Проектирование системы обнаружения сетевых атак на базе решений с открытым исходным кодом Snort и ELK Stack

В.Д. Зимнюкова, А.С. Ершов

Саратовский государственный технический университет имени Гагарина Ю.А., Саратов, Россия

Аннотация **– В статье рассматривается процесс проектирования и практической реализации интегрированной системы обнаружения сетевых атак на основе решений с открытым исходным кодом – Snort и ELK Stack. Проводится анализ современных подходов к мониторингу информационной безопасности, исследуются требования нормативных документов ФСТЭК России и российского законодательства к системам обнаружения вторжений и управления событиями безопасности. Описывается архитектура лабораторного стенда, включающая четыре виртуальные машины с распределением ролей: сенсор Snort IDS, сервер ELK Stack, целевой сервер-жертву и машина атакующего. Демонстрируется процесс настройки пересылки логов, разработки правил обнаружения и создания визуализаций в Kibana. Представлены результаты тестирования системы при проведении различных типов атак: сканирование сети, DoS-атаки, веб-атаки, подбор учетных данных и использование сканера уязвимостей. Анализ эффективности разработанной системы подтверждает высокую точность обнаружения и практическую применимость предложенного подхода 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 и повсеместного распространения информационных технологий вопросы обеспечения информационной безопасности приобретают критическую важность. Современные организации сталкиваются с беспрецедентным ростом количества и сложности сетевых атак, которые становятся все более изощренными и целенаправленными. Особую тревогу вызывает эволюция методов киберпреступников — от массовых автоматизированных атак к целевым сложносоставным кампаниям, использующим социальную инженерию и продвинутые техники уклонения от обнаружения. Традиционные системы защиты периметра оказываются недостаточно эффективными против современных угроз, требующих комплексного подхода к мониторингу безопасности.

В этой связи особую актуальность приобретают системы обнаружения вторжений (Intrusion Detection System, IDS), способные выявлять аномальную активность внутри сетевой инфраструктуры, и системы управления событиями безопасности (Security Information and Event Management, SIEM), обеспечивающие централизованный сбор, корреляцию и анализ событий безопасности. Однако их разрозненное использование не позволяет в полной мере реализовать потенциал современных технологий защиты.

I. ПОСТАНОВКА ЗАДАЧИ

Целью данной работы является проектирование и практическая реализация интегрированной системы обнаружения и визуализации сетевых атак на базе решений с открытым исходным кодом. Такой подход позволяет не только продемонстрировать эффективность комплексного мониторинга безопасности, но и предложить экономически эффективное решение для организаций различного масштаба.

II. СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ

Системы обнаружения вторжений функционируют на основе анализа сетевого трафика в режиме, близком к реальному времени [1]. Основополагающим принципом является пассивный мониторинг передаваемых данных без воздействия на сетевые потоки. Система осуществляет захват пакетов, их декодирование и последующий анализ с применением методов выявления аномалий. Сигнатурный анализ позволяет идентифицировать известные угрозы путем сравнения с эталонными шаблонами атак, в то время как поведенческие методы направлены на обнаружение

отклонений от базового профиля нормальной сетевой активности [1].

Традиционные системы обнаружения вторжений обладают рядом принципиальных ограничений, сужающих область их эффективного применения в современных условиях. Наиболее существенным недостатком является контекстная изоляция анализа, при которой IDS обрабатывает сетевые события обособленно, без учета данных от других источников безопасности. Значительной проблемой остается высокий уровень ложных срабатываний, требующий постоянного вмешательства аналитиков для верификации инцидентов и тонкой настройки правил детектирования.

Эволюция подходов к мониторингу информационной безопасности демонстрирует закономерный переход от изолированных систем обнаружения вторжений к комплексным платформам управления событиями безопасности. SIEM-системы представляют собой платформы для централизованного сбора, хранения, анализа и корреляции событий безопасности из разнородных источников [2]. Ключевой функцией современных SIEM-решений является агрегация данных безопасности из различных систем. Сбор и нормализация логов позволяют привести разноформатные данные к единому стандарту, что существенно облегчает их последующий анализ.

Интеграция систем обнаружения вторжений и платформ управления событиями безопасности создает взаимоусиливающий эффект, значительно повышающий эффективность защиты информационной инфраструктуры. Основное преимущество интеграции заключается в возможности комплексного анализа данных безопасности из различных источников, что позволяет выявлять сложные целевые атаки, остающиеся незамеченными при раздельном использовании этих систем. Архитектура системы с интеграцией SIEM и IDS изображена на Рис. 1.

