеллекта (ИИ) в космической сфере, в том числе, в системах управления искусственных спутников Земли (ИСЗ) и многоспутниковых группировок. Приведены ключевые факторы целесообразности применения и основные направления использования ИИ в космической индустрии. Выявлены перспективные технологии ИИ в космических робототехнических средствах, исследовании дальнего космоса, контроле, диагностике и управлении техническим состоянием спутников, управлении многоспутниковой группировкой, обработке спутниковых изображений. Сформулированы задачи, связанные с влиянием состояния космической группировки на уровень стратегической стабильности, национальной и международной безопасности, а также с ролью ИИ в развитии космических технологий. Выработаны предложения по расширению потенциала использования ИИ в освоении ближнего космоса, околоземной орбиты для обеспечения экономического, научно-технологического развития и безопасности России.

Ключевые слова: космическая индустрия, искусственный спутник Земли (ИСЗ), искусственный интеллект, орбитальная группировка, спутниковая система управления, многоспутниковая группировка, космический потенциал России

Введение

Искусственный интеллект (ИИ), как одно из направлений ускоренно развивающихся технологий, активно используется в космической сфере. При этом уровень развития космических технологий является на современном этапе важнейшим показателем статуса и глобального влияния государства [1-3]. Наряду с несомненными позитивными возможностями ИИ лавинообразно растут риски и угрозы: военные и невоенные методы применения ИИ преступниками, террористами и государственными акторами, могут привести к серьезным вызовам стратегической стабильности, глобальному миру и безопасности [4-7]. Отсутствие отлаженного международного механизма отслеживания, управления и контроля над технологиями ИИ может привести к возникновению новых конфликта по всему миру. Поэтому тема создания на базе ООН органа, который мог бы разработать глобальные стандарты по регулированию сферы ИИ, стала одной из важнейших в 2023–2024 гг. Лидирующую роль в вопросах регулирования применения ИИ должен играть Совет Безопасности ООН.

Области применения ИИ в космической индустрии

Технологии ИИ в космической области к настоящему времени приобретают статус стратегических. Объем инвестиций в создание и развитие технологий ИИ со стороны ведущих мировых ИТ-компаний исчисляется миллиардами долларов. Согласно прогнозу аналитической компании *Tractica*, к 2025 г. мировой доход рынка от программного обеспечения для ИИ достигнет $126,0 млрд.[143]

Основные факторы, определяющие целесообразность применения ИИ в космической индустрии:

---

[142] Ромашкина Наталия Петровна, кандидат политических наук, профессор, ЦМБ ИМЭМО РАН, Москва, Romachkinan@yandex.ru

[143] Artificial Intelligence Software Market to Reach $126.0 Billion in Annual Worldwide Revenue by 2025, According to Tractica // https://www.businesswire.com/news/home/20200106005317/en/Artificial-Intelligence-Software-Market-to-Reach-126.0-Billion-in-Annual-Worldwide-Revenue-by-2025-According-to-Tractica.

• решение прикладных задач освоения Вселенной с более высоким выходным качеством и оперативностью при необходимых вычислительных и других ресурсах;

• обеспечение более высокого уровня автономности КА и (или) орбитальной группировки, в том числе, в условиях существенной априорной неопределенности условий их функционирования, без ущерба эффективности их целевого применения [8].

Основные направления применения ИИ в космической индустрии:

• робототехнические средства (РБС) (начиная со стадии производства КА);

• исследование дальнего космоса и реализация дальних космических миссий;

• контроль, диагностика и управление техническим состоянием КА;

• бортовая обработка целевой информации;

• тематическая обработка спутниковых изображений;

• управление многоспутниковыми орбитальными группировками;

• интеллектуальные системы поддержки проектных решений;

• обработка больших массивов разнородной спутниковой информации.

Основные направления применения РБС:

• орбитальное обслуживание КА (ремонт, заправка, сборка, увод с орбиты);

• космические зонды;

• линии сборки, обеспечивающие массовое серийное производство КА нового поколения для создания многоспутниковых систем;

• автономное выполнение опасных работ [9].

Кроме того, в последние десятилетия наблюдается тенденция коммерциализации космоса, в том числе, планы массовых туров за пределы Земли. Именно применение ИИ уже стало катализатором для запуска наиболее амбициозных проектов по изучению внеземного пространства, поэтому преимущества ИИ будут ускоренно совершенствоваться и использоваться в космической индустрии [10, 11].

ИИ для спутниковых систем

ИИ успешно внедряется для улучшения функционирования спутниковых систем:

- бортовые системы контроля, диагностики и управления техническим состоянием ИСЗ, в том числе, с целью существенного повышения уровня автономности КА (в перспективе – интеллектуальные системы для прогнозирования изменения состояния во времени с расширением функций адаптивности и самообучаемости);
- сенсоры и механизмы для отслеживания положения ИСЗ и его корректировки, для изучения структуры других КА, планет и космического мусора с целью прогнозирования риска столкновения;
- системы обеспечения кибербезопасности и мониторинга работоспособности;
- динамические экспертные системы, способные по результатам измерения и обработки различных параметров бортовых систем осуществлять управление их техническим состоянием;
- механизмы для поддержания стабильной связи путем постоянного измерения параметров на борту ИСЗ для передачи данных на Землю или на другие ИСЗ с целью определения оптимального пути сообщения и эффективного распределения ресурсов КА;
- устройства тематической обработки спутниковых изображений (использование ИИ непосредственно на борту ИСЗ уменьшают необходимость коммуникации между наземными и космическими станциями);
- системы оповещения о катаклизмах путем расчета вероятности явлений, прогноза вариантов развития и последствий;
- системы навигации и обработки данных;

- системы мониторинга и управления спутниками с наземных станций с целью повышения эффективности оператора при принятии оперативных решений и выборе корректирующих мер [12, 13].

Ускоренное развитие многоспутниковых низкоорбитальных космических систем с использованием малых КА привело к необходимости разработки новых подходов к их управлению, в том числе, ориентированных на повышение автономности решения задач, позволяющих упростить наземную инфраструктуру управления орбитальной группировкой и повысить живучесть системы в целом.

Выводы

Представленный анализ позволяет сделать вывод о важной роли ИИ в развитии современных космических технологий и их влиянии на уровень стратегической стабильности, национальной и международной безопасности.

Для обеспечения экономического и научно-технологического развития и безопасности России целесообразно использовать технологии ИИ в следующих направлениях:

• расширение потенциала использования ближнего космоса, околоземной орбиты на основе российских и совместных международных разработок;

• обеспечение безопасности КА;

• увеличение количественного и качественного потенциала спутниковой группировки, создания и эксплуатации многоспутниковых группировок РФ;

• обеспечение безопасной космической обстановки;

• ключевые космические сервисы для решения задач в области экологии и климата, экономического и технологического развития территорий, расширения транспортно-логистических коридоров, в том числе Северного морского пути;

• космические услуги для развития перспективных секторов экономики (робототехника, экономика данных, беспилотный транспорт и др.);

• отражение возможного нападения противника с применением КА, недопущения завоевания им превосходства в стратегической космической зоне;

• разработка инновационного национального российского проекта в области спутниковых технологий с привлечением внебюджетных средств;

• решение задач, поставленных Президентом РФ В.В. Путиным на Совещании по вопросам развития космической отрасли от 26 октября 2023 г.[144]:

• налаживать серийное производство КА;

• снижать стоимость доставки КА на околоземную орбиту, создавать инфраструктуру для массовых запусков ИСЗ, включая малые КА, и обеспечить доступ к ней для частных технологических компаний;

• развивать экспорт российских космических продуктов и услуг;

• расширять международное сотрудничество в сфере ИИ, в первую очередь, в рамках СНГ, ЕврАзЭС, ШОС, БРИКС и ОДКБ.

Литература

1. 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.

2. Ромашкина Н.П. Спутниковые информационные технологии в период кризиса и военных операций: состояние, проблемы, перспективы // Международная жизнь. 2024. № 4. С. 96-107.

[144] Совещание по вопросам развития космической отрасли // http://www.kremlin.ru/events/president/news/72606.

3. 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.

4. 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. // https://www.imemo.ru/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s.

5. 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.

6. Марков А.С., Шеремет И.А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. 2019. № 2 (67). С. 82–90.

7. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Information Technologies and International Security : [electronic resource]. – Moscow : IMEMO, 2023. – 111 p. – ISBN 978-5-9535-0613-7. – DOI 10.20542/978-5-9535-0613-7. – URL: https://www.imemo.ru/publications/info/information-technologies-and-international-security.

8. Ромашкина Н.П. Спутниковые системы управления с применением искусственного интеллекта // Вопросы кибербезопасности. 2023. № 6 (58). С. 128-137. DOI 10.21681/2311-3456-2023-6-128-137.

9. Искусственный интеллект в космической технике: состояние, перспективы развития // Ракетно-космическое приборостроение и информационные системы. 2019. Том 6, выпуск 1. С. 65–75. DOI 10.30894/issn2409-0239.2019.6.1.65.75.

10. Bassel Al Homssi, Kosta Dakic, Ke Wang, Tansu Alpcan, Ben Allen, Russell Boyce, Sithamparanathan Kandeepan, Akram Al-Hourani, and Walid Saad. Artificial Intelligence Techniques for Next-Generation Massive Satellite Networks // IEEE COMMUNICATION MAGAZINE, VOL. X, NO. X, MAY 2022.*

11. Ромашкина Н.П. Искусственный интеллект в космической индустрии: состояние, проблемы, перспективы // Искусственный Интеллект. Теория и практика. 2024. № 2. С. 23-34.

12. 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.

13. Ромашкина Н.П. Космос как сфера конфронтации: спутники США в новых реалиях // Информационные войны. 2023. № 2 (66). С. 16-24.

14. Wynbrandt J. The Space Sector's Digital Launch: New Emphasis on Cutting-Edge Technologies Is Transforming Aerospace, 2020. // https://www.nasdaq.com/articles/the-space-sectors-digital-launch%3A-new-emphasis-on-cutting-edge-technologies-is.

Artificial Intelligence in Space Technologies: Current Situation, Tasks, Prospects

Romashkina N.P.[145]

Abstract. The article presents an analysis of the use of artificial intelligence (AI) technologies in the outer space sector, including in control systems of artificial Earth satellites and multi-satellite constellations. The article presents the key factors that determine the feasibility of AI use, as well as the main directions of its use in the space industry. The article identifies promising AI technologies in space robotics, deep space exploration, monitoring, diagnostics and management of the technical condition of satellites, management of a multi-satellite constellation, and processing of satellite images. The author poses the problems of the influence of the state of the satellite constellation on the level of strategic stability, national and international security, the importance of AI for the development of space technologies. Proposals have been developed to expand the potential of AI using in the exploration of near space, near-Earth orbit to ensure the economic, scientific and technological development and security of Russia.

Keywords: space industry, artificial Earth satellite, artificial intelligence, orbital group, satellite control system, multi-satellite group, space potential of Russia

[145] 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

Информация в теории задач информационной войны

Рюмшин К.Ю.[146], **Капицын С.Ю.** [147]

Критически важным ресурсом, оказывающим определяющее влияние на национальную безопасность, становятся информация и процессы информационной деятельности, циркулирующие в обществе и обеспечивающие принятие государственных решений в интересах управления (регулирования) обстановкой. В статье обоснована необходимость разработки фундаментальной теории и механизмов решения задач информационной войны, проведён анализ основных интерпретаций и базовых концепций, предложен естественно-научный поход к представлению содержания системообразующего понятия "информация".

Военно-политическая обстановка, социально-экономическое образование, лицо принимающее решение, информация, естественно-научный подход, закон сохранения целостности объекта, целевой объект воздействия, информационная потребность.

Введение

К началу нового десятилетия информационное оружие выходит на одно из лидирующих мест среди средств поражения, вторжения в сознание. Важное значение приобретает открытое и (или) скрытное, массированное, целенаправленное информационное воздействие на сознание граждан государств – объектов агрессии посредством информационных технологий в глобальной сети Интернет.

Современные информационные технологии становятся перспективным оружием, позволяющим обеспечить разрешение геополитических кризисов, без единого выстрела [1, 2].

Широкое их использование позволяет в считанные дни раскачать ситуацию в стране изнутри до кризисного состояния. Последствия деструктивных информационных воздействий, видны на примере "цветных революций" в Белоруссии, Украине, Киргизии, серии "революций Арабской весны", событий в Армении, Венесуэле, Нагорном Карабахе.

Задача информационной войны

Информационные ресурсы стали одним из самых эффективных средств в формировании требуемой информационной потребности, как отдельного человека, социальных групп, так и государства – социально-экономического образования (далее – СЭО) в целом. В процессе деятельности СЭО различного уровня иерархии при несовпадении целей возникают конфликты (информационные, вооружённые).

В основе деятельности лежит решение человека – лица принимающего решение (далее – ЛПР), органа государственного и военного управления. Деятельность основывается на модели [3-7]. Под информацией обычно понимают сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством.

Сведения, используемые человеком в своей деятельности, имеют у него модельную интерпретацию – модель обстановки.

Зависимость деятельности человека (военно-политического руководства) от информации (модельного представления) сформировала новое направление в

[146] Рюмшин Константин Юрьевич, доктор технических наук, Московский технический университет связи и информатики, г. Москва, e-mail: e8@mail.ru

[147] Капицын Сергей Юрьевич, кандидат технических наук, доцент, Санкт-Петербургский политехнический университет, г. Санкт-Петербург, e-mail: e8@mail.ru

противоборстве СЭО как информационное, которое в конце XX-го века получило название "информационная война".

Решение – это условие реализации предназначения объекта управления или самоуправления. Деятельность реализуется через управление.

Предназначение информационной войны – разрушение процесса управления, самоуправления противника. Это осуществляется через разрушение модели решения в различных условиях обстановки, возможностью вторжения в сознание целевого объекта воздействия (военно-политического руководства, социальных групп и т.п.) и гарантированного изменения у него информационной потребности в интересах скрытного формирования требуемой модели социального поведения (модели социального поведения "побежденного").

В условиях гибридизации современных конфликтов политические меры ***сводятся к попытке сменить (подменить) информационную потребность военно-политического руководства (далее – ВПР) государства с последующей сменой фундаментальной ответственности государства***. Как следствие этого, задачи информационной войны сводятся *к подмене информационной потребности лица принимающего решение (далее – ЛПР) противостоящей стороны и подчинение ее деятельности своим интересам для гарантированного обеспечения военно-политического превосходства.*

Информация с точки зрения естественно-научного похода

Так, при разработке фундаментальной теории и механизмов решения задач информационной войны в условиях "гибридизации", необходимо дать определении системообразующему понятию теории информационного противоборства – "информации".

