DOI 10.36622/1682-7813.2025.28.1.008
УДК 349:004.056

РАЗВИТИЕ И АВТОМАТИЗАЦИЯ МЕТОДИК ОРГАНИЗАЦИОННО-ПРАВОВОЙ ЗАЩИТЫ СЕТЕЙ В КОНТЕКСТЕ РИСК-АНАЛИЗА КИБЕРАТАК

Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, Е.А. Москалева, В.И. Белоножкин, Б.Г. Смирнов

В данной статье изложено исследование аналогов технологий автоматизации организационно-правовой защиты корпоративных сетей от кибератак. В рамках исследования проведен анализ существующих подходов к созданию таких документов, выявлены их слабые стороны и предложены методы их оптимизации. На основании информации из открытых источников, таких как базы данных Positive technologies, MITRE Att&ck, SecurityCode и Securitm, а также с учетом современных методов кибератак, разработаны документы мер противодействия, включающие актуальные подходы защиты информации. В статье представлена схема комплексного применения этих методов, учитывая все сильные и слабые стороны аналогов, для повышения эффективности защиты и оперативного реагирования на инциденты информационной безопасности.

Ключевые слова: техники, регламенты, меры обнаружения, меры смягчения, матрица техник, организационно-правовая защита.

Введение

Информационные технологии стали неотъемлемой частью повседневной жизни, что привело к постоянному росту значения цифровых данных. Поэтому и охота за цифровыми данными тоже постоянно развивается, приобретая всё большие масштабы и всё более изощрённые способы. Растущая угроза кибератак и увеличение числа инцидентов, связанных с безопасностью, требуют постоянного развития и совершенствования подхода к обеспечению информационной безопасности.

С каждым днем хакеры и злоумышленники разрабатывают все более сложные и совершенные методы атаки на информационные системы. [1]. Особенно актуальной проблемой является необходимость оперативного реагирования на угрозы и создания надежной системы защиты, обеспечивающей устойчивость корпоративных систем перед целенаправленными атаками. Проблемы разработки локальных политик, регламентов и инструкций в области информационной безопасности связаны с недостаточной адаптацией к динамическим изменениям в ландшафте угроз, что повышает риски нарушения конфиденциальности, целостности и доступности информации.

Для решения этой проблемы необходима модернизация методик формирования указанных документов с акцентом на автоматизацию процессов и использование результатов риск-анализа актуальных кибератак.

В настоящее время существуют подходы и решения по формированию организационно-правовых документов и их оптимизации на основе передовых практик и открытых данных, такие как базы Positive technologies, MITRE Att&ck, SecurityCode и Securitm. Однако, данное направление повышения эффективности организационно-правовой защиты (ОПЗ) компьютерных систем и сетей за счет автоматизации формирования пакета документов остается актуальным и требует дальнейшего развития.

Оценка эффективности существующих аналогов

Positive Technologies Матрица MITRE ATT&CK описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру. В PT указывают как правило процент покрытия техник. Процент покрытия вычислен на основе информации из пяти продуктов Positive Technologies: MaxPatrol EDR, MaxPatrol SIEM, PT Application Firewall, PT Network

Attack Discovery и PT Sandbox. Securitm выделяется полным покрытием техник MITRE Enterprise [2], но имеет ограничения в части русификации, автоматизации и проектирования сценариев атак. SecurityCode сервис, описывающий тактики и техники, которые используются при атаках на ИТ-инфраструктуру компаний. Полученная информация позволяет предугадать дальнейшие действия киберпреступников и построить комплексную систему безопасности для предотвращения критичных событий.

В целях оценки текущего уровня технологической поддержки было проведено сравнение по нескольким показателям продуктов компаний Positive Technologies, Securitm и SecurityCode, решающих задачи автоматизации применения матрицы MITRE Enterprise [5], результат которого отражен в табл. 1.

