УДК 004.056

# РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ДЛЯ ПОИСКА ОШИБОЧНЫХ ПРАВИЛ И АНАЛИЗА СТРУКТУРЫ ПОЛИТИКИ МЕЖСЕТЕВЫХ ЭКРАНОВ

**Фильченко А. П.**
**Научный руководитель – инженер Савков С. В.**
Университет ИТМО
368971@niuitmo.ru

## Введение

Межсетевые экраны являются одним из важных инструментов обеспечения сетевой безопасности. Они позволяют контролировать и фильтровать проходящий через них трафик, сегментировать локальную сеть на зоны с различными правами доступа и реализовывать политики доступа между этими зонами. Поскольку современные межсетевые экраны выполняют инспекцию трафика не только на периметре сети, но и внутри распределенных и виртуализованных сред, корректность их конфигурации становится критически важной для поддержания целостности, доступности и работоспособности всей инфраструктуры. Ошибки в настройках могут приводить как к непреднамеренному открытию критичных сервисов, так и к отказам в обслуживании легитимных приложений, что делает задачу верификации политик при эксплуатации особенно актуальной.

Политики межсетевых экранов могут содержать в себе большое количество правил, которые создаются или изменяются несколькими администраторами в разное время. В связи с этим могут возникать типичные ошибки: дублирование, частичные или полные перекрытия, неподходящая гранулярность. Эти ошибки повышают риски снижения защищенности сети, нарушения доступности сервисов, а также увеличивают операционные затраты на сопровождение и аудит политик. Многие межсетевые экраны не имеют встроенных средств для верификации политик, что усложняет своевременное обнаружение и исправление ошибок.

Цель работы – повысить защищенность компьютерных сетей и управляемость политик межсетевых экранов за счет создания программного модуля выявления типичных ошибок при разработке и конфигурировании политик межсетевых экранов.

## Основная часть

В качестве решения предлагается программный модуль для автоматизированной верификации политик межсетевых экранов, рассчитанный на интеграцию в эксплуатационные процессы. Модуль выполняет три основные задачи: нормализация и валидация входящих данных, поиск ошибок в правилах и ошибок в структуре политики, генерация отчета с выявленными нарушениями.

На вход модуль принимает политику межсетевого экрана в текстовом формате. После загрузки производится синтаксическая и семантическая проверка полей, приведение к единым структурам данных и предварительная агрегация сетей и портов для сокращения объема сравниваемых элементов. На этапе поиска ошибок производятся проверки загруженной политики на наличие ошибок в правилах, дублирования, частичного или полного перекрытия одного правила другим. Механизмы проверок основаны на операциях включения и пересечения множеств параметров правил. По результатам анализа формируется детализированный отчет, содержащий перечисление найденных ошибок со ссылками на идентификаторы правил.

Для реализации модуля был выбран язык Python как быстрый в разработке и хорошо интегрируемый со скриптовыми процессами инструмент. Модуль запускается на компьютере пользователя из командной строки. Данный подход облегчает

интеграцию и дальнейшее использование, а также минимизирует требования к среде развертывания.

Было проведено тестирование работы программного модуля. Для проверки использовались как синтетические политики, так и политики с устройств, работающих в реальных корпоративных сетях. После завершения работы модуля был выполнен ручной анализ данных для проверки и полученного отчета. Расхождений между ручным анализом и сгенерированным отчетом выявлено не было, что подтверждает корректность работы программного модуля.

## Выводы

В результате тестирования программный модуль продемонстрировал свою эффективность при анализе и верификации политик межсетевых экранов. Разработанное решение позволяет выявлять дублирование, перекрытия и иные структурные ошибки правил. Применение модуля позволяет сократить время на аудит конфигураций, снизить вероятность человеческих ошибок при ручном анализе и повысить управляемость политик при масштабировании инфраструктуры. В одинаковых условиях проверки результаты автоматического анализа совпали с результатами ручной верификации, что подтверждает корректность реализованных алгоритмов. Заявленная цель работы достигнута: обеспечено повышение защищенности и управляемости политик межсетевых экранов за счет их автоматизированной проверки.

## Список источников

1. Хеирхабаров Т. С., Шаляпин А. А. Обнаружение аномалий в наборах правил фильтрации межсетевых экранов // Решетневские чтения. 2014. №18. URL: https://cyberleninka.ru/article/n/obnaruzhenie-anomaliy-v-naborah-pravil-filtratsii-mezhsetevyh-ekranov (дата обращения: 15.02.2026).
2. How to Clean Up a Firewall Rulebase: Tufin Firewall Expert Tip #6 [Электронный ресурс]. – Режим доступа: https://www.tufin.com/blog/how-to-clean-up-a-firewall-rulebase-tufin-firewall-expert-tip-6 (дата обращения: 15.02.2026).
3. Security Policy Rulebase Best Practices [Электронный ресурс] // Palo Alto Networks Documentation. – Режим доступа: https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rulebase-best-practices(дата обращения: 15.02.2026).