Естественно-научный поход (далее – ЕНП) к представлению содержания базового понятия "информация" определяется интеграцией свойств мышления человека, всеобщей связью явлений, окружающего Мира и познания.

Для адекватного военно-политической обстановки решения, военному руководству (ЛПР) всех звеньев управления целесообразно руководствоваться тремя базовыми принципами, представленными в структурной схеме формирования модели решения на рис. 1.

Рис. 1. Структурная схема формирования модели решения

1 Принцип трехкомпонентности познания.

Методологический аспект – условия существования процесса деятельности, т.е. как у специалиста формируется адекватная модель;

Методический аспект – механизм воздействия на ЦОВ;

Технологический аспект – условия реализации воздействия.

2 Принцип целостности. Базируется на ЗСЦО и позволяет описать физический смысл процессов решения задач информационной войны.

3 Принцип познания. Основу принципа составляют методы: декомпозиции, абстрагирования, агрегирования. Что является фундаментальной составляющей для интеллектуального развития специалистов.

Системообразующим понятием процесса формирования модели решения, является "информация". К основным положениям трактовки понятия "информации" можно отнести следующие.

Существует три основные интерпретации понятия "информация":

−научная интерпретация – исходная общенаучная категория, отражающая структуру материи и способы её познания, несводимая к другим, более простым понятиям;

−абстрактная интерпретация – некоторая последовательность символов, образов, которые несут как вместе, так в отдельности некоторую смысловую нагрузку для исполнителя;

−конкретная интерпретация – В данной плоскости рассматриваются конкретные исполнители с учётом специфики их систем команд и семантики языка (например, для машины информация – "нули" и "единицы"; для человека – звуки, образы, и т.п.).

Анализ трактовки понятия "информация" основных базовых концепций [8-10] можно выразить следующим образом:

−концепция №1 (К. Шеннона) – отражает количественно-информационный подход, определяет информацию как меру неопределённости (энтропию) события. Количество информации зависит от вероятности его получения: чем более вероятным является сообщение, тем меньше информации содержится в нем;

−концепция №2 (академик АН СССР В.М. Глушков) [10] – рассматривает информацию как свойство материи и основано на утверждении, что информацию содержат любые сообщения, воспринимаемые человеком или приборами;

−концепция №3 (академик АН СССР В.Г. Афанасьев, Н. Винер) [8, 9] – основана на логико-семантическом (семантика – изучение текста с точки зрения смысла, значения смысловых конструкций) подходе, при котором информация трактуется как знание, которое используется для активного действия, управления и самоуправления. Информация – это действующая, полезная, "работающая" часть знаний.

Исходя из анализа традиционных концептуальных взглядов, на основе ЕПН к адекватной формализации толкования структурная схема развёртывания содержания понятия "информация" представлена на рис. 2.

Вывод

Проведённый анализ показывает, что общество находится в состояниях, формируемых непрерывными информационными процессами [12].

Полагая под информационным процессом – целостную совокупность последовательных действий, производимых над информацией с целью получения результата [11], при разработке фундаментальной теории и механизмов решения задач информационной войны в условиях "гибридизации", под "информацией" как базовым понятием информационного противоборства необходимо понимать модельную

интерпретацию процессов окружающей действительности, в частности, военно-политической обстановки.

Рис. 2. Структурная схема развёртывания содержания понятия "информация"

Литература

1. Международная безопасность в среде информационно-коммуникационных технологий / под ред. А.А. Стрельцова и др. М.: НАМИБ, 2023. - 132 с.

2. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.

3. Бурлов В.Г., Васильев М.Н., Капицын С.Ю. Об интеллектуализации процесса пропаганды на базе математической модели решения человека // XV Всероссийская научная конференция "Нейрокомпьютеры и их применение". Тезисы докладов. – М: ФГБОУ ВО МГППУ, 2017. С. 263 – 264.

4. Бурлов В.Г., Веревкин С.А., Грозмани Е.С., Капицын С.Ю., Петров С.В. Разработка модели управления процессом обеспечения информационной безопасности киберфизических систем // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. №4(36). – С. 94 – 98.

5. Бурлов В.Г., Васильев М.Н., Грачев М.И. Капицын С.Ю. Модель управления в социальных и экономических системах с учетом воздействия на информационные процессы в обществе // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. №5. – С. 46 – 55.

6. Burlov V.G., The Methodological Basis for Solving the Problems of the Information Warfare and Security Protection. 13th International Conference on Cyber Warfare & Security (ICCWS 2018) // National Defense University, Washington DC, USA, 2018. –Pp. 64 – 74.

7. Burlov V.G., Information Warfare: Modeling a decision makers processes. European Conference on Information Warfare and Security, ECCWS, 2018. Pp. 66 – 76.

8. Афанасьев В.Г. Социальная информация и управление обществом. – М., 1975. – 407 с.

9. Винер Н. Кибернетика, или Управление и связь в живом и машине. – М., 1968. – 344 с.

10. Глушков В.М. Математизация научного знания и теория решений // Философия, естествознание, современность. – М., 1981.

11. Рюмшин К.Ю., Капицын С.Ю., Вареница В.В. Логико-лингвистический механизм формирования "бумажных" пуль при информационном противоборстве. // Вопросы кибербезопасности. 2023, № 1, с. 93–99.

12. Proceedings of the 16th International Conference on Cyber Warfare & Security (ICCWS 2021) // Tennessee Tech University and Oak Ridge National Laboratory, Cooksville, Tennessee, USA, 2021. – 545 p.

Information in the Theory of Information Warfare Tasks

Ryumshin K.Yu., Kapitsyn S.Yu. [148]

Information and processes of information activity circulating in society and ensuring the adoption of state decisions in the interests of managing (regulating) the situation are becoming a critical resource that has a decisive influence on national security. The article substantiates the need to develop a fundamental theory and mechanisms for solving information warfare problems, analyzes the main interpretations and basic concepts, and proposes a natural-scientific approach to presenting the content of the system-forming concept of "information".

Military-political situation, socio-economic education, decision maker, information, natural science approach, law of conservation of integrity of an object, target object of influence, information need.

148 Ryumshin Konstantin Yurievich, Dr.Sc., Moscow Technical University of Communications and Informatics, Moscow, e8@mail.ru
Kapitsyn Sergey Yurievich, Ph. D, Associate Professor, St. Petersburg Polytechnic University, St. Petersburg, wolf76@mail.ru

УДК 004.056

Логико-лингвистический подход при информационном противоборстве

Рюмшин К.Ю.[149], **Капицын С.Ю.** [150]

Характерная особенность системных исследований состоит в создании формализованных методов описания и решения основных задач в соответствующих областях и сферах жизнедеятельности общества, требующих всестороннего учёта всех процессов и явлений. Решение проблемных вопросов в области информационного и гибридного противостояния – не исключение.

Информационная война, закон сохранения целостности объекта, логико-лингвистическая модель.

Введение

Моделирование вообще, а математическое моделирование в частности, определяют технологию познания. На основе адекватного познания мы и адекватно существуем в действительности.

Мерой адекватности является полнота учёта закономерностей рассматриваемой предметной области. Базовым законом является закон сохранения целостности объекта (далее – ЗСЦО) [1, 2, 8-12]. К сожалению, в логике представлении знаний для разработки эталонных словарей информационных элементов ("бумажных" пуль) вторжения в сознание целевого объекта воздействия (далее – ЦОВ) этот закон не используется. Не учёт этого закона приводит к возникновению неоднозначности определения значения понятий естественного языковых структур требуемой информационной потребности (далее – ИП) и как следствие снижению смыслового воздействия на мировоззрение ЦОВ.

Базовый подход к представлению целостности семантики знаний информационной потребности целевого объекта воздействия

Логико-лингвистическое моделирование (семиотическое, понятийное, "нечисловое") относится к одному из разделов теории искусственного интеллекта [3-7]. Оно базируется на воспроизведении (имитации) таких механизмов мышления человека, как восприятие и накопление знаний, структурирование и оценка ситуаций, целеобразование и планирование поведения, а также на использовании для этих целей искусственных языков, близких по свойствам к естественным. Логико-лингвистические модели (далее – ЛЛМ) оперируют не с количественной, а с качественной, понятийной информацией. Подход к логике построения лингвистических моделей "бумажных" пуль основывается на ЗСЦО.

Исходя из анализа и прогнозирования развития обстановки сформированной вокруг Российской Федерации, особенностей социального поведения ЦОВ в кризисных ситуациях, их ИП с достаточной определённостью поддаётся структуризации.

При этом в предлагаемом подходе на основе ЗСЦО, к целостности естественно-языкового описания семантических структур требуемой ИП, представленном на рис.1, учитываются следующие закономерности:

−закономерности построения смысловых структур естественно-языкового текста (информационной потребности, "бумажных" пуль);

−закономерности построения объектов различной физической природы, в частности, описание требуемой ИП ЦОВ.

[149] Рюмшин Константин Юрьевич, доктор технических наук, Московский технический университет связи и информатики, г. Москва, e-mail: e8@mail.ru

[150] Капицын Сергей Юрьевич, кандидат технических наук, доцент, Санкт-Петербургский политехнический университет, г. Санкт-Петербург, e-mail: e8@mail.ru

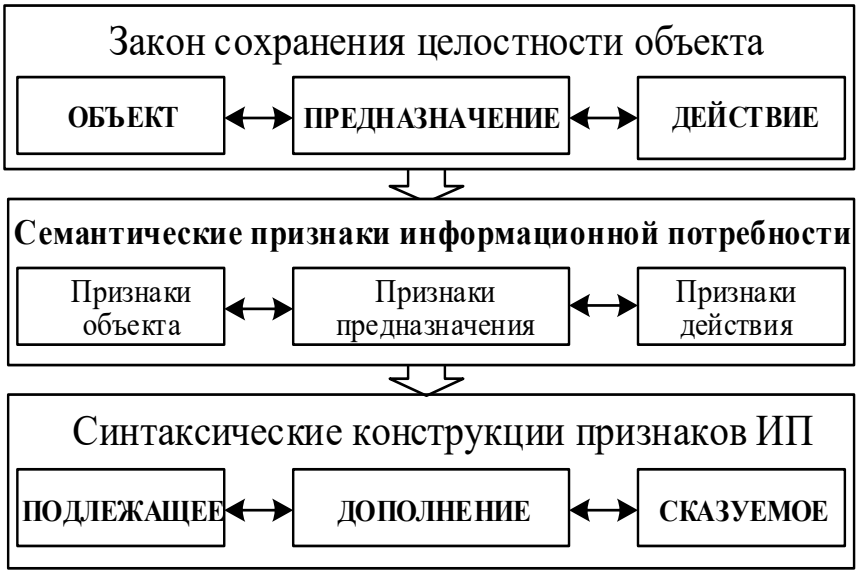


Рис.1. Схема подхода к представлению целостности естественно-языкового описания семантических структур ИП ЦОВ

В рамках выбранного подхода к целостности семантического описания ИП ЦОВ в виде лексических единиц и их синтактико-семантического взаимодействия, необходимо:

−сформировать словарь семантических признаков, определяющих ИП ЦОВ, т.е. представление смысла в виде устойчивой зависимости свойств (признаков) объекта от свойств (признаков) действия при фиксированном предназначении;

−сформировать словарь синтаксических конструкций признаков ИП, определяющих принадлежность семантических признаков к частям речи и предложения в текстовых структурах естественного языка.

Так, при дестабилизации обстановки в США и организации массовых беспорядков в городах штатов, обострения расовых противоречий, для формирования требуемой ИП чернокожего населения, "бумажные" пули можно представить в виде синтаксических конструкций семантических признаков, отражающих целостность смысловой области, требуемой ИП ЦОВ.

Семантические признаки, представляют признаковые структуры (комбинация слов), отражающих тематику требуемой ИП ЦОВ (ситуации). Признаковые структуры могут содержать одинаковые признаки-понятия, и могут быть объединены в одну, если они описывают один и тот же объект. Смысловая область может пополняться новыми признаками ИП.

Модель представления "бумажных" пуль краткими семантико-синтаксическими конструкциями в виде фразово-структурной грамматики

Класс контекстно-свободных грамматик широко используются для описания естественных языков [3-6]. Достоинством таких грамматик и языков является их относительно простая синтаксическая структура, с помощью которой удаётся охватить большое разнообразие теоретических и прикладных задач кибернетики.

Чтобы применить математический подход к "пониманию" смысловых текстовых структур ЕЯ, необходимо ограничиться множеством семантико-синтаксических конструкций (далее – ССК) признаков, которые определяют смысловую основу требуемой ИП ЦОВ и формируемым "бумажным" пулям. Для этого применим формально-грамматический метод, основанный

на грамматических правилах, с помощью которых можно распознавать и анализировать признаки ИП ЦОВ аналогично тому, как грамматики используются при изучении естественных языков.

Для формирования грамматических правил распознавания выявим, синтактико-семантическое взаимодействие признаков (идентификаторов) текстовых структур с элементами, играющих роль членов предложения или частей речи:

⟨предложение⟩(Пр);
⟨подлежащее⟩(П);
⟨сказуемое⟩(С);
⟨дополнение⟩(Д);
⟨имя существительное⟩(ИС);
⟨глагольная форма⟩(ГФ).

Заключение их в угловые скобки, чтобы отличать их от семантических признаков ИП ЦОВ, составляющих предложение языка. Такие элементы, как ⟨подлежащее⟩ или ⟨имя существительное⟩, играющее роль членов предложения или частей речи, называются нетерминальными (вспомогательными) признаками – N, где $N = \{< \text{Пр} >, < \text{П} >, < \text{С} >, < \text{Д} >, < \text{ИС} >, < \text{ГФ} >\}$.

В грамматике имеются определённые правила построения синтаксических конструкций признаков ИП ЦОВ – $\text{Р}_{\text{СК}}$, содержащие информацию о том, как из этих символов можно строить предложение языка. На основе ЗСЦО, вводится правила построения предложения как целостной смысловой основы.

Набор правил образует грамматику языка и определяет смысловую основу предложения. Правила синтаксиса описывают процедуру распознавания принадлежности предложений языку.

Начальный символ грамматики обозначим $S_{\text{СЗ}}$ – аксиома грамматики, т.е. синтаксическая структура, выражающая смысловую основу предложения и обладающая смысловой законченностью.