Таблица 1

Оценка эффективности инструментов для работы с матрицей Mitre Att&ck

Показатели оценивания	Positive Technologies	Securitm	Securitycode
Полнота сведений о техниках матрицы Mitre	Частичное покрытие техник	Полное покрытие техник	Полное покрытие техник
Полнота сведений о мерах противодействия	Частичное покрытие мер противодействия	Частичная покрытие мер противодействия	Отсутствие мер противодействия
Русификация	Частичная русификация мер	Отсутствует	Полная русификация техник
Автоматизация работы с мерами противодействия	Есть инструмент автоматизированного вывода мер	Отсутствует	Отсутствует
Возможность проектирование сценариев атак	Отсутствует	Отсутствует	Есть инструмент проектирования по готовым шаблонам сценариев атак
Общие недостатки	1)Отсутствие сведений по техникам Mobile Matrix и ICS Matrix Mitre Att&ck. 2) Отсутствие 100% русификации мер противодействия по техникам. 3) Невозможность проектирования сценариев атак по вводимым техникам и их сортировки по этапам Mitre.		

Проектирование схемы выработки мер противодействия комплексным кибератакам

Комплексная кибератака представляет собой многоэтапный процесс, направленный на компрометацию цели с использованием различных методов и техник.

Проанализировав представленные данные, становится очевидным, что текущие решения не полностью удовлетворяют требованиям по обеспечению комплексной защиты от многоэтапных атак. Проблема заключается в том, что рассматриваемые продукты фокусируются преимущественно на векторах атак, игнорируя взаимосвязь между отдельными техниками, используемыми злоумышленниками на разных этапах атаки.

Такие атаки могут быть адаптивными и используют широкий спектр инструментов и техник, которые реализуются в ходе каждого этапа. Схема выработки мер ОПЗ от комплексной атаки, использующая результаты риск-анализа показана на рис. 1.

Рис. 1. Схема выработки мер противодействия кибератакам

Для выработки варианта мер ОПЗ можно установить связь между техниками и мерами методики MITRE ATT&CK, которая позволяет организациям получать полное представление о состоянии кибербезопасности, выявлять и тестировать бреши в защите [6].

Матрица Enterprise ATT&CK предоставляет модель, в которой подробно описываются конкретные тактики и методы для широкого спектра платформ.

Таблица Detections матрицы включают в себя источники и компоненты данных, необходимые для определения техники атаки.

Таблица Mitigations описывает меры смягчения последствий атаки после её обнаружения.

На рис. 3 показана общая схема вывода регламентов ОПЗ для каждой техники сценария атаки, описанной в указанных таблицах.

