https://www.consultant.ru/document/cons_doc_LAW_527541/ (дата обращения 11.03.2026).

4. Правительство РФ утвердило перечень типовых объектов КИИ [Электронный ресурс] // РБК Компании. – 27 февраля 2026. – URL: https://companies.rbc.ru/news/3W11TNmuF9/pravitelstvo-rf-utverdilo-perechen-tipovyih-obektov-kii/ (дата обращения 11.03.2026).

5. Исмагилова, А. С. Теоретико-графовая интерпретация системы защиты информации / А. С. Исмагилова, И. А. Шагапов, И. В. Салов // Инженерный вестник Дона. – 2024. – № 9(117). – С. 171-179. – EDN LWCKXX.

Моисеева Карина Артемовна, студ. 4 курса ИИГУ, moiseeva_012@mail.ru
Яппаров Рауф Мидхатович, к.ю.н., доцент, доцент каф. управления информационной безопасностью, bist2002@yandex.ru

УДК 004.056.53

# РАЗРАБОТКА МЕТОДИКИ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ ПРАВИЛ ДЛЯ МЕЖСЕТЕВОГО ЭКРАНА

Н. Ф. Махмутова, И. А. Ушаков, М. М. Ковцур, С. Алькаттан
Санкт-Петербургский государственный университет телекоммуникаций им проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

**Ключевые слова**: межсетевой экран, корпоративная сеть, автоматизация проверки правил, информационная безопасность

Обеспечение информационной безопасности в корпоративных сетях является одной из приоритетных задач для организаций любого масштаба. Ключевую роль в выполнении этих функций играют межсетевые экраны (МСЭ), которые фильтруют входящие и исходящие соединения на основе заданных правил. С ростом компании поддержание актуальности правил МСЭ становится трудоемкой задачей, а поскольку большинство обращений пользователей вызвано именно отсутствием разрешающих правил, автоматизация их проверки необходима для оперативного восстановления доступа к сервисам и обеспечения непрерывности бизнеса [1].

Логика функционирования схемы корпоративной сети строится вокруг фильтрации трафика на МСЭ: все запросы от пользователей к внешним или внутренним ресурсам проходят через него, и доступ предоставляется только при наличии соответствующего разрешающего правила. Для решения проблемы оперативного реагирования на пользовательские запросы о недоступности сервисов разработана методика автоматизированного обнаружения отсутствующих правил на межсетевых экранах. Ниже описаны ключевые этапы предлагаемой методики [2].

1. Получение и первичная обработка входных параметров от пользователя. Исходными данными для работы методики служат обращения пользователей, поступающие в службу технической поддержки.

Запросы неформальны — пользователи описывают проблему на естественном языке, смешивая текстовые описания, IP-адреса, доменные имена и названия сервисов.

2. Преобразование запроса в машиночитаемые параметры с использованием LLM-модели. Ключевым элементом методики выступает применение больших языковых моделей (LLM) для анализа пользовательского запроса и извлечения структурированной информации [3]. На выходе модель генерирует структурированный JSON-объект, содержащий три ключевых параметра для последующей диагностики, представлено на рисунке 1.

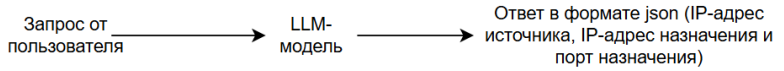


Рисунок 1— Схема обработки запроса

3. Определение целевого межсетевого экрана по IP-адресу источника. Для этого используется предварительно подготовленная таблица 1 соответствия, содержащая информацию о привязке подсетей к конкретным МСЭ.

Таблица 1 — Соответствие сетевой топологии

| **Подсеть (Net)** | **МСЭ** | **IP-адрес управления МСЭ** |
|---|---|---|
| 10.1.1.0/24<br>10.1.10.0/23 | мсэ1 | 10.1.1.7 |
| 10.2.2.0/24<br>10.2.20.0/23 | мсэ2 | 10.2.2.7 |

Алгоритм определения: из JSON-объекта извлекается IP-адрес источника, выполняется поиск подсети, определяется соответствующий МСЭ и его IP-адрес для подключения.

4. Автоматизированная проверка наличия правила на МСЭ. Автоматическое подключение к МСЭ с использованием SSH-протокола. Далее запрос текущего списка правил. Затем анализ правил с помощью LLM — полученный объемный список правил передается языковой модели с задачей найти правило.

Формирование результата проверки. Если правило найдено: система фиксирует его наличие, значит проблема не в списках доступа на МСЭ. Если правило не найдено: система генерирует отчет об отсутствии правила с указанием конкретных параметров и рекомендацией по его созданию. Результат работы методики: специалист технической поддержки получает готовый ответ о наличии или отсутствии необходимого правила на целевом

МСЭ, время проверки значительно сокращается.

Разработана методика автоматизированного обнаружения отсутствующих правил на межсетевых экранах. Она преобразует пользовательские запросы в структурированные параметры через LLM, определяет нужный МСЭ по подсети источника и проверяет наличие правила. Время диагностики сокращается с минут до секунд, что позволяет быстро выявлять причину проблем и восстанавливать доступ к сервисам.

Список использованных источников

1.Кривец, А. С. Анализ систем искуственного интелекта применяемых для работы систем обнаружения вторжений / А. С. Кривец, С. И. Штеренберг // Технологии информационного общества : Сборник трудов XVIII Международной отраслевой научно-технической конференции, Москва, 27–28 февраля 2024 года. – Москва: Московский технический университет связи и информатики, 2024. – С. 99-101. – EDN MQZRNG.

2.Разработка концепции определения нелегитимного трафика dns. Платонов А.Е., Ковцур М.М., Ушаков И.А. В книге: Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. Санкт-Петербург, 2024. С. 412-413.

3.Организация защищенного взаимодействия распределенных сетевых устройств. Ковцур М.М., Браницкий А.А., Казаков Н.И. В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 51-й Международной конференции. Москва, 2023. С. 37-39.

Махмутова Нурия Фаритовна, магистрант, iromup9898@gmail.com
Алькаттан Самех, магистрант, sameh.kt94@gmail.com.
Ковцур Максим Мхайлович, к.т.н., доцент каф. ЗСС, kovcur.mm@sut.ru
Ушаков Игорь Александрович, и.о. зав. каф. ИБКС, к.т.н., доцент, доцент каф. ИКС

УДК 004.056.53

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ ОТ АТАК ЛОКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМНЫХ СЛУЖБ ASTRA LINUX SE И КЛАССИЧЕСКИХ GNU/LINUX-ДИСТРИБУТИВОВ

Д. Е. Гилева, А. М. Гельфанд, М. М. Ковцур
СПбГУТ им проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

**Ключевые слова:** информационная безопасность, Astra Linux Special Edition, GNU/Linux, мандатный контроль целостности.

Защита системных служб от атак локальных пользователей —важная задача обеспечения безопасности операционный систем (ОС). Безопасность системных служб в классических дистрибутивах основана на комбинации механизмов, ядром которой является дискреционное управление доступом (права UNIX). Управление правами для множества служб децентрализовано,