Применяя синтаксические правила, получаем конечное множество текстовых структур семантических признаков ИП ("бумажных" пуль) ЦОВ, наделённых смысловой законченностью.

Эти текстовые структуры, формируемые контекстно-свободной грамматикой, будем называть ССК признаков ИП ЦОВ.

Логико-лингвистическая модель представления множества требуемых смысловых выводов целевого объекта воздействия после применения "бумажных" пуль – вторжения в сознание

Логико-лингвистическая модель представления умозаключений ЦОВ после вторжений в сознание "бумажной" пули в виде формальной фразово-структурной грамматики [5] аналогична текстовым структурам и представляет собой априорный словарь смысловых выводов, соответствующих конкретной ССК признаков смысловых выводов.

Выходное предложение (в частности, умозаключение) строится по правилу ⟨предложение⟩ → ⟨подлежащее⟩ ⟨сказуемое⟩ ⟨дополнение⟩ и характеризуется смысловой законченностью.

Сформированный априорный словарь смысловых выводов $\text{Т}_{\text{СВ}}$ в виде синтаксических конструкций, позволяет представить знания ЦОВ в структурированном виде, что фактически обеспечивает представление семантики входных текстовых структур естественного языка.

Контекстно-свободная грамматика информационной потребности ЦОВ задаётся фразово-структурной грамматикой и представлена в виде:

$$G_{\text{ИПЦОВ}} = \{N_i, \{\text{Т}_{\text{СП}}, \text{Т}_{\text{СВ}}\}, \text{Р}_{\text{СК}}, S_{\text{СЗ}}\}. \quad (1)$$

Фразово-структурная грамматика выступает в качестве адекватного средства представления ИП ЦОВ и начального этапа формализации семантики текстовых структур с заданными признаками [5]. Математическая модель грамматики $G_{\text{ИПЦОВ}}$ отображает семантико-синтаксическое представление ИП ЦОВ. ССК признаков ЦОВ, являются адекватной эталонной моделью представления смысловой основы для использования в системах с технологиями распознавания входных текстовых структур естественного языка [4-6] так и генерации материалов воздействия.

Исходя из анализа особенностей деятельности (в частности, индивидуальных и коллективных зависимостей, разнородных уязвимостей, ментальности и т.п.) ЦОВ при создании условий состояния "кризиса", характеризующегося отсутствием модели решения, открывается возможность подмены информационной потребности, путём вторжения (в частности, SMS-рассылка "бумажных" пуль, информационные вбросы в социальные сети) в сознание целевого объекта воздействия и гарантированного изменения у него информационной потребности в интересах скрытного формирования требуемой модели социального поведения (модели социального поведения "побеждённого").

Так, при ведении информационного противоборства в САР, подмена информационной потребности ЦОВ осуществлялась комплексным вбросом информационных сообщений средствами звуковещания, телерадиовещания, SMS-рассылки, печатной продукции (листовки, газеты), электронных ресурсов сети Интернет (аккаунты, социальные сети).

Вывод

Таким образом, проиллюстрированы механизмы формирования "бумажных" пуль и множества требуемых смысловых выводов (умозаключений, основ для формирования модели социального поведения "побеждённого") ЦОВ после применения "бумажных" пуль в виде логико-лингвистических моделей.

Предлагаемый подход к представлению логико-лингвистической модели на основе ЗСЦО, позволяет учитывать:

– закономерности построения смысловых структур естественно-языкового текста (ИП, "бумажных" пуль);

– закономерности построения объектов различной физической природы (в частности, описание требуемой ИП ЦОВ).

Логико-лингвистические модели в виде эталонных семантико-синтаксических конструкций на основе фразово-структурной грамматики, являются конструктивной базой семантических признаков и их синтактико-семантического взаимодействия.

Таким образом, технология представления логико-лингвистических моделей (семантико-синтаксических конструкций) "бумажных" пуль может быть применена при разработке лингвистических основ информационного оружия (информационно-разведывательных ударных систем) в технологиях избирательного воздействия на объект для гарантированного изменения у него информационной потребности в интересах скрытного формирования требуемой модели социального поведения (модели социального поведения "побеждённого").

Литература

1 Бурлов В.Г., Васильев М.Н., Грачев М.И. Капицын С.Ю. Модель управления в социальных и экономических системах с учетом воздействия на информационные процессы в обществе // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. №5. С. 46 – 55.

2 Бурлов В.Г., Веревкин С.А., Грозмани Е.С., Капицын С.Ю., Петров С.В. Разработка модели управления процессом обеспечения информационной безопасности киберфизических систем // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. №4(36). С. 94 – 98.

3 Ловцов Д.А. Архитектура базы данных и знаний подсистемы планирования и координации информационных процессов в иерархической эргасистеме // Правовая информатика. 2020. № 4. С. 4 – 19.

4 Рюмшин К.Ю., Капицын С.Ю., Вареница В.В. Логико-лингвистический механизм формирования "бумажных" пуль при информационном противоборстве. Вопросы кибербезопасности. 2023, № 1, с. 93–99.

5 Язов Ю.К., Соловьев С.В., Тарелкин М.А. Логико-лингвистическое моделирование угроз безопасности информации в информационных системах. // Вопросы кибербезопасности. 2022. № 4 (50). С. 13 – 25.

6 Burlov V.G., The Methodological Basis for Solving the Problems of the Information Warfare and Security Protection. 13th International Conference on Cyber Warfare & Security (ICCWS 2018)//National Defense University, Washington DC, USA, 2018, pp. 64 – 74.

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

8 Burlov V.G., Information Warfare: Modeling a decision makers processes. European Conference on Information Warfare and Security, ECCWS, 2018, pp. 66 – 76.

9 Proceedings of the 13th International Conference on Cyber Warfare & Security (ICCWS 2018)//National Defense University, Washington DC, USA, 2018. – 688 p.

10 Proceedings of the 5th European Conference on Social Media // Limerick Institute of Technology, Ireland, 2018. – 484 p.

11 Proceedings of the 17th European Conference on Cyber Warfare & Security (ECCWS 2018) // University, Oslo, Norway, 2018. – 622 p.

12 Proceedings of the 16th International Conference on Cyber Warfare & Security (ICCWS 2021) // Tennessee Tech University and Oak Ridge National Laboratory, Cooksville, Tennessee, USA, 2021. – 545 p.

Logical-linguistic approach in information warfare

Ryumshin K.Yu., Kapitsyn S.Yu. [151]

A characteristic feature of system research is the creation of formalized methods for describing and solving the main problems in the relevant areas and spheres of society's life, requiring a comprehensive consideration of all processes and phenomena. Solving problematic issues in the field of information and hybrid confrontation is no exception.

Information warfare, the law of preserving the integrity of an object, logical-linguistic model.

151 Ryumshin Konstantin Yurievich, Dr.Sc., Moscow Technical University of Communications and Informatics, Moscow, e8@mail.ru
Kapitsyn Sergey Yurievich, Ph. D, Associate Professor, St. Petersburg Polytechnic University, St. Petersburg, wolf76@mail.ru

УДК 004.021: 004.056: 519.832

Защита авторского права с использованием цифровой голографии

Сысоев В.В.[152], **Быков А.Ю.**[153]

Данная статья посвящена цифровой стеганографии на основе БПФ. В статье описан алгоритм шифрования метки в контейнер и извлечение закодированной метки из стеганограммы. Представлены примера работы описанного алгоритма. Проведено сравнение с другими популярными стеганографическими алгоритмами. Показана стойкость алгоритма к различному виду атак на стеганограмму.

Ключевые слова: стеганография, голография Фурье, цифровая метка.

Введение

Проблема защиты авторского или эксклюзивного права на информацию является актуальной в коммерческих и государственных организациях в силу ценности как самой информации, так и прямым требованием действующего законодательства РФ. Несанкционированное/неправомерное применение данной информации может приводить для организаций как к репутационному ущербу, к прямым финансовым убыткам.

Предлагаемый алгоритм делает возможным защиту цифрового изображения путем нанесения маркировки, достаточно трудно обнаружимой для стегоаналитка, стойкой к различному виду атак (например, к обработке изображения белым шумом), при этом оставаясь визуально не отличимым от оригинального изображения.

Одна из особенностей алгоритма, приведенного в данной статье в том, что оно использует дискретное быстрое преобразование Фурье (FFT) [1-3] в процессе создания стеганограммы.

1. Математическая постановка задачи

В рамках данной статьи рассматривается две задачи – внедрение сообщения в контейнер (создание стеганограммы) и извлечение из стеганограммы внедренного сообщения.

Внедрение метки в контейнер

Дано следующее

Изображение Ci – контейнер в произвольном формате размерностью $w \times h$, где w – ширина изображения в пикселях, h – высота изображения в пикселях. Таким образом, что изображение Ci можно изобразить матрицей пикселей:

$$Ci_{w\times h} = \begin{pmatrix} p_{11} & \cdots & p_{w1} \\ \vdots & \ddots & \vdots \\ p_{1h} & \cdots & p_{wh} \end{pmatrix} \quad (1)$$

где p_{ij}- пиксель изображения в цветовом пространстве RGB, характеризирующийся тремя цветовыми спектрами $p_{ij} = [r, g, b]$.

Сообщение M в текстово-числовом виде, которое предстоит внедрить в контейнер.

[152]Сысоев Валентин Валерьевич, главный инженер, аспирант, ПАО Сбербанк, МГТУ им. Н.Э. Баумана, Москва, valsus88@mail.ru. SPIN-код РИНЦ 7387-4600, ORCID 0000-0002-6157-5815

[153]Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru. SPIN-код РИНЦ 6050-6574, Scopus Author ID 57201646483, ORCID 0000-0001-6336-5603

Необходимо найти

Стеганограмму Cm , представляющую собой изображение, той же размерности $w \times h$, со встроенным сообщением M, визуально неотличимое от изображения Ci. Такую, что:

$$Cm_{w\times h} = \begin{pmatrix} p''_{11} & \cdots & p''_{\mathrm{w}1} \\ \vdots & \ddots & \vdots \\ p''_{\mathrm{h}1} & \cdots & p''_{wh} \end{pmatrix} \quad (2)$$

Извлечение метки из стегоконтейнера

Дано следующее

Изображение $Cm_{w\times h}$ – стеганограмма в произвольном формате размерностью $w \times h$, где w – ширина изображения в пикселях, h – высота изображения в пикселях.

$$Cm_{w\times h} = \begin{pmatrix} p''_{11} & \cdots & p''_{\mathrm{w}1} \\ \vdots & \ddots & \vdots \\ p''_{\mathrm{h}1} & \cdots & p''_{wh} \end{pmatrix} \quad (3)$$

где p''_{ij}- пиксель изображения в цветовом пространстве RGB, характеризирующийся тремя цветовыми спектрами $p''_{ij}(r''_{ij}, g''_{ij}, b''_{ij})$.

Необходимо найти

Сообщение M в текстово-числовом виде.

2. Описание алгоритма

Внедрение метки в контейнер

Сообщение M из текстово-числового вида преобразуется в метку – изображение Mi произвольного размера $k \times$ l, где k – ширина изображения метки, а l – высота изображения метки, $k < w,\ \mathrm{l} < h$. Осуществляется попиксельный перевод изображения Mi из цветового пространства RGB в цветовое пространство HSV $Mi \rightarrow Mi'$. Из каждого пикселя p'^{M}_{ij} матрицы $Mi'_{k\times l}$ извлекаем соответствующую компоненту яркости v_{ij} и составляем соответствующую матрицу яркости метки $V^{M}_{k\times l}$:

$$V^{M}_{k\times l} = \begin{pmatrix} v^{M}_{11} & \cdots & v^{M}_{k1} \\ \vdots & \ddots & \vdots \\ v^{M}_{1l} & \cdots & v^{M}_{kl} \end{pmatrix} \quad (4)$$

В изображении – контейнере Ci переводим каждый пиксель из цветового пространства RGB в цветовое пространство HSV $\mathrm{C}i \rightarrow Ci'$. Для каждого $p^{\mathrm{C}}_{ij} = [r_{ij}, g_{ij}, b_{ij}] \rightarrow p'^{\mathrm{C}}_{ij} = [h_{ij}, s_{ij}, v_{ij}]$. Из каждого пикселя p'^{C}_{ij} матрицы $\mathrm{C}i'$ извлекаем соответствующую компоненту яркости v_{ij}. Матрицу яркости контейнера $V^{\mathrm{C}}_{w\times h}$ переводим в матрицу-строку V^{C}_{wh} путем соединения всех, h строк матрицы $V^{\mathrm{C}}_{w\times h}$ в одну строку: $V^{\mathrm{C}}_{w\times h} \rightarrow V^{\mathrm{C}}_{wh}$, где $wh = w \cdot h$ - длина матрицы строки. Над матрицей-строкой V^{C}_{wh} проводится быстрее преобразование Фурье $FFT()$:

$$FFT(V^{\mathrm{C}}_{wh}) = Z^{\mathrm{C}}_{wh} = \begin{pmatrix} z^{C}_{1} & \ldots & z^{C}_{wh} \end{pmatrix} \quad (5)$$

Матрица-строка Z^{C}_{wh} переводится в матрицу размерности $w \times h$ путем перевода w чисел из Z^{C}_{wh} на новую строку:

$$Z^{\mathrm{C}}_{wh} \rightarrow Z^{\mathrm{C}}_{w\times h} = Z^{\mathrm{C}}_{w\times h} = \begin{pmatrix} z^{C}_{11} & \cdots & z^{C}_{w1} \\ \vdots & \ddots & \vdots \\ z^{C}_{1h} & \cdots & z^{C}_{wh} \end{pmatrix} \quad (6)$$

Матрица $Z^{\mathrm{C}}_{w\times h}$ складывается с матрицей $V^{M}_{k\times l}$ по определенным правилам.

$$Z^{\mathrm{C}}_{w\times h} + V^{M}_{k\times l} = Z^{CM}_{w\times h} \quad (7)$$

Полученную про сложении матрицу $Z^{CM}_{w\times h}$ переводим в матрицу-строку Z^{CM}_{wh} путем соединения всех, h строк матрицы $Z^{CM}_{w\times h}$ в одну строку: $Z^{CM}_{w\times h} \rightarrow Z^{CM}_{wh}$. Над матрицей-строкой Z^{CM}_{wh} проводится обратное быстрее преобразование Фурье $FFFT()$. В результате получаем матрицу-строку V^{CM}_{wh}:

$$FFFT\left(Z_{wh}^{CM}\right) = V_{wh}^{\mathrm{CM}} = (v_1^{CM} \quad \dots \quad v_{wh}^{CM}) \tag{8}$$