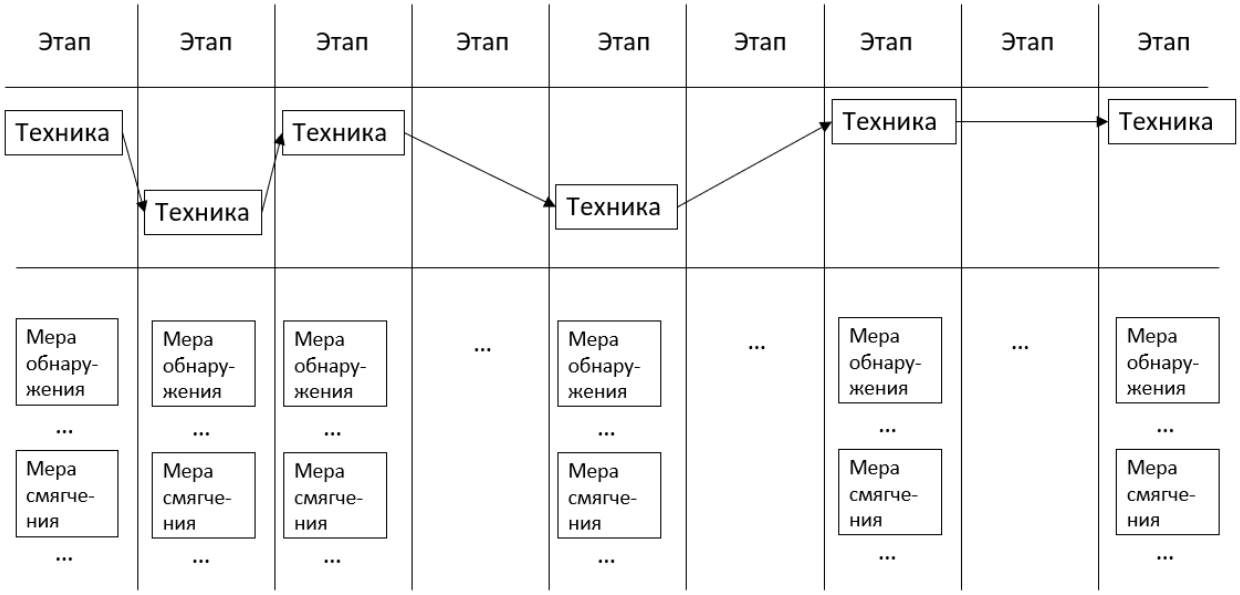

Рис. 2. Схема вывода мер Mitre Att&ck по техникам сценария атаки

Алгоритмизация выработки мер противодействия

Меры обнаружения атак позволяют выявить угрозу на ранней стадии и включают мониторинг сети, анализ логов, использование систем обнаружения вторжений и других аналогичных технологий. Меры смягчения последствий помогают минимизировать ущерб и восстановить работоспособность системы. Комбинация этих двух категорий мер позволяет повысить эффективность регламентов ОПЗ.

Внедрение схемы частных регламентов значительно повышает эффективность процессов управления инцидентами и обеспечивает соответствие требованиям современной информационной безопасности.

Схема, демонстрирующая принцип работы модернизированной технологии генерации регламентов противодействия кибератакам, показана в рис. 3. Реализация технологии начинается с сбора данных о техниках, применяемых для атаки. Затем собранные данные проходят через обработку формата из json в blob [4]. Далее сортированные по этапам данные о техниках записываются в файл и выводятся пользователем.

Разработка средства автоматизированного формирования регламентов

Для создания программного обеспечения, выбран проект на Python, благодаря своей простоте, универсальности и широкому сообществу разработчиков. Кроме того, Python хорошо подходит для быстрой разработки прототипов и тестирования новых решений, что важно при создании сложных систем защиты информации.

Для хранения информации о техниках MITRE ATT&CK используется БД «Техника Mitre – Меры», которая имеет структуру данных, соответствующую стандартам описания тактик и техник атак в рамках фреймворка MITRE ATT&CK. Каждая техника связана с конкретными мерами обнаружения и смягчения.