Рис. 1. Архитектура системы с интеграцией SIEM и IDS

III. ТРЕБОВАНИЯ К МОНИТОРИНГУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

Основополагающим документом, регламентирующим процессы мониторинга, является ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности». Данный стандарт устанавливает требования к системам мониторинга информационной безопасности, включая сбор, нормализацию, анализ и корреляцию событий безопасности, а также определяет порядок их функционирования в автоматизированных системах различного уровня [3].

Приказ ФСТЭК России от 18 февраля 2013 г. № 21 определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах. Данный документ включает требования по реализации мер по обнаружению (предотвращению) вторжений, а также мер по мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них [4].

С 1 марта 2026 вступил в силу приказ ФТЭК 117 от 11 апреля 2025 г. «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». В данном приказе указано, что для достижения целей защиты информации оператором (обладателем информации) должны проводиться мероприятия по осуществлению мониторинга информационной безопасности в соответствии с разделами 4 и 5 ГОСТ Р 59547-2021 [5,6].

Совокупность рассмотренных документов формирует комплексную систему требований, обеспечивающих создание эффективных систем обнаружения и противодействия кибератакам. Соответствие выбранных в данном проекте решений требованиям ФСТЭК обеспечивается за счет использования Snort (система предотвращения и обнаружения вторжений), поддерживающего необходимые функции обнаружения и документирования атак в соответствии с мерой 8.7 Приказа № 21, и ELK Stack (набор инструментов для обработки логов, полученных системой обнаружения вторжений) предоставляющего требуемые возможности сбора, хранения, нормализации, анализа и визуализации событий безопасности в соответствии с мерой 8.5 и требованиями ГОСТ Р 59547-2021. Таким образом, предлагаемое решение не только демонстрирует техническую эффективность, но и учитывает требования российского законодательства в области мониторинга информационной безопасности.

IV. ОБОСНОВАНИЕ ВЫБОРА ТЕХНОЛОГИЙ ДЛЯ ПРОЕКТА

Выбор технологий для практической реализации системы обнаружения сетевых атак осуществлялся на основе комплексного анализа технических характеристик, экономической целесообразности и образовательной ценности решений. В качестве базовых технологий были выбраны Snort для функций обнаружения вторжений и ELK Stack для задач сбора, обработки и визуализации событий безопасности.

Выбор технологии Snort обусловлен ее технической зрелостью, подтвержденной более чем 20-летней историей развития, что обеспечивает стабильность работы и предсказуемость поведения системы. Архитектура Snort, основанная на модульном принципе, позволяет глубоко изучить механизмы работы современных систем обнаружения атак, начиная от захвата сетевого трафика и заканчивая применением сложных правил корреляции [7]. Открытая модель разработки правил обнаружения обеспечивает неограниченные возможности для создания специализированных сигнатур, адаптированных под конкретные исследовательские задачи.

Выбор технологии ELK Stack основан на ее исключительной гибкости и мощных возможностях аналитики. Модульная архитектура, состоящая из набора инструментов Elasticsearch, Logstash и Kibana, предоставляет полный цикл обработки данных безопасности – от приема и нормализации логов до их индексирования, хранения и интерактивной визуализации [8]. Компонент Elasticsearch обеспечивает высокопроизводительное полнотекстовое индексирование и поиск по большим объемам данных, программа Logstash предлагает богатый набор фильтров для преобразования данных, а Kibana предоставляет развитые средства построения дашбордов [8].

V. ПРОЕКТИРОВАНИЕ ЛАБОРАТОРНОГО СТЕНДА

Архитектура лабораторного стенда включает четыре виртуальные машины с четким распределением ролей и специализированным подбором операционных систем. Сервер ELK Stack выполняет функции центрального узла сбора и анализа событий безопасности на базе Ubuntu Server 22.04 LTS. Сенсор Snort IDS осуществляет мониторинг сетевого трафика, выявляя потенциально вредоносную активность, и также функционирует под управлением Ubuntu Server 22.04 LTS. Целевой сервер на базе уязвимой виртуальной машины Metasploitable 2, а машина атакующего использует операционную систему Kali Linux 2025.3 для генерации тестового вредоносного трафика.