Переведем матрицу-строку V_{wh}^{CM} в матрицу размерности $w \times h$ путем перевода w чисел из V_{wh}^{CM} на новую строку. В матрице $Ci'_{w\times h}$ заменим все компоненты яркости v_{ij} в каждом пикселе $p_{ij}^{\prime M}$ на компоненты яркости из $V_{w\times h}^{\mathrm{CM}}$. Переведем пиксели в матрице $Ci''_{w\times h}$ из цветового пространства HSV в цветовое пространство RGB. Для каждого $p_{ij}^{M}(h_{ij}, s_{ij}, v_{ij}^{CM})$ из $Ci''_{w\times h}$:

$$Cm_{w\times h} = \begin{pmatrix} p''_{11} & \cdots & p''_{\mathrm{w1}} \\ \vdots & \ddots & \vdots \\ p''_{\mathrm{h1}} & \cdots & p''_{wh} \end{pmatrix} \tag{9}$$

Извлечение метки из стегоконтейнера

Пиксели матрицы $Cm_{w\times h}$ переводится из цветового просранства RGB в цветовое пространство HSV. Из матрицы $Ci''_{w\times h}$ извлекаем компоненту яркости v_{ij}^{CM}, создавая таким образом, новую матрицу яркостей стегоконтейнера $V_{w\times h}^{\mathrm{CM}}$. Матрица $V_{w\times h}^{\mathrm{CM}}$ переводится в матрицу-строку V_{wh}^{CM}. Над матрицей-строкой V_{wh}^{CM} проводится быстрее преобразование Фурье $FFT()$. В результате получаем матрицу-строку Z_{wh}^{CM}: Матрицу-строку Z_{wh}^{CM} переводят в матрицу $Z_{w\times h}^{\mathrm{CM}}$ размерности $w \times h$ путем перевода каждых w элементов матрицы из Z_{wh}^{CM} на новую строку. Из матрицы $Z_{w\times h}^{\mathrm{CM}}$ составляется матрица $Z'^{\mathrm{CM}}_{w\times h}$ путем выделения действительной части z_{ij}^{CM}. Создаем матрицу изображения дешифрованного стегоконтейнера $Cz_{w\times h}^{\mathrm{CM}}$, в которой пиксели заданы в формате HSV, значения H и S в котором выставлены в 0, а значение V взято из матрицы $Z'^{\mathrm{CM}}_{w\times h}$:

$$Cz_{w\times h}^{\mathrm{CM}} = \begin{pmatrix} p_{11}^{M}(h_{11}, s_{11}, z_{11}^{\prime CM}) & \cdots & p_{w1}^{M}(h_{w1}, s_{w1}, z_{w1}^{\prime CM}) \\ \vdots & \ddots & \vdots \\ p_{1l}^{M}(h_{1h}, s_{1h}, z_{1h}^{\prime CM}) & \cdots & p_{wh}^{M}(h_{wh}, s_{wh}, z_{wh}^{\prime CM}) \end{pmatrix} \tag{10}$$

Переводим пиксели матрицы $Cz_{w\times h}^{\mathrm{CM}}$ из формата HSV в формат RGB, получаем таким образом визуальное изображение $Czi_{w\times h}^{\mathrm{CM}}$. По визуальному изображению находим искомое сообщение M.

3. Примеры работы алгоритма.

Отработаем вышеописанный алгоритм на четырех изображениях Ci_1, Ci_2, Ci_3, Ci_4, сгенерированных нейросетью, размерностью 1024×576. Изображения (рис. 1) подобраны с разной цветовой нагрузкой и разной тематикой.

Рис.1 Изображения-контейнеры Ci_1, Ci_2, Ci_3, Ci_4

В каждый из них необходимо встроить в контейнер сообщение M: «АВТОРСКОЕ ПРАВО» и, в дальнейшем, извлечь его из полученной стеганограммы. Ниже приведены визуальные примеры матриц $Z_{w\times h}^{CM}$ для со встроенной меткой M, для каждого из контейнеров (рис. 2).

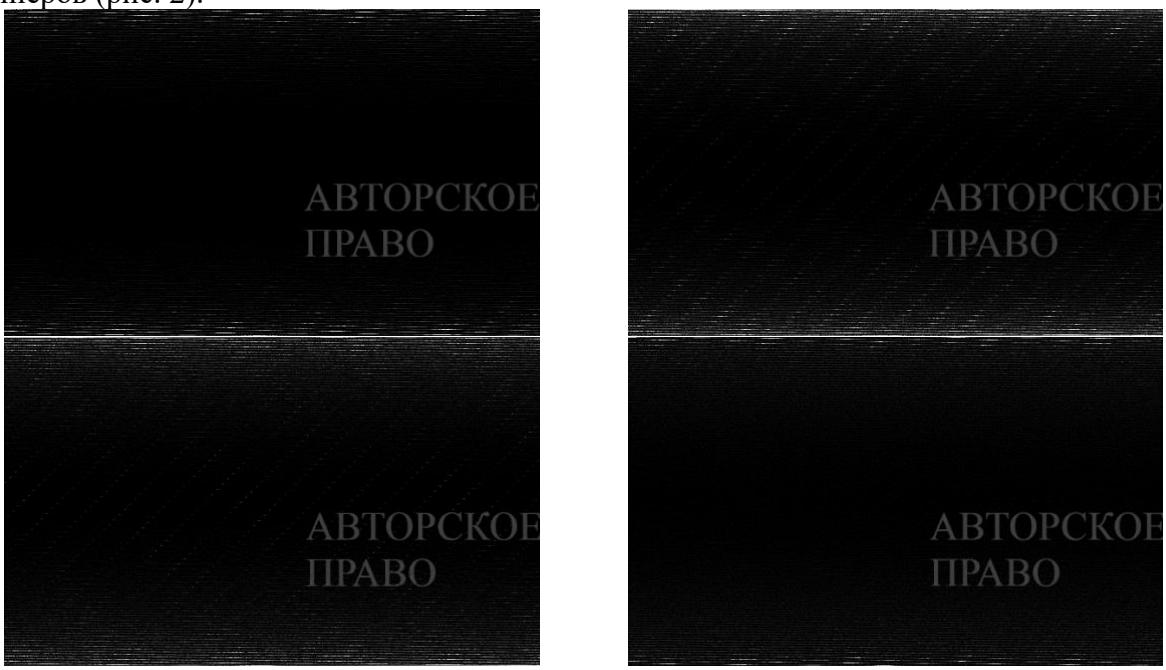


Рис.2 Визуальные изображения матриц $Z_{1\,w\times h}^{CM}, Z_{2\,w\times h}^{CM}, Z_{3\,w\times h}^{CM}, Z_{4\,w\times h}^{CM}$

В результате работы алгоритма, получим стеганограммы $Cm_{w\times h}$ для каждого из изображений (рис. 3).

Рис.3 Стеганограммы $Cm_{1\,w\times h}$, $Cm_{2\,w\times h}$, $Cm_{3\,w\times h}$, $Cm_{4\,w\times h}$.

Изображения извлеченных меток из стеганограмм $Czi^{\mathrm{CM}}_{w\times h}$ представлены ниже (рис. 4).

Рис.4 Изображения извлеченных меток $Czi^{\mathrm{CM}}_{1\,w\times h}$, $Czi^{\mathrm{CM}}_{2\,w\times h}$, $Czi^{\mathrm{CM}}_{3\,w\times h}$, $Czi^{\mathrm{CM}}_{4\,w\times h}$.

4. Сравнение с другими алгоритмами

Сравнение нашего алгоритма цифровой голографии (ЦГ) производилось со следующими популярными стеганографическими алгоритмами (табл. 1): LSB [4], F5 [5-7], Jsteg [8-10], дифференциально яркостной ячеистый алгоритм (Digital Brightness Cell Algoritm, DBCA) [11], Куттера [12-14], Patchwork [15-17], Голография Фурье в синем спектре XYZ (Hologhrafy Furie Blue, HFB).

В качестве оценки выбралось способность алгоритмов противостоять различным видам атак на стеганограмму. В поле стойкость ставится:

«+» - если стеганограмма, закодированная данным алгоритмом, выдержала атаку, при декодировании метка была успешно извлечена.

«−» - если стеганограмма, закодированная данным алгоритмом, не выдержала атаку, при декодировании метка не была успешно извлечена.

«$\mp$» - если стеганограмма, закодированная данным алгоритмом, выдержала атаку, но при декодировании получились неясные результаты, метка была извлечена частично или в некоторых изображениях она извлекается полностью, в некоторых не извлекается вообще.

Таблица 1.

Сравнение уязвимости от атак алгоритмов цифровой голографии

	LSB	F3	Jsteg	DBCA	Куттера	Patchwork	HFB	ЦГ
Конверсия в другие форматы	+	−	−	+	∓	∓	+	+
Вырезание частей из стеганограммы	−	−	−	+	∓	∓	+	+
Обрезание части стеганограммы	−	−	−	+	∓	∓	−	+
Ухудшение качества стеганограммы	−	−	−	−	∓	∓	+	+
Изменение яркостных характеристик стеганограммы	−	−	−	−	∓	∓	−	+
Атака белым шумом	−	−	−	−	∓	∓	−	+

Заключение

В статье была подробно описан алгоритм создания стеганограммы БПФ, был приведен алгоритм извлечения метки из созданной стеганограммы.

Представлены примера работы описанного алгоритма на примере четырёх различных контейнеров разного тематического содержания и цветовой гаммы.

Проведена экспериментальная часть, которая сравнивает новый алгоритм с семью популярными стеганографическими алгоритмами. Показана стойкость алгоритма к шести различным видам виду атак на стеганограмму.

Однако, в статье не раскрыта возможность подбора яркостных характеристик для матрицы яркостей контейнера $V_{k\times l}^{M}$, поскольку при бинарных значениях $\{0,1\}$, качество стеганограммы и извлекаемой метки будет вирироваться, в зависимости от контекста контейнера Ci, что предстоит исследовать в дальнейших работах.

Литература

1. Голд Б., Рэйдер Ч. Цифровая обработка сигналов. М.: Сов. радио, 1973. 368 с.

2. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов. Москва: Мир, 1989. 448 с.

3. Власенко В.А., Лаппа Ю.М., Ярославский Л.П. Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов. М.: Наука, 1990. 180 с.

4. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.

5. Westfeld A. F5—A Steganographic Algorithm // Technische Universit¨at Dresden, Germany, 2001. DOI: 10.1007/3-540-45496-9_21

6. Jicang Lu and another. Recognizing F5-like stego images from multi-class JPEG stego images // KSII Transactions on Internet and Information Systems, 2014, v. 8, pp. 4153-4169. DOI: 10.3837/tiis.2014.11.028.

7. Brūzgienė Rasa and another. Enhancing Steganography through Optimized Quantization Tables // Electronics, 2024, 13, 2415. DOI: 10.3390/electronics13122415.

8. Qiao, Tong and another. Steganalysis of JSteg algorithm using hypothesis testing theory // EURASIP Journal on Information Security, 2015. DOI: 10.1186/s13635-015-0019-7.

9. Binmin P., Qiao, and another. Novel Hidden Bit Location Method towards JPEG Steganography // Security and Communication Networks, 2022. DOI: 10.1155/2022/8230263.

10. Jie W., Chunfang Y., Ping W. and another. Payload location for JPEG image steganography based on co-frequency sub-image filtering // International Journal of Distributed Sensor Networks, 2020, 16. DOI: 10.1177/1550147719899569.

11. Крамаренко С.М. Способ внесения цифровых меток в цифровое изображение и устройство для осуществления способа. RU2739936C1 Роспатент, 2020.

12. Hartung F., Kutter M. Multimedia Watermarking Techniques // Proceedings of the IEEE, vol. 87, no. 7, 1999.

13. Kiseleva, A., Kudrina, M. Computer-aided system of data protection by steganography methods, 2014, pp. 277-284. DOI: 10.18287/1613-0073-2015-1490-277-284.

14. Zhigalov, I.E., Ozerova, M.I., Evstigneev, A.V. Application of Cutter–Jordan–Bossen method for data hiding in the image spatial area // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2022. 23. С. 16-23. DOI: 10.14529/ctcr230302.

15. Yeo, In-Kwon and another Generalized patchwork algorithm for image watermarking. // Multimedia Systems, 2003, 9, pp. 261-265. DOI: 10.1007/s00530-003-0097-0.

16. Perdana, A. H., Rahim, R. Application of Invisible Image Watermarking, 2018, DOI: https://doi.org/10.31219/osf.io/9z7du

17. Кушнеревич, П. М. Анализ эффективности алгоритмов Patchwork и LSB для защиты графических образов с помощью водяных знаков // Интеграция науки, общества, производства и промышленности: проблемы и перспективы: сборник статей по итогам Международной научно-практической конференции, Волгоград, 2021. С. 121-124.

Copyright protection using digital holography

Bykov A.Yu. [154]**, Sysoev V.V.** [155]**,**

This article is devoted to digital steganography based on FFT. The article describes an algorithm for encrypting a label into a container and extracting an encoded label from a steganogram. Examples of the operation of the described algorithm are presented. A comparison is made with other popular steganographic algorithms. The algorithm's resistance to various types of attacks on the steganogram is shown.

Keywords: steganography, Fourier holography, digital mark.

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

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

УДК 004.94

Разработка методики трассировки стека программы с использованием пошаговой эмуляции

Титов А.С.[156], Кутаев К.С.[157],

Данная работа посвящена разработке методики, целью которой является получение информации о функциях программы в процессе её выполнения. Рассматриваются программы с отсутствующим исходным кодом и их выполнение в эмулирующей среде. Приводится описание способов выполнения низкоуровневых (ассемблерных) функций некоторыми процессорными архитектурами, в частности, AMD64, MIPS64 и ARMv7. На основе этих способов предложена методика, предназначенная для трассировки стека программы без исходного кода, выполняемой в эмулирующей среде. Методика реализована программно для процессорной архитектуры AMD64 в эмуляторе программно-аппаратных платформ Korycat. Получен практический результат для функций, вызываемых в эмулируемом ядре операционной системы Linux, скомпилированной без отладочной информации. Разработанная методика трассировки стека позволяет повысить точность определения функций в процессе динамического анализа программного обеспечения с отсутствующим исходным кодом для разных процессорных архитектур.

