

*Савенков Станислав Владимирович,
студент, 4 курс
кафедра информационной безопасности,
Сибирский государственный университет геосистем и технологий, РФ,
г. Новосибирск*

РАЗРАБОТКА УНИВЕРСАЛЬНОГО ПРОГРАММНОГО МОДУЛЯ РЕАГИРОВАНИЯ И ПРЕДОТВРАЩЕНИЯ СЕТЕВЫХ АТАК

***Аннотация:** Данная работа посвящена решению задачи повышения эффективности систем кибербезопасности при отражении сетевых атак на уровне протоколов. В условиях роста целенаправленных атак и ухода зарубежных вендоров рассматривается проблема разработки отечественного универсального программного модуля класса SOAR (Security Orchestration, Automation and Response). Предлагаемый модуль SOC 4 обеспечивает автоматический анализ трафика, корреляцию событий и мгновенное реагирование на угрозы (DDoS, DNS-туннелирование, сканирование портов) с использованием локальных средств (iptables) и облачных сервисов (SberCloud). Имитационное моделирование в среде AnyLogic подтвердило высокую скорость реакции и точность детектирования атак.*

***Ключевые слова:** кибербезопасность; сетевые атаки; SOC; имитационное моделирование; AnyLogic; автоматическое реагирование; корреляция событий; ГОСТ Р 34.10-2012.*

***Abstract:** This work is dedicated to solving the problem of improving the efficiency of cybersecurity systems in repelling network attacks at the protocol level. In the context of the growth of targeted attacks and the departure of foreign vendors, the problem of developing a domestic universal software module of the SOAR (Security Orchestration, Automation and Response) class is considered. The*

proposed SOC 4 module provides automatic traffic analysis, event correlation, and instant response to threats (DDoS, DNS tunneling, port scanning) using local tools (iptables) and cloud services (SberCloud). Simulation modeling in the AnyLogic environment confirmed the high reaction speed and accuracy of attack detection.

Keywords: *cybersecurity; network attacks; SOC; simulation modeling; AnyLogic; automated response; event correlation; GOST R 34.10-2012.*

Цифровой мир характеризуется непрерывным ростом киберугроз, направленных на компрометацию информационных систем. Традиционные подходы, основанные на периметровой защите и сигнатурном анализе, оказываются недостаточными для противодействия сложным и эволюционирующим видам атак. Согласно данным аналитиков, количество целенаправленных атак на российские организации в 2023–2024 годах увеличилось на 40%, причем значительная часть из них эксплуатирует уязвимости сетевых протоколов (TCP/IP, DNS, HTTP/3). Уход с российского рынка зарубежных вендоров сетевой безопасности обострил необходимость создания отечественных решений, соответствующих требованиям ФСТЭК России. Существующие аналоги часто обладают высокой стоимостью или недостаточной гибкостью. В связи с этим, разработка универсального программного модуля, способного в режиме реального времени обнаруживать аномалии и автоматически блокировать угрозы на уровне сетевых протоколов, является актуальной научно-практической задачей.

Разработанный программный модуль реагирования и предотвращения сетевых атак (SOC 4) представляет собой комплексное решение, соответствующее уровню зрелости экспертного центра управления безопасностью (SOC). Архитектура адаптирована к требованиям высокой степени автоматизации, поведенческому анализу и интеграции с внешними системами. Модульность является ключевым принципом проектирования. Система состоит из отдельных функциональных блоков:

- Модуль захвата и фильтрации трафика (реализация правил iptables/nftables);
- Модуль детектирования угроз и поведенческий анализатор (выявление аномалий через лог-анализ);
- Модуль автоматического ответа на инциденты (блокировка IP на уровне фаервола и облачных провайдеров);
- Модуль интеграции с Threat Intelligence и SIEM-системами.

Особое внимание уделено криптографической защите. Каждый логовый файл и команда блокировки подписываются с использованием алгоритма электронной цифровой подписи (ЭЦП) по ГОСТ Р 34.10-2012 на эллиптической кривой «К-256», что обеспечивает юридическую значимость и неизменность событий безопасности. Взаимодействие компонентов построено по асинхронной архитектуре с использованием очередей сообщений, что гарантирует отказоустойчивость системы даже при временной недоступности внешних API (например, SberCloud API или ГосСОПКА).

Для оценки эффективности разработанного модуля SOC 4 было проведено планирование имитационного эксперимента. Целью эксперимента являлась оценка производительности, точности обнаружения сетевых атак и времени реакции системы в условиях, приближенных к реальным. Этапы планирования включали:

Определение сценариев атак: DDoS (SYN-флуд), массовое сканирование портов, DNS-туннелирование, загрузка вредоносных файлов и координированные многоэтапные атаки.

Выбор среды моделирования: платформа AnyLogic, позволяющая сочетать агентное и дискретно-событийное моделирование.

