

РЕАЛИЗАЦИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ОСНОВЕ РЕШЕНИЙ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

В.Д. Зимнюкова¹, А.С. Ершов¹

¹*Саратовский государственный технический университет им. Гагарина Ю.А.,
г. Саратов,
e-mail: veronikazimnukova@gmail.com*

Аннотация

В статье рассматривается проектирование и реализация интегрированной системы обнаружения сетевых атак на базе открытых решений Snort и ELK Stack. Анализируются современные подходы к мониторингу ИБ и требования нормативных документов ФСТЭК России. Описывается лабораторный стенд из четырёх виртуальных машин: сенсор Snort, сервер ELK, целевой сервер и машина атакующего. Представлены результаты тестирования при различных типах. Эффективность системы подтверждает высокую точность обнаружения и применимость для организаций с ограниченными ресурсами.

Ключевые слова: обнаружение сетевых атак, Snort, ELK Stack, SIEM, IDS, мониторинг информационной безопасности, кибератака, система мониторинга ИБ, система обнаружения вторжений.

Введение

В условиях цифровой трансформации вопросы информационной безопасности становятся критически важными. Организации сталкиваются с ростом сложных сетевых атак, которые постоянно эволюционируют. В связи с этим особую актуальность приобретают системы обнаружения вторжений (IDS) и управления событиями безопасности (SIEM). Цель работы – проектирование и реализация интегрированной системы обнаружения и визуализации сетевых атак на базе open-source решений.

1. Системы обнаружения вторжений и управления событиями безопасности

Системы обнаружения вторжений (IDS) работают в режиме, близком к реальному времени [10]. Они захватывают и декодируют пакеты, используя сигнатурный анализ для выявления известных угроз и поведенческие методы для обнаружения аномалий.

Эволюция подходов к мониторингу информационной безопасности демонстрирует закономерный переход от изолированных IDS к комплексным платформам управления событиями безопасности. SIEM-системы представляют собой платформы для централизованного сбора, хранения, анализа и корреляции событий безопасности из разнородных источников [6]. Интеграция IDS и SIEM создаёт взаимоусиливающий эффект.

2. Требования к мониторингу информационной безопасности в Российской Федерации

Основополагающим документом по мониторингу информационной безопасности является ГОСТ Р 59547-2021. Он устанавливает требования к системам мониторинга [2].

Приказ ФСТЭК России №21 от 18 февраля 2013 г. определяет организационные и технические меры для защиты персональных данных. Документ включает требования к обнаружению вторжений, а также к мониторингу событий безопасности [1].

В совокупности эти документы формируют комплексную систему требований для создания эффективных систем обнаружения и противодействия кибератакам. В представленном проекте соответствие требованиям ФСТЭК достигается за счёт использования Snort (поддерживает меру 8.7 Приказа №21 по обнаружению и документированию атак) и ELK Stack (обеспечивает меру 8.5 и требования ГОСТ Р 59547-2021 по сбору, хранению, нормализации, анализу и визуализации событий). Таким образом, предлагаемое решение сочетает техническую эффективность и соблюдение российского законодательства в области мониторинга информационной безопасности.

3. Обоснование выбора технологий для проекта

Выбор технологий для практической реализации системы обнаружения сетевых атак основывался на анализе технических характеристик, экономической целесообразности и образовательной ценности. В качестве базовых решений выбраны Snort (обнаружение вторжений) и ELK Stack (сбор, обработка, визуализация событий безопасности). Snort выбран благодаря технической зрелости, подтверждённой более чем 20-летней историей, что обеспечивает стабильность и предсказуемость работы [8]. ELK Stack выбран за исключительную гибкость и мощную аналитику. Модульная архитектура (Elasticsearch, Logstash, Kibana) обеспечивает полный цикл обработки данных безопасности. Elasticsearch обеспечивает высокопроизводительный поиск по большим объёмам данных, Logstash – богатый набор фильтров для преобразования, Kibana – развитые средства построения дашбордов [9].

4. Проектирование лабораторного стенда

Лабораторный стенд включает четыре виртуальные машины с чётким распределением ролей (рис.1). Сервер ELK Stack (Ubuntu Server 22.04 LTS) – центральный узел сбора и анализа событий. Сенсор Snort IDS (Ubuntu Server 22.04 LTS) мониторит сетевой трафик. Целевой сервер – Metasploitable 2 (имитация уязвимой системы), машина атакующего – Kali Linux 2025.3 (генерация тестового вредоносного трафика).

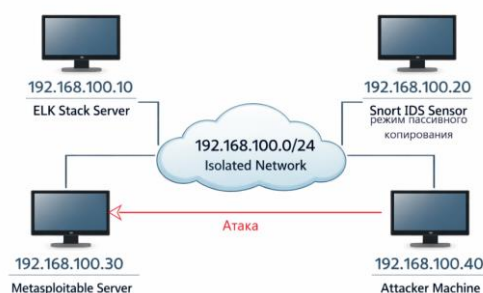


Рисунок 1 – Схема стенда

Все ВМ объединены в изолированную сеть 192.168.100.0/24 для исключения влияния на внешние системы и воспроизводимости экспериментов. IP-адреса: Snort – 192.168.100.20 (режим пассивного копирования), ELK – 192.168.100.10 (приём событий по syslog), целевой сервер – 192.168.100.30, атакующий – 192.168.100.40.