Ключевые слова: информационная безопасность, исполняемый файл, чёрный ящик, анализ поведения программ, динамический анализ, исследование программ

Введение

В современном мире всё больше расширяется спектр разрабатываемого программного обеспечения и программно-аппаратных устройств с разными процессорными архитектурами, в которых оно используется. Одной из категорий программного обеспечения является так называемый «чёрный ящик» – программы, распространяемые разработчиками без предоставления исходного кода. Подобные программы могут быть вредоносными и распространяться злоумышленником, что порождает необходимость подробного исследования этой категории программ специалистами [1-4]. Для исследования используют различные методы, например, выделение функций в программе [5, 6] и построение графа, отражающего последовательность вызовов этих функций [7, 8].

В настоящей работе для выделения функций и информации об их последовательности вызовов предлагается использовать *трассировку стека* – анализ данных, находящихся в стеке вызовов процессора, с целью получения информации о вызванных функциях.

При исследовании программ категории «чёрный ящик» в контексте информационной безопасности нередко используют инструменты для *пошаговой эмуляции программы* – симуляции выполнения низкоуровневых инструкций программы [9-11]. В настоящей работе применение эмуляции позволяет, во-первых, выполнить трассировку стека в произвольный момент выполнения программы и, во-вторых, исследовать программное обеспечение независимо от процессорной архитектуры устройства, на котором выполняется эмуляция.

Таким образом, разрабатываемая методика позволит получать информацию о вызванных функциях в эмулируемой программе с отсутствующим исходным кодом независимо от процессорной архитектуры, на которой выполняется эмуляция. Это, в свою

[156] Титов Анатолий Сергеевич, аспирант, МГТУ им. Н. Э. Баумана, Москва. toliakpurple@gmail.com
[157] Кутаев Кирилл Сергеевич, аспирант, МГТУ им. Н. Э. Баумана, Москва. kirSM2010@gmail.com

очередь, позволит более точно определять функции в процессе исследования безопасности программ.

Ниже рассмотрен способ выполнения низкоуровневых функций процессорными архитектурами AMD64, MIPS64 и ARMv7. Далее описана методика трассировки стека программы с использованием пошаговой эмуляции. Затем показана практическая реализация методики и полученные результаты трассировки функций эмулируемого ядра Linux.

1. Низкоуровневое выполнение функций

В этой работе *стек вызовов процессора* рассматривается как область оперативной памяти, используемая для хранения локальных переменных и адресов возврата функции.

Шаг эмуляции программы – выполнение одной инструкции процессора.

Введём следующие обозначения:

- «RA» – адрес возврата из текущей функции;
- «PC» – адрес последней выполненной процессорной инструкции;
- «SP» – адрес стека;
- «prevRA» – адрес возврата из текущей функции для предыдущего шага;
- «prevPC» – адрес предыдущего шага выполнения программы;
- «prevSP» – адрес стека на предыдущем шаге выполнения программы.

Операцией $[SP]$ обозначим обращение к оперативной памяти по указанному адресу (например, SP).

Далее рассмотрены процедуры сохранения адреса возврата и работы со стеком процессорной архитектуры AMD64, MIPS64 и ARMv7 при вызове функции и возврате из функции.

Вызов (1) и возврат (2) из функции в архитектуре AMD64 реализуется, как правило, командами «call» и «ret». Отметим, что в архитектуре AMD64 отсутствует регистр для сохранения адреса возврата из текущей функции, а операции вызова и возврата из функции размещают этот адрес в стеке.

$$\begin{gathered}[SP] := PC + < \text{длина текущей процессорной инструкции} > \\ SP := SP + 8 \\ PC := < \text{адрес вызванной функции} >\end{gathered} \quad (1)$$

$$\begin{gathered}PC := [SP] \\ SP := SP - 8\end{gathered} \quad (2)$$

Вызов (3) и возврат (4) из функции в архитектуре MIPS64 и ARMv7 обычно реализуется в соответствии с выражениями, представленными ниже.

$$\begin{gathered}RA := PC + < \text{длина текущей процессорной инструкции} > \\ PC := < \text{адрес вызванной функции} >\end{gathered} \quad (3)$$

$$PC := RA \quad (4)$$

Приведённые процедуры являются основой для разработки методики.

Ниже (рис.1) приведён пример содержащейся в стеке информации для скомпилированной для архитектуры AMD64 программы с известным исходным кодом. Показана таблица адресов стека (слева) и исходный код (справа). Информация в стеке показана на момент вызова функции printf (строка 28). Цветами выделены адреса возврата из функций, сохранённые в стеке и соответствующие участки исходного кода.

Адрес стека	Значение	Комментарий
00007FFFFFFDAC0	0000504000000010	
00007FFFFFFDAC8	0000003C00000000	
00007FFFFFFDAD0	00007FFFFFFDAF0	
00007FFFFFFDAD8	00005555556B3B65	Адрес возврата в foo
00007FFFFFFDAE0	0000000000000000	
00007FFFFFFDAE8	0000001E00000010	
00007FFFFFFDAF0	00007FFFFFFDB10	
00007FFFFFFDAF8	00005555556B3B49	Адрес возврата в sum
00007FFFFFFDB00	0000555556047400	
00007FFFFFFDB08	0000000A00000014	
00007FFFFFFDB10	00007FFFFFFDB30	
00007FFFFFFDB18	00005555556B3B1D	Адрес возврата в start
00007FFFFFFDB20	0000504000000010	
00007FFFFFFDB28	0000000A00000014	
00007FFFFFFDB30	00007FFFFFFDB50	
00007FFFFFFDB38	00005555556B3AEE	Адрес возврата в main
00007FFFFFFDB40	00007FFF7FFD000	
00007FFFFFFDB48	000000000000000A	
00007FFFFFFDB50	00007FFFFFFDBF0	
00007FFFFFFDB58	00007FFFF7C9AC88	Адрес возврата в __libc_start_main

```c
#include <stdio.h>

void start(int a);
void sum(int c, int d);
void foo(int e);
void bar(int f);

int main() {
    int a = 10;
    start(a);
    return 0;
}

void start(int a) {
    int b = 20;
    sum(a, b);
}

void sum(int c, int d) {
    foo(c + d);
}

void foo(int e) {
    bar(e * 2);
}

void bar(int f) {
    printf("result = %d\n", f);
}
```

Рис.1. Демонстрация информации в стеке для программы с известным исходным кодом

2. Описание методики

Как было показано выше, процедура вызова и возврата из функции специфична для любой процессорной архитектуры, а значит и процедура обнаружения вызова функции будет также специфична. Отметим, что входными данными этой процедуры являются: RA, PC, SP, prevRA, prevPC, prevSP. А выходное значение процедуры: 1 – если на текущем шаге эмуляции программы была вызвана функция; 0 – иначе.

Входными данными методики являются:

- эмулируемое программное обеспечение;
- PC начала выполнения эмуляции и PC окончания;

Выходными данными методики является массив (множество значений) DATA с данными о вызванных функциях.

Приведена структурная схема потока данных методики (рис.2). Буфером названа некоторая структура данных, которая для каждого шага выполнения программы возвращает текущее и предыдущее значение (например, RA).

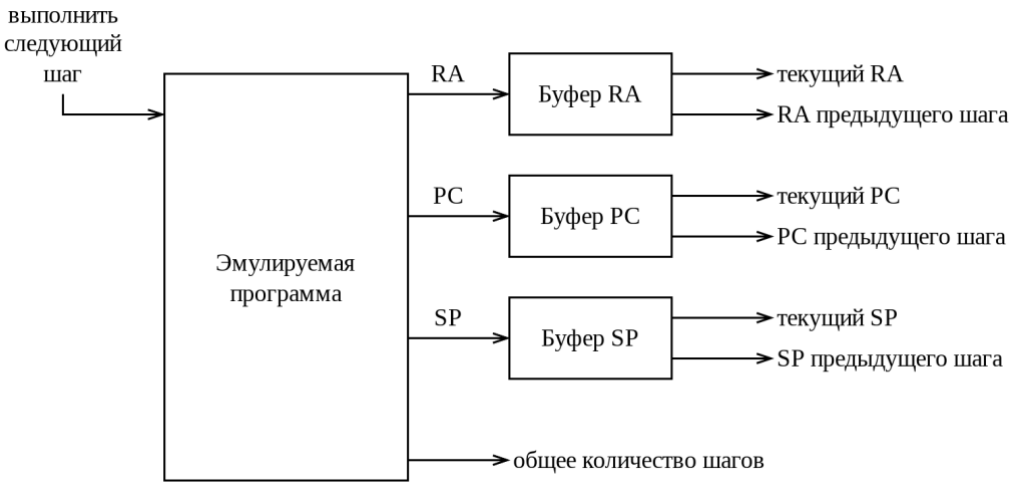


Рис.2. Структурная схема потока данных методики

Приведена последовательность действий методики (рис.3). Заметим, что для архитектуры AMD64 в качестве RA используется значение $[SP]$.

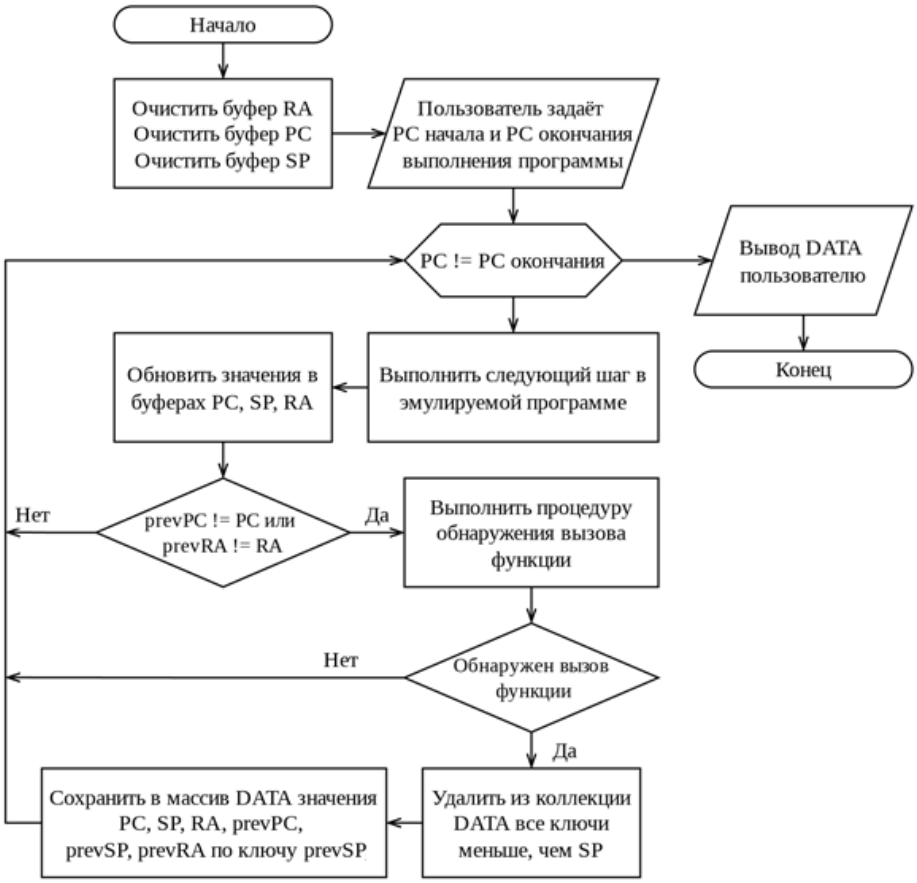


Рис.3. Последовательность действий методики

Процедура обнаружения вызова функции включает в себя проверку корректности значения, расположенного в RA – оно должно отличаться от prevPC на некоторое фиксированное значение ε: $|RA - prevPC| < \varepsilon$.

Также данная методика может быть расширена процедурой обнаружения возврата из функции, который будет состоять из проверки выполнения условия (5):

$$DATA[SP].RA = PC \quad (5)$$

Процедура обнаружения вызова функции и возврата из неё может быть дополнена или изменена в зависимости от исследуемой процессорной архитектуры. Тем не менее, использование методики с этими процедурами позволяет получить информацию о функциях программы в процессе её выполнения.

3. Пример реализации методики в эмуляторе Kopycat

Среди всего множества эмуляторов программного обеспечения, к которым, например, относят QEMU, Unicorn или Kopycat. Для программной реализации методики выбран эмулятор Kopycat. Это связано с удобным интерфейсом дополнения эмулятора и встроенными возможностями динамического внесения изменений в эмулирующую среду [12-14].

В качестве эмулируемой процессорной архитектуры выбрана AMD64. Значение ε задано равным 32. Также процедура обнаружения вызова и возврата из функции дополнена условием (6):

$$prevSP \neq SP \quad (6)$$

Методика и процедура реализована программно на языке Kotlin в библиотеке «ru.inforion.lab403.kopycat.runtime.analyzer.stack». Продемонстрирован пример результата выполнения для функции «isa_bus_init» скомпилированного без отладочной информации ядра Linux 4.3.15 (рис.4).

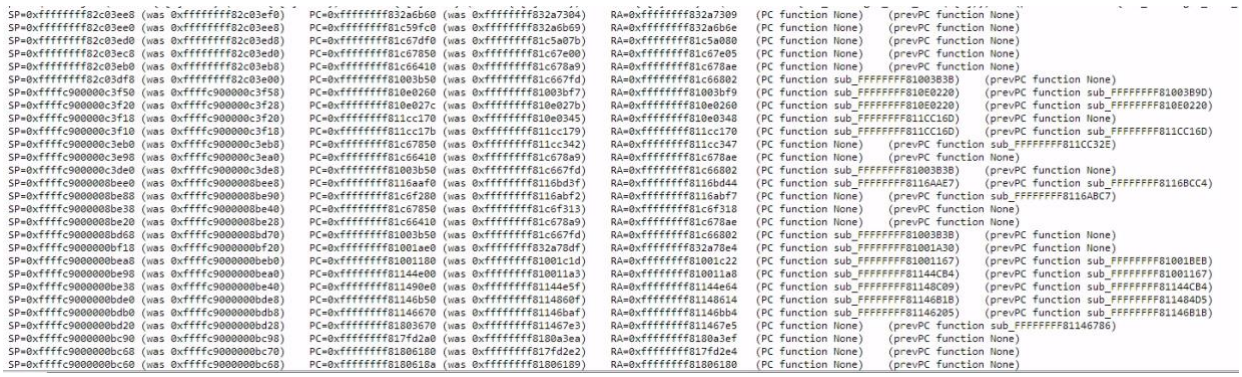


Рис.4. Пример выходных данных методики

Полученный результат в полной мере демонстрирует возможность методики трассировки стека пошагово эмулируемой программы получать информацию о вызываемых в программе функциях. Методика может быть применена к любому программному обеспечению категории «чёрный ящик» и позволяет улучшить точность определения функций в процессе динамического анализа.