Организация сетевой инфраструктуры построена на принципах сегментации и контролируемого взаимодействия между компонентами. Все виртуальные машины объединены в изолированную сеть с адресным пространством 192.168.100.0/24, что исключает непреднамеренное воздействие на внешние системы и обеспечивает воспроизводимость экспериментов. Сенсор Snort IDS с адресом 192.168.100.20 выполняет пассивный мониторинг всего сетевого трафика, сервер ELK Stack на адресе 192.168.100.10 принимает события через syslog-протокол, целевой сервер с адресом 192.168.100.30 представляет собой уязвимую систему, а машина атакующего с адресом 192.168.100.40 генерирует тестовые атаки. Схема виртуального стенда представлена на Рис. 2.

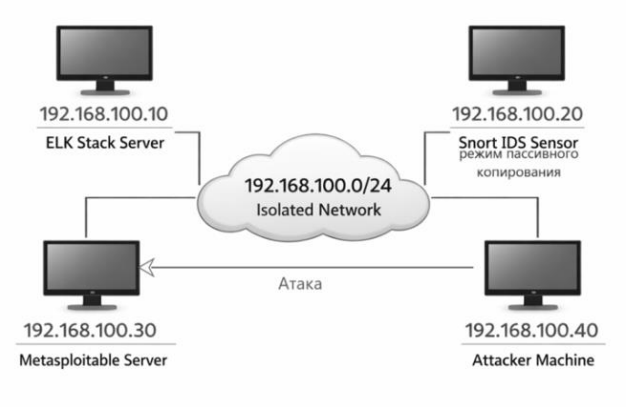

Рис. 2. Схема виртуального стенда

Критически важным аспектом являлась настройка режима promiscuous mode для сетевого интерфейса сенсора Snort IDS, позволяющего принимать и анализировать весь трафик, проходящий через сетевой сегмент, независимо от адреса назначения.

Для эффективного выявления различных типов атак в виртуальном стенде был разработан комплекс кастомных правил для сенсора Snort. При создании правил была изучена официальная документация и применялись различные опции: анализ флагов TCP, поиск специфического содержимого в пакетах, пороговые значения для обнаружения аномальной активности.

В ходе работы были разработаны правила для обнаружения следующих типов атак: подбор учётных данных (SSH, FTP, RDP), сканирование сети и портов (ICMP-запросы, SYN-, FIN- и XMAS-сканирование), веб-атаки (Directory Traversal, SQL-инъекции, XSS, Local File Inclusion, Remote File Inclusion, попытки загрузки веб-шеллов), атаки типа «отказ в обслуживании» (SYN-флуд, UDP-флуд), а также подозрительная активность. Для каждого правила подобраны пороговые значения, исключающие ложные срабатывания на фоновом трафике виртуальной сети. Разберем синтаксис правил на примере правила распознавания SYN-сканирования: alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SYN

Scan Detection"; flags:S; detection_filter:track by_src, count 10, seconds 10; sid:1000006; rev:1;).

alert – сгенерировать алерт.

tcp – только TCP-пакеты.

$EXTERNAL_NET any – любой внешний IP, любой порт источника.

-> – направление от источника к получателю.

$HOME_NET any – защищаемая сеть (любой IP), любой порт назначения.

msg – текст алерта.

flags:S – установлен только флаг SYN.

detection_filter: track by_src, count 10, seconds 10 – сработает, когда от одного IP-источника за 10 секунд будет 10 или более таких пакетов.

sid, rev – идентификатор и версия.

VI. ТЕСТИРОВАНИЕ СИСТЕМЫ

Методика тестирования разработанной системы была основана на комплексном подходе, включающем проведение контролируемых атак различных типов с последующей оценкой эффективности их обнаружения. План проведения тестовых атак предусматривал последовательное выполнение сценариев, имитирующих реальные угрозы информационной безопасности.

A. Сканирование сети и портов

Первый этап тестирования включал сканирование сети и портов с использованием утилиты nmap.

nmap -sU 192.168.100.30 -p 53,161,123,137,138,139,500,514 – UPD-сканирование.

nmap -sS 192.168.100.30 – TCP-сканирование.

После выполнения атак с Kali Linux на Metasploitable дашборды Kibana показали обнаружение SNMP и DNS сканирования с атакующей машины 192.168.100.40 (Рис. 3). В логах видны запросы к UDP-порту 161 (SNMP), TCP-порту 161 (SNMP), TCP-порту 705 (SNMP AgentX) и UDP-порту 53 (DNS). Это соответствует выполненным командам nmap -sU и nmap -sS.