Определение метрик эффективности: общее время обработки инцидента (от обнаружения до блокировки), процент успешно выявленных атак (качество обнаружения), количество ложных срабатываний.

Разработка концептуальной модели, включающей генератор атак (Source), фаервол, модуль SOC 4 и SIEM-сервер.

Экспериментальные исследования проводились в среде AnyLogic в пять этапов. Каждый этап имитировал 10 минут реальной работы системы под нагрузкой. Генератор атак создавал агентов типа AttackPacket с различными параметрами интенсивности (от 10 до 10000 пакетов в секунду). В ходе экспериментов были получены следующие количественные данные:

Время обработки инцидентов. Устойчивая тенденция снижения общего времени обработки с 26,16 секунд (эксперимент 1) до 17,67 секунд (эксперимент 5). Это свидетельствует о накоплении опыта системой, кэшировании данных и оптимизации внутренних процессов. Наиболее ресурсоемкой операцией оказался поведенческий анализ в модуле SOC 4 (около 1,92 сек), что оправдано сложностью эвристических алгоритмов.

Качество обнаружения угроз. Общая эффективность системы выросла с 92,0% до 94,2% за пять экспериментов. Массовое сканирование портов детектируется с точностью до 98,9%, корреляция множественных событий от одного источника составляет 100%.

Сравнение с классической моделью. Проведенный анализ показал, что классическая связка «Фаервол + SIEM» является пассивной и требует ручного вмешательства администратора. Модель с модулем SOC 4 трансформирует систему в активного защитника (SOAR), способного автоматически выполнять локальную и облачную блокировку (через SberCloud API) за время менее 20 секунд без участия человека.

В ходе исследования был разработан и смоделирован универсальный программный модуль SOC 4 для автоматического обнаружения и предотвращения сетевых атак. Архитектура модуля, спроектированная с использованием UML-диаграмм и реализованная на связке Python/Bash, обеспечивает высокую масштабируемость и интеграцию с отечественными облачными сервисами и системами SIEM. Результаты имитационного моделирования в AnyLogic подтвердили, что внедрение модуля позволяет сократить время реакции на инцидент до 17–26 секунд и повысить общую точность детектирования угроз до 94,2%. Использование отечественной

криптографии (ГОСТ Р 34.10-2012) гарантирует соответствие требованиям регуляторов (ФСТЭК) при защите критической информационной инфраструктуры. В дальнейшем планируется расширить функционал модуля за счет внедрения алгоритмов машинного обучения для улучшения поведенческого анализа и оптимизации асинхронных API-запросов для снижения нагрузки на внешние сервисы Threat Intelligence.

Использованные источники:

- 1 Баланов, А. Н. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 680 с.
- 2 Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. — Москва: НИЯУ МИФИ, 2023. — 224 с.
- 3 Воробьев, С. П. Компьютерные сети и сетевая безопасность: учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск: ЮРГПУ (НПИ), 2022. — 216 с.
- 4 Гарсиа, Х. Анализ трафика с помощью tcpdump и Wireshark / Хосе Гарсиа. — Санкт-Петербург: БХВ-Петербург, 2022. — 272 с.
- 5 ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Стандартинформ, 2012. — 28 с.
- 6 Зенкин, А. А. Анализ сетевых атак. Методология и практика / А. А. Зенкин, С. Е. Кузнецов. — Москва: Горячая линия — Телеком, 2020. — 304 с.
- 7 Иванов, А. С. Анализ сетевого трафика с помощью Wireshark / А. С. Иванов. — Москва: СОЛОН-Пресс, 2020. — 224 с.
- 8 Культин, Н. Б. Программирование на Python в примерах и задачах / Н. Б. Культин. — Санкт-Петербург: БХВ-Петербург, 2021. — 400 с.
- 9 Лихтенштейн, В.Е. Мультиагентные системы: самоорганизация и развитие / В. Е. Лихтенштейн [и др.]. — Москва: Финансы и статистика, 2022. — 264 с.

10 Сеницын, И. В. Моделирование программных систем. Теоретические основы: учебное пособие / И. В. Сеницын, А. Л. Бескин, Ю. А. Воронцов. — Москва: РТУ МИРЭА, 2023. — 170 с.

11 Симонова, Е. В. Моделирование информационных систем: учебное пособие / Е. В. Симонова. — Самара: Самарский университет, 2022. — 204 с.

12 Уилсон, К. А. Анализ сетевого трафика. Методы мониторинга и расследования инцидентов / Крис А. Уилсон. — Санкт-Петербург: БХВ-Петербург, 2020. — 368 с.

13 Фёдоров, С. Ю. Реализация ГОСТ Р 34.10-2012 в сетевых системах: практическое руководство / С. Ю. Фёдоров. — М.: ДМК Пресс, 2022. — 178 с.

14 Черемушкин, А. В. Лекции по арифметике и информационной безопасности / А. В. Черемушкин. — М.: МЦНМО, 2021. — 272 с.