Выводы

В этой работе была рассмотрена методика трассировки стека пошагово эмулируемой программы, которая позволяет получать информацию о функциях в процессе выполнения программы. Разработка методики основана на базовых принципах вызова и возврата из низкоуровневых (ассемблерных) функций, реализованных в различных процессорных архитектурах (например, AMD64, MIPS64 и ARMv7). В работе показано описание этих принципов, приведены основные шаги разработанной методики.

На примере эмулятора программно-аппаратных платформ Kopycat продемонстрирована практическая применимость методики и получен результат получения информации о вызываемых функциях ядра Linux.

Разработка этой методики позволяет повысить точность определения функция в программном обеспечении категории «чёрный ящик», что может быть использовано в процессе исследования на наличие вредоносных функций программного обеспечения без исходного кода.

Литература

1. Аудит безопасности программ / Барабанов А.В., Вареница В.В., Марков А.С. Учебно-методическое пособие / Москва, Издательство: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2021. – 56 с.

2. Бегаев А.Н., Кашин С.В., Маркевич Н.А., др. Выявление уязвимостей и недекларированных возможностей в программном обеспечении. Учебно-методическое пособие, Университет ИТМО, Санкт-Петербург. – 38 с., 2020.

3. Водяной Д.А., Жуковский Е.В. Применение нейронных сетей в задачах обнаружения уязвимостей в программном обеспечении без исходных кодов // Методы и технические средства обеспечения безопасности информации, № 31, с. 134-136, 2022.

4. Junfeng T., Wenjing X., Zhen L. BVDetector: A program slice-based binary code vulnerability intelligent detection system // Information and Software Technology, vol. 123, 2020.

5. Bao T., Burket J., Woo M., et al. BYTEWEIGHT: Learning to recognize functions in binary code // Proceedings of the 23rd USENIX Security Symposium. USENIX Association, pp.845-860, 2014.

6. Lin W., Guo Q., Yin J., et al. FSmell: Recognizing Inline Function in Binary Code // Computer Security – ESORICS 2023, vol 14345. Springer, Cham, pp. 487-506, 2024. DOI: 10.1007/978-3-031-51476-0_24

7. Pettersen H., Morrison D. Call graph discovery in binary programs from unknown instruction set architectures // arXiv preprint arXiv:2401.07565, 2024.

8. Qiu J., Su X., Ma P. Using reduced execution flow graph to identify library functions in binary code. // IEEE Transactions on Software Engineering. 42(2), pp. 187–202, 2015.

9. Бугеря А.Б., Ефимов В.Ю., Кулагин И.И., др. Программный комплекс для выявления недекларированных возможностей в условиях отсутствия исходного кода // Труды ИСП РАН, том 31, выпуск 6, с. 33-64, 2019.

10. Коваленко Р.Д., Макаров А.Н. Динамический анализ IoT-систем на основе полносистемной эмуляции в Qemu // Труды ИСП РАН, том 33, выпуск 5, с. 155-166, 2021.

11. Liu S., Feng P., Wang S., et al. Enhancing malware analysis sandboxes with emulated user behavior // Computers and Security, vol. 115, p.24, C, 2022. DOI: 10.1016/j.cose.2022.102613

12. Аристов Р. С., Гладких А. А., Давыдов В. Н., др. Разработка программной платформы Kopycat эмуляции сложных вычислительных систем // Наноиндустрия, № S, 2019, с. 350-352.

13. Гладких А. А., Кемурджиан А.Р., Комахин М.О. Отладка и анализ устройств и приложений с операционной системой на базе Linux в эмуляторе Kopycat // Наноиндустрия, 13, № S5-2, 2020, с. 406-408.

14. Кутаев К.С., Титов А.С., Островский А.С. Изменение поведения программы путем внесения модификации в последовательность выполнения процессорных инструкций в эмулируемой среде. Безопасные информационные технологии (БИТ – 2023): материалы конференции. – Москва : Издательство МГТУ им. Н.Э. Баумана, с. 85-91. 2024.

Научный руководитель: Гордеев Эдуард Николаевич, доктор физико-математических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: werhorn@yandex.ru

Software stack tracing technique development using step-by-step emulation

Titov A.S.[158], **Kutaev K.S.** [159]

This paper is devoted to the development of a technique aimed at obtaining information about software functions during its runtime. Software execution without source code in an emulation environment is being considered. The authors describe the ways of executing low-level functions by some processor architectures, in particular, AMD64, MIPS64 and ARMv7. On the basis of these methods, the authors propose a technique intended for stack tracing of software without source code, that is being executed in an emulation environment. The technique is implemented for AMD64 processor architecture in the Kopycat hardware platform emulator. Practical results were obtained for functions called in the emulated Linux kernel compiled without debugging information. The developed stack tracing technique allows researchers to improve the accuracy of function detection during dynamic analysis of software without source code for different processor architectures.

Keywords: information security, executable binary, black-box, program behavior analysis, dynamic analysis, program research.

[158] Anatoly Titov, postgraduate student, BMSTU, Moscow. E-mail: toliakpurple@gmail.com
[159] Kirill Kutaev, postgraduate student, BMSTU, Moscow. E-mail: kirSM2010@gmail.com

УДК 004.415.52

Мониторинг операций доступа к файловой системе при сборке программного обеспечения в задачах информационной безопасности

Тихомиров Н.А.[160], Ключарёв П.Г.[161]

В данном исследовании в области безопасной разработки программного обеспечения рассматривается подход к исследованию процесса сборки программ с мониторингом дополнительных доступов в файловой системе и перспективы применимости данного подхода для обеспечения информационной безопасности с целью повышения количества полезной достоверной информации, которой располагает специалист по информационной безопасности относительно исследуемого (или контролируемого) им проекта. В результате работы было проведено прототипирование предложенного подхода с использованием помощью средства перехвата системных вызовов Strace, была успешно достигнута поставленная цель.

Ключевые слова: мониторинг сборки программного обеспечения, системные вызовы, Strace, разработка безопасного программного обеспечения.

Введение

В рамках существующих научных и прикладных исследований в области безопасной разработки программного обеспечения в целом и автоматизированного статического анализа исходного кода в частности значительное внимание уделяется технической задаче мониторинга (контроля) сборки программного обеспечения [1-3].

На сегодняшний день научные и технологические начала мониторинга сборки программного обеспечения в первую очередь прорабатываются в статусе вспомогательного механизма статического анализа. Мониторинг сборки при этом не реализует сложных операций и моделей анализа, так как акцент всего процесса в совокупности смещён как на получение результата сборки, так и на основной части статического анализа [4].

Представленное ограничение в определённой степени сужает внимание разработчиков статических анализаторов и препятствует мониторингу возникающих в ходе сборки программного обеспечения событий безопасности, связанных с привлечением неожиданных посторонних компонентов. Из практики работы с несколькими различными статическими анализаторами с реализованным механизмом мониторинга сборки мы можем заключить, что подобные события не фиксируются для оповещения пользователей, что, вообще говоря, является тёмным пятном в обеспечении безопасности разработки, работе над которым и посвящено настоящее исследование [5].

Общая часть

Подходы к мониторингу сборки могут базироваться на различных механизмах, однако в большинстве своём представляют собой фиксацию команд и аргументов запуска инструментов компиляции, которые задействуются в ходе сборки[162]. Одним из основных

[160] Тихомиров Никита Александрович, аспирант кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: nicktikhomirov02@gmail.com.

[161] Ключарёв Пётр Георгиевич, доктор технических наук, профессор кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: pk.iu8@yandex.ru

[162] В.Н. Игнатьев. Использование легковесного статического анализа для проверки настраиваемых семантических ограничений языка программирования. Труды ИСП РАН, том 22, 2012, с. 169-188. DOI: 10.15514/ISPRAS-2012-22-11.

способов сбора подобных сведений является модификация системных библиотечных функций, которые соответствуют системному вызову «execve» (в терминах POSIX-совместимых операционных систем) [6, 7].

Подобный подход можно заметить не только в коммерческих продуктах, но и в бесплатных. Например, перехват соответствующих системных вызовов реализуется в инструменте Bear (Build Ear), и в утилите из семейства технологий LLVM под названием scan-build, которая компилирует вспомогательную библиотеку для перехвата прямо в момент запуска сборки, о чём можно судить по её публично доступному исходному коду [8, 9].

Основным недостатком существующих в данной области работ является то, что мониторинг сборки в интересах статического анализа не ожидает появления в ходе сборки посторонних файлов, включая файлы, загруженные по сети, а также файлы, заимствованные из среды сборки без исходных текстов (для компилируемых языков).

Помимо ранее упомянутого системного вызова «execve», в настоящей работе к перехвату (мониторингу) также предлагаются системные вызовы семейства доступов на чтение («read», «pread64», «readv» и другие), а также на запись («write», «write64», «writev» и другие). Данный подход позволяет легко распознать нежелательные конструкции сборки, к которым можно отнести как получение файлов из сетевых источников, так и менее очевидные классы проблем сборки вроде модификации исходных (эталонных) текстов в результате сборки.

Положим, к объекту x осуществляется последовательность операций доступа $a_1, a_2 \dots a_n$. Формально говоря, если среди a_i осуществляется доступ на запись (при $i \in [1; n]$), то состояние объекта меняется, однако можно заметить, что изменение состояния объекта требует присутствия наблюдателя, – если осуществляется несколько подряд идущих доступов на запись, то они неотличимы от одного доступа на запись. Таким образом, состояния объекта x могут быть определены как элементы разбиения на множестве $a_1, a_2 \dots a_n$ при условии, что элементы эквивалентного разбиения на множестве индексов $[1; n]$ являются выпуклыми. Критерий формирования очередного состояния $\varkappa(i)$ (между элементами a_i и a_{i+1}) может быть определён из ранее приведённых соображений в соответствии с соотношением (1).

$$\varkappa(i) = \begin{cases} 1, \text{ если } (a_i \in W) \wedge (a_{i+1} \in R) \\ 0, \text{иначе} \end{cases}, \quad (1)$$

где W – семейство изменяющих данные доступов (запись в файл, открытие файла с удалением старого содержимого), R – семейство детектирующих изменение доступов (в частности, доступ на чтение).

Подобная модель позволяет обнаружить часть недостатков сборки, а кроме того, на её основе можно построить граф, в котором узлами будут являться версии файлов, а рёбрами – отношения между ними по преобразованию и по потенциальным потокам данным. По отношению (не)достижимости на таком графе можно определить, осуществляются ли в ходе сборки лишние операции.

Результаты апробации технического прототипа

Для реализации описанного подхода на базе инструмента Strace был разработан инструмент-прототип. Было проведено исследование нескольких общедоступных библиотек, включая, например, библиотеку libffi, которая используется для интерфейсов подключения нативного программного кода. Было определено, что разработанный инструмент перехвата действительно успешно собирает информацию о задействованных в ходе сборки исходных файлах. В рамках исследования не было обнаружено проектов на

нативных языках с недекларированными возможностями в области привлечения неожиданных посторонних файлов, однако это наблюдение может измениться в ходе исследования последующих программных продуктов и в ходе совершенствования предложенного подхода.

С другой стороны, в ходе испытаний было определено, что разработанный инструмент не в полной мере отвечает потребностям предложенного подхода в части языков Java-семейства, так как для получения достоверных результатов требуется проработать различные вспомогательные технологические аспекты перехвата сборки в соответствии с современными стандартами индустрии. Мониторинг сборки программ Java-семейства обычно осуществляется с использованием внедряемых в инфраструктуру сборки специальным образом спроектированных Java-агентов, которые оказывают существенную поддержку средствам мониторинга сборки через дублирование передаваемых компилятору сведений в форме отдельных процессов [1, 3].

Ещё одним интересным побочным наблюдением по результатам данной работы стало то, что выбор общедоступных библиотек для визуализации процессов сборки (графов) нельзя назвать богатым. Как одно из лучших средств для визуализации масштабных графов зарекомендовал себя фреймворк «Cosmograph», который как раз и предназначен для подобных задач [10].

Выводы

В ходе работы был предложен прототип инструмента для мониторинга сборки с учётом системных вызовов, соответствующие доступам к файлам на чтение и на запись, а также были сделаны

Исходя из общедоступных сведений о текущем развитии технологий обеспечения безопасности разработки программного обеспечения, можно заключить, что предложенный подход и соответствующий реализующий его прототип входят в число первых решений в области самостоятельного (не подчинённого статическому анализу) мониторинга процессов сборки.

В ходе испытаний разработанного прототипа не было обнаружено нарушений в процессах сборки на нативных языках программирования, однако функционирование разработанного прототипа для программ на языках Java-семейства требует дальнейшей доработки.

Литература

1. Афанасьев В.О., Бородин А.Е., Белеванцев А.А. Статический анализ для языка Scala. Труды ИСП РАН, 2024, том 36 вып. 3, с. 9–20. DOI: 10.15514/ISPRAS–2024–36(3)–1.

2. Статический анализ на основе обобщённого абстрактного синтаксического дерева / В. О. Афанасьев, А. Е. Бородин, К. И. Вихлянцев, А. А. Белеванцев // Труды Института системного программирования РАН. – 2023. – Т. 35, № 6. – С. 103-120. – DOI 10.15514/ISPRAS-2023-35(6)-6. – EDN OBIDXT.

3. Kotlin from the Point of View of Static Analysis Developer / V. O. Afanasyev, S. A. Polyakov, A. E. Borodin, A. A. Belevantsev // Programming and Computer Software. – 2023. – Vol. 49, No. 7. – P. 549-558. – DOI 10.1134/s0361768823070022. – EDN DMGBRS.

4. Бородин, А. Е. Внутрипроцедурный анализ для поиска ошибок на основе символьного выполнения / А. Е. Бородин, И. А. Дудина // Труды Института системного программирования РАН. – 2020. – Т. 32, № 6. – С. 87-100. – DOI 10.15514/ISPRAS-2020-32(6)-7. – EDN KBIJRQ.

5. Бегаев А.Н., Кашин С.В., Маркевич Н.А., Марченко А.А. Выявление уязвимостей и недекларированных возможностей в программном обеспечении. Учебно-методическое пособие. СПб.: Университет ИТМО, 2020. 38 с.

6. Вишняков А.В. Поиск ошибок в бинарном коде методами динамической символьной интерпретации: дис. … кандидата физико-математических наук 2.3.5 / Вишняков А.В. – М., 2022. – 131 с.