Рис. 3. Изменения дашбордов после проведения сканирования сети и портов

B. Dos-атака

Были проведены тестовые DoS-атаки 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, доля TCP-трафика возросла до 90,7%, появились алерты категорий "BAD-TRAFFIC tcp port 0 traffic" и "MISC Source Port 0/53 to +1024", характерные для SYN-флуд атак (Рис. 4).

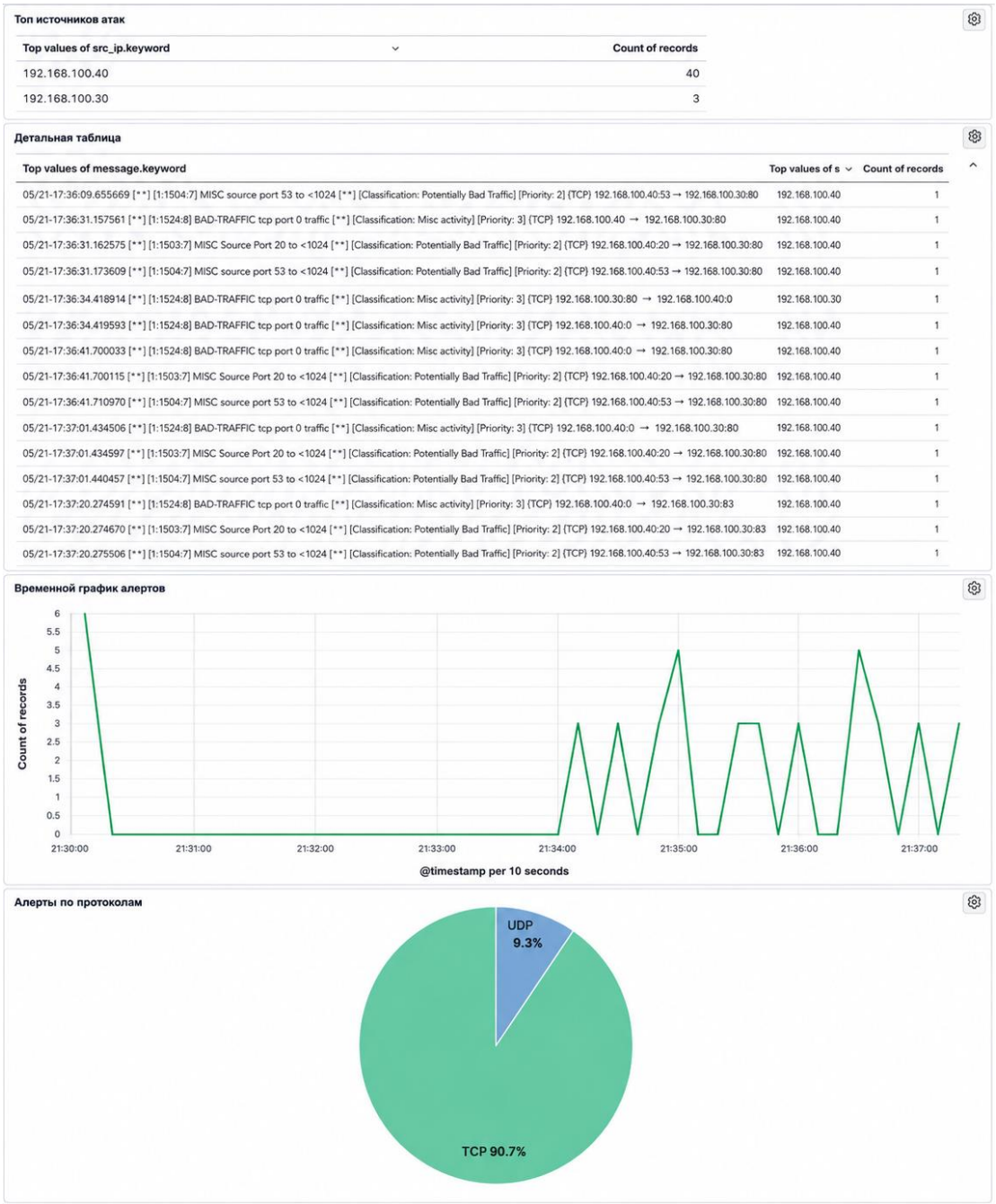

Рис. 4. Изменения дашбордов после проведения Dos-атаки

C. Веб-атаки

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” – Path Traversal

curl “http://192.168.100.30/../../../etc/shadow” – Path Traversal

curl “http://192.168.100.30/search.php?q=<script>alert(‘XSS’)</script>” – внедрение тега <script>alert('xss')</script> в параметр q запроса.