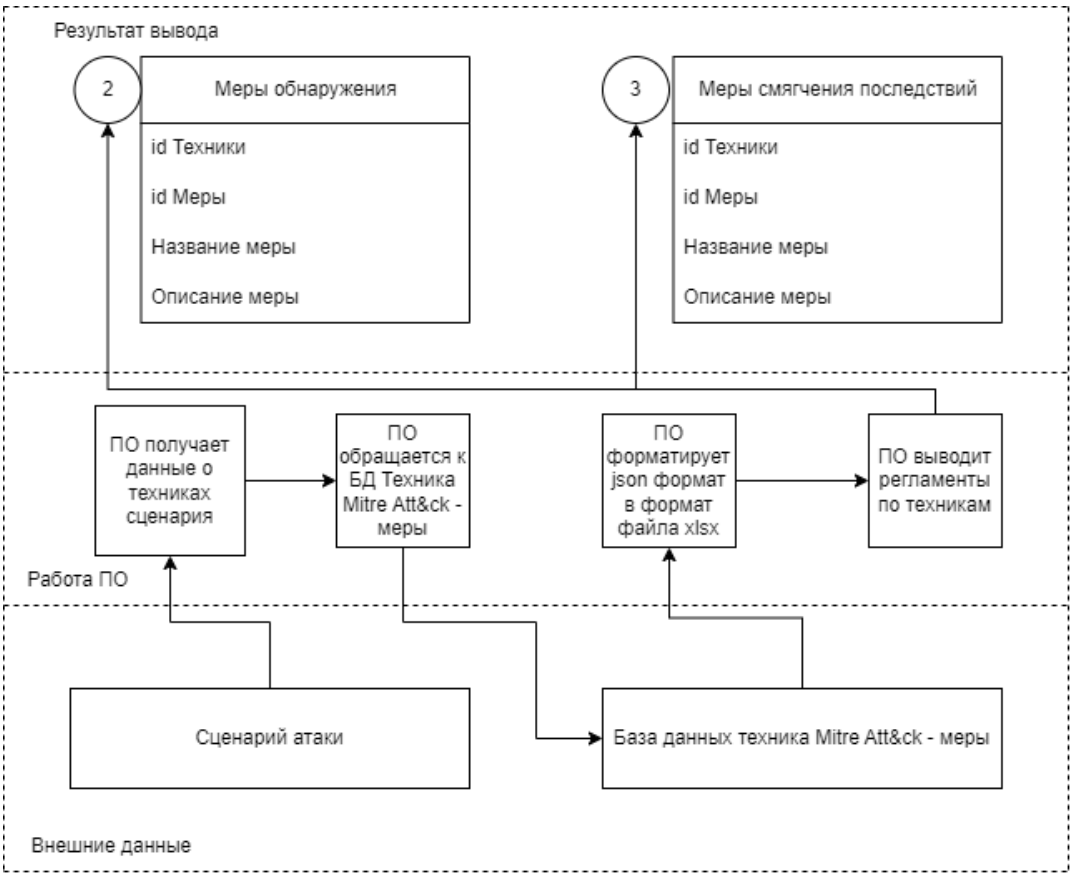

Рис.3. Схема работы модернизированной технологии выработки мер ОПЗ

Общая структура проекта включает в себя (рис.4):

– файл mitigations_and_detections.json - БД с информацией о мерах обнаружения исмягчения последствий;

– файл techniques_db.json хранит информацию о техниках и этапах атак;

– библиотека openpyxl для работы с таблицами в формате Excel [3];

– основной скрипт main.py, который управляет выполнением других скриптов;

– скрипт generateTable.py, отвечающий за создание таблицы «сценарии атаки» и добавление её в Excel-файл.

– скрипт generateDetectionsTable.py для создания таблицы «меры обнаружения» и добавление её в Excel-файл;

– скрипт generateMitigationsTable.py для создания таблицы «меры смягчения последствий» и добавление её в Excel-файл.

В результате выполнения скриптов создается файл xlsx, содержащий таблицы с информацией о мерах смягчения последствий, мерах обнаружения и сценариях атак. Ввод сценария осуществляется через массив номеров техник.

Данные проходят предварительную обработку, включающую фильтрацию, нормализацию и агрегацию. Это позволяет исключить дубликаты, привести все записи к единому формату и подготовить их для дальнейшего анализа. Запуск программы осуществляется через скрипт `main.py` (рис. 4).

Результаты сохраняются в результирующем файле, который может быть представлен в формате HTML, PDF или Excel.

Рис.4. Структура проекта

Этот файл можно использовать для дальнейшего анализа и принятия решений по

улучшению защиты информационной системы.

В результирующий файл выводится первый лист техник по этапам Mitre Att&ck (табл. 2).

Таблица 2

Результат вывода данных о сценарии атаки

Этап	Техника
Первоначальный доступ	T1566.001: Целевой фишинг с вложением
Выполнение	T1203: Эксплуатация уязвимостей в клиентском ПО
Выполнение	T1204.002: Вредоносный файл
Организация управления	T1568.003: Расчет на основе DNS
Организация управления	T1102.002: Двусторонняя связь

В результирующий файл выводится второй лист мер по обнаружению Mitre Att&ck (табл. 3).