7. Барабанов А.В., Вареница В.В., Марков А.С. Аудит безопасности программ Учебно-методическое пособие / Москва, МГТУ им. Н.Э.Баумана, 2021. 56 с.

8. Мыльников, В. А. Автоматизация процессов поиска уязвимостей в исходном коде на этапе разработки программного приложения / В. А. Мыльников // Завалишинские чтения 23 : Сборник докладов XVIII Международной конференции по электромеханике и робототехнике, Санкт-Петербург, 18–19 апреля 2023 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2023. – С. 51-54. – DOI 10.31799/978-5-8088-1823-1-2023-18-51-54. – EDN UZZOLN.

9. Thien, T. Application of automatic code generation and fuzzing technology for C/C++ library testing / T. Thien // IX International Conference «Engineering & Telecommunication En&T - 2022» : Book of Abstracts. IX International Conference, Москва, 23–24 ноября 2022 года. – Москва: Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», 2022. – P. 36-43. – EDN TWMHPQ.

10. Xue Y., Hosobe H. CRV: A Framework for Visualizing Card Relationships in Digital Collectible Card Games // Hosei University. – 2024. – Т. 6. – С. 04.

Filesystem access operations monitoring application to software build process from the perspective of information security problems

Tikhomirov N.A.[163], Klyucharev P.G.[164]

The article in the field of secure software development lifecycle dwells on an approach for software build process analysis with an extended range of monitored filesystem accesses as well as on information security enforcement prospects of such approach. The goal of the article is a growth in quantity of useful trustful information about a monitored project that information security expert is able to work with. As a result, an implementation prototype was developed with use of system call monitoring tool Strace and the goal was reached.

Keywords: software build process monitoring, system calls, Strace, secure software development lifecycle.

[163] Tikhomirov Nikita A., doctoral student of the «Information Security» department, Bauman Moscow State Technical University, Moscow, Russia. E-mail: nicktikhomirov02@gmail.com.

[164] Klyucharev Petr G., D.Sc., professor of Information Security department, Bauman Moscow State Technical University, Moscow, Russia. E-mail: pk.iu8@yandex.ru

УДК 004.451.83

Обеспечение доверенной среды и управления доступом в экосистеме транспортных средств: подходы и решения на базе кибериммунного автомобильного шлюза безопасности

Фадин А.А.[165]

В данной работе представлены результаты исследования в области кибербезопасности подключенных транспортных средств. Рассматриваются подходы к разграничению доступа между электронными блоками управления (ЭБУ) автомобиля и внешней экосистемой, а также создание доверенной среды с использованием кибериммунного автомобильного шлюза безопасности. Описаны примеры реализации разграничения доступа на основе компонентов PDP, PIP, PAP, с применением модели доступа ABAC и пятимерного пространства Хартсона. Показано, как осуществляется динамическое изменение политик безопасности, что позволяет повысить уровень защиты систем управления автомобилем и обеспечить соответствие требованиям UN R155 и ISO/SAE 21434.

Ключевые слова: управление доступом, ABAC, автомобильная кибербезопасность, шлюз безопасности, телематика, измеримая загрузка, MQTT, подключенный автомобиль

Введение

Современные автомобили превратились в сложные киберфизические системы, интегрированные в экосистему автопроизводителя (OEM), владельцев автопарков и потребителя. Развитие новых бизнес-моделей, таких как «Mobility as a Service», появление отдельных платных функций, таких как подписки и маркетплейсы приложений (в т.ч. от сторонних поставщиков), потребовало сделать автомобили подключенными и динамически обновляемыми по воздуху (OTA, Over-the-Air). Это коренным образом изменило EE архитектуру электронных блоков автомобилей (ЭБУ), увеличив поверхность атаки для потенциальных злоумышленников и разнообразие угроз для владельцев и производителей авто [5].

Особенности угроз в автоиндустрии заключаются в том, что автомобили подключены к интернету и обладают критически важными функциями, что делает их привлекательной целью для атак как в аспекте кибербезопасности (cybersecurity), так и функциональной безопасности (safety). Примеры реальных атак на автомобили Jeep Cherokee, Tesla, Nissan, Mercedes, Kia показывают важность внедрения систем защиты [4]. В ответ индустрия внедряет стандарты и регуляции, такие как UN R155/R156, новые китайские стандарты серии GB/T, ISO/SAE 21434, а также американские стандарты серии NIST SP800, требующие коренного изменения процедур разработки и управления в части кибербезопасности транспортных средств. Также идёт гармонизация нормативной базы и в Российской Федерации со стороны ФГУП «НАМИ».

Методы, материалы, результаты

1. Особенности модели угроз для автомобильной экосистемы

Автомобили подключены к интернету и обладают критически важными функциями, что делает их привлекательной целью для атак, как в аспекте кибербезопасности (cybersecurity), так и в аспекте функциональной безопасности (safety), включая защиту жизни и здоровья людей, а также окружающей среды. Административные меры с ограничением доступа зачастую не работают, так как существует множество сценариев для внедрения и начала атак (например, в рамках car-sharing, valet parking, такси), где злоумышленник имеет прямой доступ к электронным блокам и их разъёмам в салоне авто (фазы MITRE ATT&CK: Initial Access, Exploitation). При этом любой злоумышленник

[165] Фадин Андрей Анатольевич, АО "Лаборатория Касперского", г. Москва, fadin.andrey@gmail.com

может получить в своё полное распоряжение серийный автомобиль и провести сколь угодно детальный reverse engineering для планирования последующей атаки (фазы MITRE ATT&CK: Discovery и Attack Planning).

2. Подключенный автомобильный шлюз безопасности как решение для защиты от таких угроз

Для обеспечения доверенной среды и эффективного управления доступом предлагается использовать кибериммунный автомобильный шлюз безопасности. В классической распределённой (distributed) и даже в некоторых централизованных (domain centralized) архитектурах автомобиля задачи защищенной связи с облаком и маршрутизации сетевого трафика (CAN/LIN/Ethernet и т.п.) внутри авто выполняли разные ЭБУ. Как правило это телематический блок (TCU, Telematic Control Unit) и центральный шлюз (CGW, Central Gateway), они предоставлялись разными поставщиками (Tiers), не были интегрированы друг с другом и зачастую не имели зрелых механизмов безопасности [7]. Подключенный автомобильный шлюз безопасности (SGW, Secure Gateway) выполняет функции телематического блока и центрального шлюза, обеспечивая безопасность данных и взаимодействий внутри и вне автомобиля.

Основные задачи шлюза:

- Разграничение доступа между различными ЭБУ (с преобразованием между разными протоколами связи):
    - Кузовные ЭБУ — примеры: Engine Control Unit (ECU), Body Control Module (BCM), Transmission Control Module (TCM), которые коммуницируют на основе сигналов в шинах связи CAN, LIN.
    - Полнофункциональные (richOS) ЭБУ с сервисно-ориентированной архитектурой — Infotainment (IVI), Advanced Driver Assistance Systems (ADAS) с протоколами MQTT, DDS, SOME/IP.
- Разграничение доступа к функциям автомобиля со стороны субъектов из внешней экосистемы:
    - Автосервисов с доступом к автомобилю через диагностический разъём (OBD-II)
    - Приложений (от сторонних поставщиков), установленных на электронном блоке IVI (In-Vehicle Infotainment, мультимедийная система автомобиля, обеспечивающая доступ к информационно-развлекательным сервисам).
    - Мобильных устройств водителя, подключающихся к автомобилю через Bluetooth или облако OEM.
    - Облачных сервисов:
        - Облачные сервисы самого OEM.
        - Облачные сервисы владельцев автопарков (например, carsharing, логистика).
        - Сторонние облачные сервисы партнёров, например OTA (Over-the-Air) — обновление по воздуху, или же онлайн-диагностика (SoVD, Service-oriented Vehicle Diagnostics и DOTA, Diagnostics Over-the-Air).
- Обеспечение доверенной среды:
    - Доверенная загрузка самого ЭБУ шлюза безопасности (Secure Gateway) от HSM (Hardware Security Module) до уровня приложений.
    - Контроль времени (внутренняя синхронизация).
    - Защищенное хранилище данных и мониторинг кибербезопасности (Vehicle SOC).

Также для обеспечения доверенной загрузки шлюза и других ЭБУ используется подход, описанный в работе [3].

Модель безопасности

Требования к политике безопасности и выбор модели

Шлюз безопасности (SGW) реализует унифицированную модель безопасности внутри автомобиля. Ключевой момент заключается в том, что доступ должен работать с учетом изменения состояния автомобиля. Основные цели и задачи политики безопасности заключаются в следующем:

- **Основные цели политики безопасности**:
  - Определить условия, при которых автомобиль и его системы находятся в безопасном состоянии.
  - Задать четкие границы доступа, разграничивая права для разных субъектов (например, водителей, приложений, облачных сервисов), как и для других типов информационных систем [2, с. 34].
- **Основные задачи политики безопасности**:
  - Обеспечение защиты данных и функций автомобиля от несанкционированного доступа.
  - Управление доступом к функциям автомобиля с учетом динамики изменения состояния (например, при переходе из режима парковки в режим движения).
  - Применение ограничений на основе бизнес-логики производителя, включая соблюдение политик безопасности в зависимости от ситуации.
- **Применение модели в динамическом изменении политики безопасности**:
  - **Текущее состояние автомобиля**: В зависимости от состояния автомобиля (движение, диагностика, парковка) меняются разрешения на доступ к функциям и данным. Например, в режиме «движение» доступ к функциям, которые не связаны с безопасностью, может быть ограничен для минимизации отвлекающих факторов.
  - **Добавление новых субъектов доступа**: При появлении нового субъекта (например, приложение или пользователь) модель безопасности обновляет политики для учета новых прав и ограничений.
  - **Появление новых объектов доступа**: При добавлении нового объекта (например, новой функции или блока управления) политика безопасности адаптируется для учета и защиты нового элемента.
  - **Изменение полномочий субъектов**: При изменении ролей и прав субъектов (например, изменение прав владельца или арендатора автомобиля) модель обновляет соответствующие политики для контроля доступа.

На основе требований к модели безопасности был выбран подход с использованием пятимерного пространства безопасности по Хартсону [1]. Пятимерное пространство безопасности позволяет структурировать и управлять безопасностью в автомобиле, учитывая различные параметры системы. Комбинация с моделью доступа ABAC (Attribute-Based Access Control) позволяет адаптировать доступ в зависимости от контекста и состояния системы.

Пятимерное пространство Хартсона определяется множествами:

- **A (Authority)** — Полномочия субъектов, определенные OEM, включая доступ к функциям автомобиля.
- **U (Users)** — Субъекты доступа, такие как водители, пассажиры, приложения, облачные сервисы.
- **E (Operations)** — Операции, выполняемые над объектами, такие как чтение, запись, удаление и другие.
- **R (Resources)** — Ресурсы автомобиля, например, CAN шина, данные из хранилища, диагностические данные.
- **S (States)** — Состояния автомобиля (например, движение, диагностика), определяющие текущий уровень доступа.

Доступ рассматривается как запрос:

где , , , . Система находится в безопасном состоянии, если все запросы соответствуют политике безопасности и не выходят за пределы заданного пространства.

Компоненты управления доступом

Механизмы управления доступом реализуются через следующие компоненты:

- PDP (Policy Decision Point) — принимает решения о предоставлении доступа на основе политик безопасности.
- PEP (Policy Enforcement Point) — обеспечивает исполнение решений PDP, контролируя доступ субъектов к ресурсам.
- PIP (Policy Information Point) — предоставляет PDP информацию об атрибутах субъектов и ресурсов.
- PAP (Policy Administration Point) — отвечает за администрирование и управление политиками безопасности.

Условия применения модели доступа

Модель доступа должна предоставлять возможности смены текущих разрешений (политик безопасности) по одному из событий извне:

- изменение состояния автомобиля (переход в режим drive, stop, diagnostic и т.д.);
- появление нового субъекта доступа (пользователь или приложение);
- появление нового объекта доступа;
- изменение полномочий субъекта доступа;

В каждый конкретный момент доступа должнf быть явно определённа политика безопасности, описывающая разрешённые доступы. Субъекты обращаются к ресурсам за объектами доступа через PEP (Policy Enforcment Point) модули, которые применяют политику, получаемую от PDP (Policy Decision Point).

Таким образом PDP обладает полнотой информации о текущих разрешениях. Текущая Матрица доступа PDP представлена в табл. 1.

Таблица 1.

Матрица доступа

	Ресурс 1	Ресурс 2	Ресурс 3	Ресурс 4	Ресурс 5
Субъект 1	R/W				
Субъект 2	R		W		D
Субъект 3			R	L/R/W	
Субъект 4			R		

Модуль PAP управляет политиками PDP и переконфигурирует политику безопасности по одному из событий, описанных выше. Таким образом получается Обновленная Матрица доступа PDP в табл. 2.

Таблица 2.

	Ресурс 1	Ресурс 2	Ресурс 3	Ресурс 4	Ресурс 5
Субъект 1	R/W				
Субъект 2			R		
Субъект 3		L/R/W			
Субъект 4					

Область безопасности

Область безопасности в данной модели представляет собой **декартово произведение** данных наборов:$A \times U \times E \times R \times S$. **Доступ** в модели рассматривается как

ряд запросов, осуществляемых субъектами u для выполнения операций e над ресурсами R в то время, когда система находится в состоянии s. Запрос на доступ представляется четырехмерным кортежем: $(q = (u, e, R, s)), (u \in U, e \in E, s \in S, r \subseteq R)$

. Таким образом, запрос на доступ – подпространство четырехмерной проекции пространства безопасности. Запросы получают право на доступ в том случае, когда они полностью заключены в соответствующие подпространства.

Система находится в безопасном состоянии — означает, что все запросы на доступ к объектам соответствуют заданной политике **в каждый момент времени**, и не существует запроса, выходящего за пределы четырехмерного кортежа: $q = (u, e, R, s)$.

Реализация модели безопасности

Для определения доступа к объекту или выполнения действия используется бизнес-правило, которое представляет собой логическое выражение, оперирующее атрибутами (роль пользователя, состояние автомобиля и т.п.) и константными значениями (VIN и т.п.). Результатом вычисления этого логического выражения является булево значение, представляющее из себя один из двух вариантов ответа: «Да» или «Нет». Вердикт о доступе выносит PDP, основываясь на бизнес-правилах, полученных от PAP. Правила подготавливаются OEM исходя из бизнес модели и требований безопасности.