В ходе работы разработан комплекс кастомных правил Snort для выявления различных типов атак: подбор учётных данных (SSH, FTP, RDP), сканирование сети и портов (ICMP, SYN-, FIN-, XMAS-сканирование), веб-атаки (Directory Traversal, SQL-инъекции, XSS, LFI, RFI, попытки загрузки веб-шеллов), DoS-атаки (SYN-флуд, UDP-флуд), а также подозрительная активность. Для каждого правила подобраны пороговые значения, исключающие ложные срабатывания на фоновом трафике.

5. Тестирование системы

Методика тестирования разработанной системы была основана на комплексном подходе, включающем проведение контролируемых атак различных типов с последующей оценкой эффективности их обнаружения.

1. Сканирование сети и портов

Первый этап тестирования включал сканирование сети и портов с использованием утилиты nmap (TCP сканирование – nmap -sS 192.168.100.30, UDP сканирование – nmap -sU 192.168.100.30 -p 53,161,123,137,138,139,500,514).

После выполнения атак с Kali Linux на Metasploitable дашборды Kibana показали обнаружение SNMP и DNS сканирования с атакующей машины 192.168.100.40.

2. DoS-атаки

Для проверки обнаружения DoS-атак, была проведена тестовая DoS-атака с использованием hping3 на порт 80 с флудом SYN-пакетов (sudo hping3 -S -flood -p 80 192.168.100.30). После проведения Dos-атак временной график зафиксировал всплеск алертов в период атаки, появились алерты категорий "BAD-TRAFFIC tcp port 0 traffic" и "MISC Source Port 0/53 to +1024", характерные для SYN-флуд атак.

3. Веб-атаки

Для проверки обнаружения Веб-атак были проведены веб-атаки, включая попытки доступа к /etc/passwd, /etc/shadow и XSS-атаку через параметр search.php (curl «http://192.168.100.30/../../../../etc/passwd», curl «http://192.168.100.30/../../../../etc/shadow»). В результате дашборды продемонстрировали следующие изменения: Snort успешно выявил все три типа веб-атак, количество записей увеличилось до 25.

4. Использование сканера уязвимостей

Был применен сканер уязвимостей dirb для сканирования веб-директорий (dirb http://192.168.100.30). В результате проведения атаки временной график показывал пик около 1200 событий, общее количество алертов достигло 1456, протокольное распределение стало практически полностью TCP-ориентированным (99.73%).

5. Атаки на аутентификацию

Были проведены естовые атаки на аутентификацию методом грубой силы на SSH и FTP сервисы с использованием Hydra и Medusa (hydra -l anonymous -P test_pass.txt -t 2 ftp://192.168.100.30, medusa -h 192.168.100.30 -u root -P test_pass.txt -M ssh). В результате система зафиксировала события "INFO FTP Bad login" с источником 192.168.100.30, показывающие направление трафика от сервера к клиенту, что подтверждает фиксацию системой реакции сервисов на атаки.

Анализ результатов и выводы

Тестирование показало высокую эффективность системы: все запланированные атаки обнаружены с минимальной задержкой, все кастомные правила сработали корректно.

Практическая значимость проведенного исследования заключается в создании рабочего прототипа системы мониторинга ИБ, доступного для организаций с ограниченными финансами.

Список использованных источников

1. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – 2013.
2. ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности». – 2021.
3. Информационное письмо ФСТЭК России «Об утверждении требований к системам обнаружения вторжений».
4. Академия Selectel – Что такое SIEM. – URL: <https://selectel.ru/blog/what-is-siem/> (дата обращения: 01.07.2026).
5. Kaspersky SecureList Статистика. – URL: <https://statistics.securelist.com/ru/intrusion-detection-scan/day> (дата обращения: 01.07.2026).
6. Snort – Network Intrusion Detection & Prevention System. – URL: <https://snort.org> (дата обращения: 01.07.2026).
7. ELK Stack – Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash | Elastic. – URL: <https://www.elastic.co/elastic-stack> (дата обращения: 01.07.2026).
8. Академия Selectel – IPS/IDS – системы обнаружения и предотвращения вторжений. – URL: <https://selectel.ru/blog/ips-and-ids/> (дата обращения: 01.07.2026).

IMPLEMENTATION OF A NETWORK ATTACK DETECTION SYSTEM BASED ON OPEN-SOURCE SOLUTIONS

V.D. Zimnyukova¹, A.S. Ershov¹

*¹Yuri Gagarin State Technical University, Saratov
e-mail: veronikazimnukova@gmail.com*

Abstract

The article discusses the design and implementation of an integrated network attack detection system based on open-source solutions Snort and ELK Stack. It analyzes modern approaches to information security monitoring and the requirements of the Federal Service for Technical and Export Control of Russia. The article describes a laboratory setup consisting of four virtual machines: a Snort sensor, an ELK server, a target server, and an attacker's machine. The article presents the results of testing the system under different conditions. The effectiveness of the system is confirmed by its high detection accuracy and its suitability for organizations with limited resources.

Keywords: network attack detection, Snort, ELK Stack, SIEM, IDS, information security monitoring, cyber attack, information security monitoring system, intrusion detection system.