Таблица 3

Пример результата вывода данных о мерах обнаружения

ID техники	ID меры	Название меры обнаружения	Описание
T1203	DS0009	Процесс	Мониторьте процессы, запущенные на системе, обращая внимание на использование ими пространства памяти, а также на загружаемые модули (DLL или общие библиотеки)..
T1203	DS0009	Процесс	Анализируйте выделенные области памяти процессов, содержащие данные, такие как пользовательский ввод и структуры данных, специфичные для каждого приложения
T1203	DS0015	Журнал приложений	Интегрируйте сбор событий, генерируемых сторонними сервисами, такими как почтовые серверы, веб-приложения или другие устройства, для анализа и мониторинга активности, не связанной с вашей основной операционной системой или платформой.
T1203	DS0022	Файл	Создайте объект компьютерного ресурса, такой как файл, который будет управляться системой ввода-вывода для хранения различных типов данных, например, изображений, текстов, видео, программ или других медиафайлов.
T1566.001	DS0009	Процесс	Мониторьте процессы, запущенные на системе, обращая внимание на использование ими пространства памяти, а также на загружаемые модули (DLL или общие библиотеки). Анализируйте выделенные области памяти процессов, содержащие данные, такие как пользовательский ввод и структуры данных, специфичные для каждого приложения.

Продолжение табл. 3

ID техники	ID меры	Название меры обнаружения	Описание
T1566.001	DS0015	Журнал приложений	Интегрируйте сбор событий, генерируемых сторонними сервисами, такими как почтовые серверы, веб-приложения или другие устройства, для анализа и мониторинга активности, не связанной с вашей основной операционной системой или платформой.

В структуре результирующего файла также будет третий лист. В результирующий файл выводится третий лист мер по смягчению Mitre Att&ck (табл. 4).

Таблица 4

Пример результата вывода данных о мерах смягчения

ID техники	ID меры	Название меры смягчения	Описание
T1203	M1048	Изоляция приложений и "Песочница"	Ограничьте выполнение кода виртуальной средой на конечной системе или при передаче данных в конечную систему.
T1203	M1050	Защита от эксплойтов	Используйте возможности для обнаружения и блокировки условий, которые могут привести к эксплуатации программного обеспечения или указывать на неё.
T1203	M1051	Обновление программного обеспечения	Выполняйте регулярные обновления программного обеспечения, чтобы снизить риск эксплуатации.
T1566.001	M1049	Антивирус / Защита От Вредоносных программ	Используйте сигнатуры или эвристику для обнаружения вредоносного программного обеспечения.
T1566.001	M1047	Аудит	Выполняйте аудит или сканирование систем, разрешений, небезопасного программного обеспечения, небезопасных конфигураций и т. д. для выявления потенциальных уязвимостей.

В результате данного подхода проанализированы различные техники, используемые злоумышленниками для проникновения в систему, и определены наиболее вероятные сценарии развития событий. На основе полученных данных был создан сценарий атаки, который позволил смоделировать реальные условия и проверить работоспособность предлагаемых мер защиты.

Одним из ключевых аспектов проекта стало выявление мер обнаружения и смягчения по техникам атаки. Для этого использовались современные технологии и подходы, такие как анализ логов, мониторинг сети, поведенческий анализ и многие другие [7]. Особое внимание было уделено разработке алгоритмов, позволяющих автоматически обнаруживать аномалии в работе системы и оперативно реагировать на них [8].

Кроме того, были разработаны и протестированы различные методы смягчения последствий атак. Это включало в себя как технические решения, такие как фильтрация трафика и ограничение доступа, так и организационные меры, направленные на повышение осведомленности сотрудников и обучение их навыкам безопасной работы.

Проектирование сценария атаки позволило оценить эффективность предложенных мер защиты и выявить слабые места в

системе. Это дало возможность внести необходимые коррективы и улучшить защиту системы от потенциальных угроз.

Заключение

В работе предложены и обоснованы новые подходы к созданию организационно-правовых документов, направленных на защиту корпоративных сетей от современных кибератак. Разработанная методика позволяет формализовать документы, адаптировать их содержание к результатам риск-анализа и учитывать динамические изменения в технологиях реализации атак. В отличие от существующих аналогов, предложенный алгоритм автоматизации позволяет оперативно реагировать на новые вызовы и эффективно адаптировать политики, регламенты и инструкции к актуальным кибератакам. Кроме того, создано программное решение, обеспечивающее автоматизацию процесса разработки, обновления и согласования регламентирующих документов, существенно сокращает временные затраты и повышает их актуальность.