Текущие значения атрибутов PDP узнаёт от компонентов PIP. При изменении значении атрибутов PIP уведомляет PDP о необходимости смены текущей политики безопасности. После пересчёта политики с новыми значениями атрибутов, PDP транзакционно транслирует новую политику в компоненты PEP.

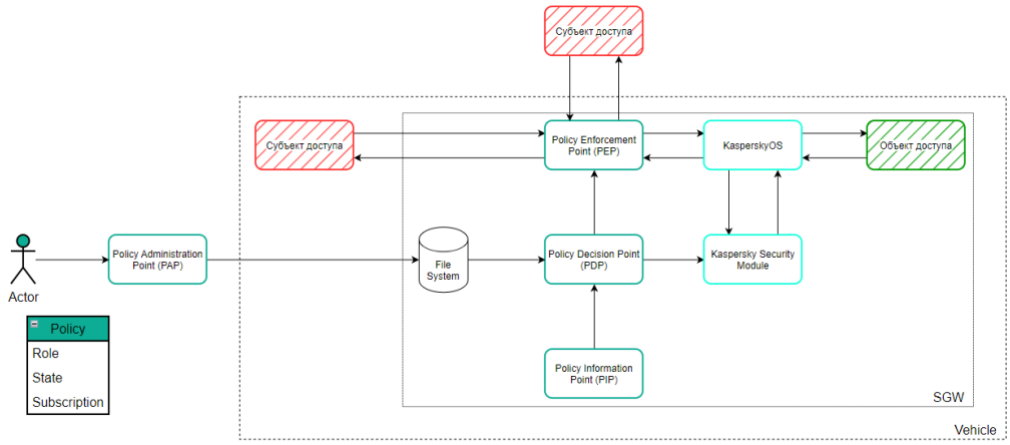


Рис.1. Взаимодействия компонентов шлюза SGW , связанных с реализации политики безопасности

Смена политик безопасности

Модель доступа должна предоставлять возможности смены текущих разрешений (политик безопасности) в ответ на следующие события:

1. **Изменение состояния автомобиля**: Это событие может вызвать изменение политик безопасности, чтобы учитывать изменение контекста доступа в зависимости от состояния автомобиля (например, режим "drive" может требовать более строгих правил доступа, чем режим "stop").
2. **Появление нового субъекта доступа**: Появление новых пользователей или приложений может потребовать обновления политик безопасности для учета новых субъектов и их прав доступа.

3. **Появление нового объекта доступа**: Если новые объекты доступа внедряются в систему, то нужно обновить политики безопасности, чтобы учесть эти объекты и их доступ.
4. **Изменение полномочий субъекта доступа**: Когда полномочия субъектов изменяются, это также может потребовать обновления политик безопасности, чтобы отразить новые права и ограничения.

Важно отметить, что шлюз безопасности (SGW, Secure Gateway), ответственный ЭБУ, по сути разграничивающий все домены внутри и вне автомобиля, реализует вышеописанный критичный функционал, поэтому для данное программное решение целесообразно реализовывать с применением концепций конструктивной безопасности (secure by design) и кибериммунитета.

Данные концепции основаны на архитектурных паттернах MILS (Multiple Independent Levels of Security) и FLASK (Flux Advanced Security Kernel) [6]. FLASK — это подход к построению операционных систем с повышенной безопасностью, обеспечивающий гибкое управление доступом на основе контекста и политик безопасности, что позволяет усилить защиту от угроз, связанных с межпроцессным взаимодействием.

Основные особенности такого подхода:

- Строгая изоляция доменов, что позволяет ограничить воздействие вредоносного кода в пределах одного домена и не распространять угрозу на другие части системы.
- Контроль межпроцессных взаимодействий на основе специализированных политик безопасности. Эти политики гарантируют, что компоненты системы могут взаимодействовать только в пределах заранее определенных правил, минимизируя риск компрометации системы [6].
- Минимизация доверенной кодовой базы с использованием микроядерной операционной системы, (например, KasperskyOS). Это позволяет значительно уменьшить поверхность атаки и обеспечить более строгий контроль доступа.

Заключение

Постоянное усложнение ландшафта угроз для автомобильной отрасли диктует необходимость создания сложных программно-аппаратных архитектур, обеспечивающих высокий динамизм в части программного кода и бизнес-логики. Шлюзы безопасности помогают решить эти задачи, становясь ключевым инструментом для качественного разграничения доступа и защиты различных доменов внутри и снаружи автомобиля. Применение модели ABAC и пятимерного пространства Хартсона обеспечивает гибкость и динамичность политик безопасности, соответствуя современным требованиям кибербезопасности в автомобильной индустрии.

Литература

1. Tverdyshev, S., Blasum, H., Rudina, E., Kulagin, D. et al. Security architecture and specification framework for safe and secure industrial automation //Critical Information Infrastructures Security: 10th International Conference, CRITIS 2015, Berlin, Germany, October 5-7, 2015, Revised Selected Papers 10. – Springer International Publishing, 2016. – С. 3-14.

2. 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.

3. Ling Z. et al. Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes //Journal of Systems Architecture. – 2021. – Т. 119. – С. 102240.

4. Карабань А.А. Кибериммунитет и KasperskyOS в ООН: поддержка UN R № 155 // Kaspersky Cyber Immunity Developers Night, июнь 2023. [Видео]. Доступно по ссылке: https://rutube.ru/video/b760b36d25ce1f5073a27ddacdf48655/

5. Костин А.А. Реалии и тренды безопасности автомобилей // Встреча DEFCON Russia, 17.11.2023. [Видео]. Доступно по ссылке: https://clck.ru/3EJrvR

6. *Соболев С. П. Кибериммунный подход к разработке. Иллюстрация применения на базе микросервисной архитектуры // Вестник СПбГУ. Серия 10. Прикладная математика. Информатика. Процессы управления. 2024. №1. URL: https://cyberleninka.ru/article/n/kiberimmunnyy-podhod-k-razrabotke-illyustratsiya-primeneniya-na-baze-mikroservisnoy-arhitektury (дата обращения: 31.10.2024).*

7. *Карабань А.А., Фадин А.А. Облачные сервисы автомобилей: где прячутся киберугрозы? // KasperskyOS Blog, 25.10.2024. Доступно по ссылке: https://os.kaspersky.ru/blog/automotive-digest-october-2024/*

Enabling trusted environments and access control in the vehicle ecosystem: approaches and solutions based on a cyberimmune automotive security

Fadin A.A.[166]

Abstract. In this study, the approaches to access control between the electronic control units (ECUs) of connected vehicles and the external ecosystem are explored. The focus is on the implementation of a cyber-immune automotive security gateway to create a trusted environment. Examples of access control implementation based on PDP, PIP, and PAP components are presented, utilizing the Attribute-Based Access Control (ABAC) model and the five-dimensional Harsanyi space. The results demonstrate how dynamic security policy changes can enhance the protection of vehicle management systems, ensuring compliance with UN R155 and ISO/SAE 21434.

Keywords access control, ABAC, automotive cybersecurity, security gateway, telematics, measured boot, MQTT, connected vehicle.

[166] Fadin Andrey Anatolyevich, Kaspersky Lab, Moscow, fadin.andrey@gmail.com

УДК 004.056

Статистическое обезличивание персональных данных

Чепик П.И.[167]

Аннотация: В условиях цифровизации и повсеместного сбора данных вопрос защиты личной информации становится особенно актуальным. Статистическое обезличивание — это метод обработки данных, направленный на предотвращение идентификации отдельных лиц. Этот процесс включает преобразование данных таким образом, чтобы сохранить их полезность для анализа, но при этом исключить возможность восстановления личной информации.

Ключевые слова: безопасность персональных данных, обезличивание персональных данные, статистическое обезличивание.

Актуальность

В условиях цифровизации и повсеместного сбора персональных данных их обезличивание является весьма востребованным [1-6]. Статистическое обезличивание персональных данных имеет несколько преимуществ по сравнению с другими методами обезличивания, такими как анонимизация и псевдонимизация. Статистическое обезличивание позволяет сохранять полезные характеристики данных для анализа. В отличие от полной анонимизации, где данные могут быть полностью удалены или изменены до такой степени, что их нельзя использовать для анализа, статистическое обезличивание обеспечивает возможность извлечения статистической информации и выявления тенденций, сохраняя при этом конфиденциальность [7].

Методы статистического обезличивания

Существует несколько распространенных методов статистического обезличивания:

1. Агрегация данных. Данные объединяются по группам, что позволяет скрыть индивидуальные записи. Например, вместо представления данных о доходах отдельных людей можно указать средний доход по группе.
2. Замена значений. В этом методе значения в данных изменяются, например, путем добавления случайного шума или замены на случайные значения в пределах определенного диапазона.
3. Кластеризация. Данные группируются по схожим характеристикам. Это затрудняет идентификацию отдельных записей, так как информация представлена в виде групповых характеристик.
4. Шумовая фильтрация. В этот метод входит добавление случайного шума к данным, что помогает скрыть точные значения и уменьшить вероятность восстановления личной информации [8].

Плюсы статистического обезличивания

Одно из основных преимуществ этого метода заключается в том, что данные представляются третьим лицам в качестве отклика на конкретный запрос. Для аудита оператор сохраняет весь перечень запросов и обращений, что предоставляет ему гарантированную возможность утверждать, что третье лицо не получило доступ к защищаемым данным.

Исследователи могут анализировать тенденции и закономерности, что может привести к новым открытиям и улучшению качества жизни. Использование обезличенных данных снижает вероятность юридических последствий, связанных с утечкой личной информации [9, 10].

[167] Чепик Полина Игоревна, МГТУ им. Н.Э. Баумана, Москва, pchepik@yandex.ru

Минусы статистического обезличивания

Несмотря на то, что известны статистически обезличивающие механизмы для многих функций статистической аналитики данных, вопрос построения интерактивного механизма, способного одновременно отвечать на любые запросы с высокой точностью (с меньшим зашумлением) и при этом сохранять конфиденциальность данных, остается открытым. Надо учитывать, что в совокупности результаты запросов могут позволить определить дополнительную информацию. В случае если история запросов не сохраняется, нарушитель может намеренно создавать запросы, до тех пор, пока не выявит конкретный признак, описывающий одного или нескольких конкретных субъектов [11, 12].

Актуальность статистического обезличивания данных в России

С учетом глобальных тенденций в области защиты персональных данных, актуальность статистического обезличивания данных в России становится особенно высокой. В 2017 году в стране вступил в силу Федеральный закон № 152-ФЗ «О персональных данных», который устанавливает строгие требования к обработке и защите личной информации граждан. Закон требует от организаций, собирающих и обрабатывающих персональные данные, обеспечения их безопасности и соблюдения прав субъектов данных [4].

Статистическое обезличивание данных позволяет организациям соответствовать требованиям законодательства о защите персональных данных. Обезличенные данные могут использоваться для анализа и исследований без риска нарушения прав субъектов данных. В условиях активного развития цифровой экономики в России, статистическое обезличивание становится важным инструментом для анализа больших объемов данных. Это позволяет компаниям извлекать ценную информацию для принятия бизнес-решений, не нарушая при этом законов о защите данных. В свете растущих случаев утечек и кибератак, применение методов статистического обезличивания может снизить риски, связанные с потенциальной идентификацией пользователей. Это особенно актуально для государственных органов и организаций, работающих с чувствительной информацией.

Заключение

Статистическое обезличивание персональных данных представляет собой важный инструмент для защиты конфиденциальности в условиях растущего внимания к вопросам личной информации. Оно предлагает множество преимуществ, включая защиту данных и возможность их использования для анализа. Однако необходимо учитывать и недостатки, такие как потеря точности и риск рекомпиляции данных. Важно находить баланс между защитой конфиденциальности и качеством данных, что требует тщательного подхода и применения современных технологий [13]. В конечном итоге, успешное применение статистического обезличивания может стать ключом к эффективному использованию данных при соблюдении прав и свобод личности.

Литература

1. 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. 2016. С. 103-104.

2. Защита персональных данных в информационных системах методом обезличивания / Шередин Р.В. - Диссертация на соискание ученой степени кандидата технических наук. 05.13.19 / Научный руководитель: Саксонов Е.А. - Московский государственный институт электроники и математики. Москва, 2011. – 138 с.

3. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах / Волокитина Е.С. - Диссертация на соискание ученой степени кандидата технических наук.

05.13.19 / Научный руководитель Добрица В.П. / Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. 2013. - 183 с.

4. 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.

5. Обезличивание персональных данных и технологии "больших данных" (bigdata) / Мавринская Т.В., Лошкарёв А.В., Чуракова Е.Н. // Интерактивная наука. 2017. № 6 (16). С. 78-80.

6. Чепик П.И. Обезличивание персональных данных как способ повышения их защиты при обработке в информационных системах. В сборнике: «Безопасные информационные технологии». Сборник трудов Двенадцатой международной научно-технической конференции. Москва, 2023. С. 150-153.

7. Karr, A. F., Whittaker, J. O., & Sanil, A. P. (2006). "Statistical disclosure limitation and the role of the data custodian." Journal of Official Statistics, 22(1), 1-18.

8. "A survey of statistical disclosure control methods" by Domingo-Ferrer, J., & Torra, V. (2005). Journal of Privacy and Confidentiality, 1(1), 1-12

9. N. R. Adam and J. C. Wortmann. Security-control methods for statistical databases: A comparative study. ACM Comput. Surv., 21(4):515-556, 1989.

10. 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.

11. 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.

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. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. -М.: НИИ РиЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.

Научный консультант: Шахалов Игорь Юрьевич, доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана, i.shahalov@npo-echelon.ru

Statistical de-personalization of personal data

Chepik P.I.[168]

Abstract: In the context of digitalization and widespread data collection, the issue of protecting personal information is becoming especially relevant. Statistical anonymization is a data processing method aimed at preventing the identification of individuals. This process involves transforming data in such a way as to preserve its usefulness for analysis, but at the same time exclude the possibility of restoring personal information.

Keywords: personal data security, personal data anonymization, statistical anonymization.

[168] Polina Chepik, BMSTU, Moscow, p.chepik@yandex.ru

СОДЕРЖАНИЕ

ISBN 978-5-6045553-9-2

Издательство:
ООО «Мастерская Печати Идей»
Россия, Москва, 129226, ул. Сельскохозяйственная, д. 12а, стр.7.
Тел. (499) 404-64-74
Подписано в печать 29.11.2024 Заказ 225
Формат 60x90.8. Гарнитура Times New Roman
Усл. печ. 20.12.2024 Тираж 100 экз.