Список литературы

1. Организационно-правовая защита от сетевых атак: методики формирования частных политик, регламентов и инструкций обеспечения безопасности организации (часть I) Остапенко Г.А., Щербакова Д.В., Мирошниченко Т.Ю., Остапенко А.А., Кривошеин А.С. Информация и безопасность. 2023. Т. 26. № 3. С. 329-340.

2. ATT&CK Matrix for Enterprise. URL: https://attack.mitre.org/techniques/enterprise/ (дата обращения 25.01.25).

3. Python is a programming language that lets you work quickly and integrate systems more effectively.. URL: https://www.python.org/(дата обращения 25.01.25).

4. JSON Schema. Быть или не быть? URL: https://habr.com/ru/articles/495766/ (дата обращения 25.01.25).

5. Сервис моделирования кибератак по матрице MITRE ATT&CK. URL: https://mitre.securitycode.ru/ (дата обращения 25.01.25).

6. MITRE ATT&CK® Navigator. URL: https://mitre-attack.github.io/attack-navigator/ (дата обращения 25.01.25).

7. Kaspersky Symphony. URL: https://www.kaspersky.ru/enterprise-security/symphony?reseller=kl-ru_symphony-xdr-sm_acq_ona_sem_gen_onl_b2b_ya_ppc-ad_____&utm_source=yandex&utm_medium=cpc&utm_campaign=Y%20-%20RU%20-%20RU%20-%20B2B%20ENT%20-%20PS%20-%20Branded%20-%20RU%20-%20BG%20-%20Kaspersky%20Symphony&utm_content=11502241218&utm_term=mitre%20attack&yclid=16897238606484865023 (дата обращения 25.01.25).

8. Как MITRE ATT&CK помогает предотвращать киберугрозы. URL: https://www.sberbank.ru/ru/person/kibrary/articles/kak-mitre-att-ck-pomogaet-predotvrashchat-kiberugrozy (дата обращения 25.01.25).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 28.01.25

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

Васильченко Алексей Павлович – аспирант, Финансовый университет при Правительстве Российской Федерации, e-mail: rainichek@yandex.ru

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com
Белоножкин Владимир Иванович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com
Смирнов Богдан Геннадьевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

DEVELOPMENT AND AUTOMATION OF ORGANIZATIONAL AND LEGAL PROTECTION TECHNIQUES FOR NETWORKS IN THE CONTEXT OF CYBERATTACK RISK ANALYSIS

G.A. Ostapenko, A.P. Vasilchenko, A.A. Ostapenko, E.A. Moskaleva, V.I. Belonozhkin, B.G. Smirnov

This article presents a study of analogs of automation technologies for the organizational and legal protection of corporate networks from cyber-attacks. The study analyzes existing approaches to creating such documents, identifies their weaknesses, and suggests methods for optimizing them. Based on information from open sources such as Positive technologies, MITRE Att&ck, SecurityCode and Securitm databases, as well as taking into account modern methods of cyber-attacks, documents of counteraction measures have been developed, including relevant approaches to information protection. The article presents a scheme for the integrated application of these methods, taking into account all the strengths and weaknesses of their analogues, to increase the effectiveness of protection and rapid response to information security incidents.

Keywords: techniques, regulations, detection measures, mitigation measures, matrix of techniques, organizational and legal protection.

Submited 28.01.25

Information about authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru
Alexey P. Vasilchenko – Graduate Student, Financial University under the Government of the Russian Federation, e-mail: rainichek@yandex.ru
Alexander A. Ostapenko – Graduate Student, Voronezh State Technical University, e-mail: alexostap123@gmail.com
Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Vladimir I. Belonozhkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
Bogdan G. Smirnov – Student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com