Дашборды продемонсрировали следующие изменения: сенсор Snort успешно выявил все три типа веб-атак, количество записей увеличилось, на графике появились новые пики в периоды выполнения атак (Рис. 5).

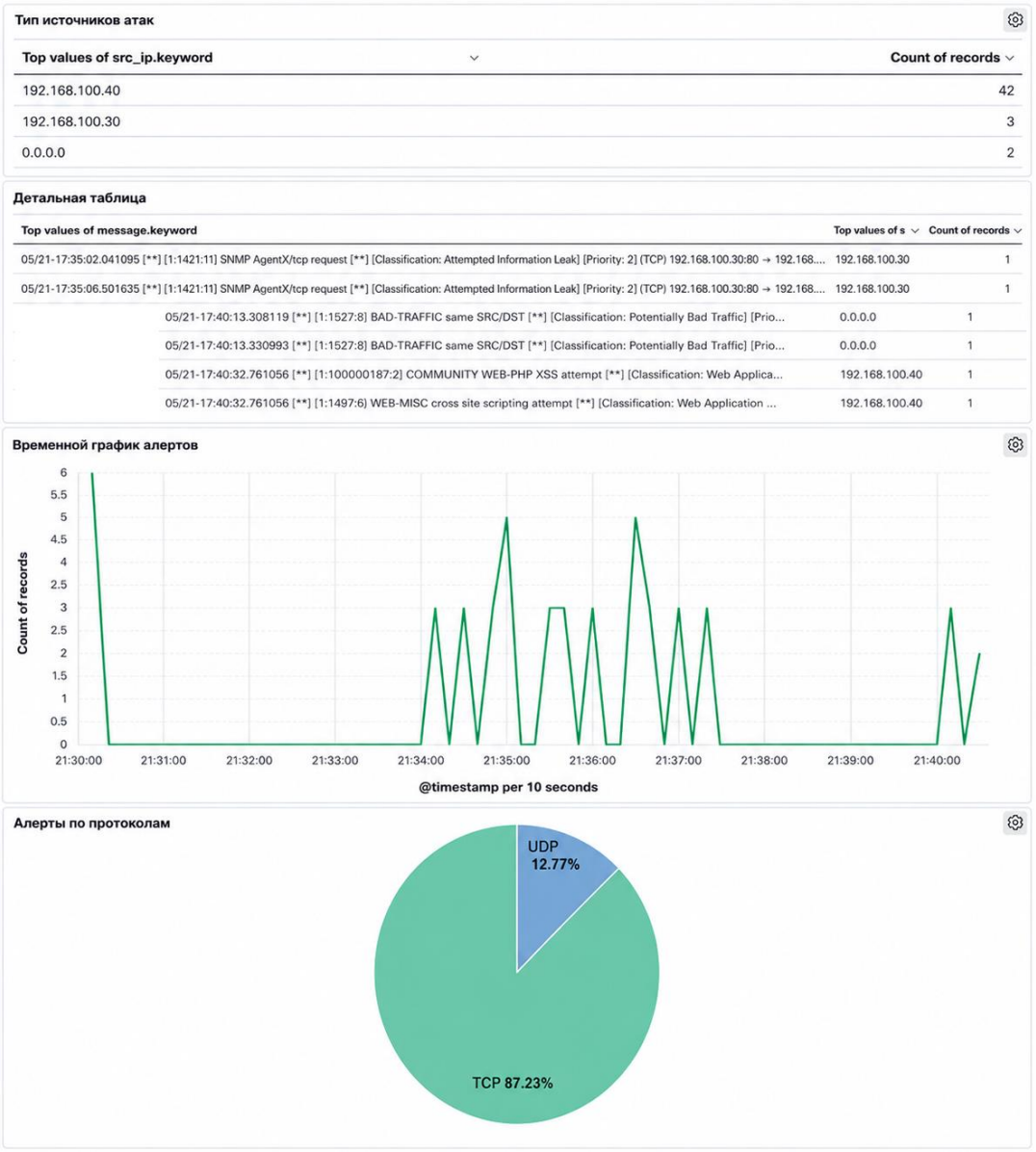

Рис. 5. Изменения дашбордов после проведения Веб-атак

D. Использование сканера уязвимостей

Использовали сканер уязвимостей dirb для сканирования веб-директорий.

dirb http://192.168.100.30

Дашборды отражают значительные изменения: временной график показывает несколько пиковых скачков, появились алерты от целевого сервера, протокольное распределение является полностью TCP-ориентированным.

На Рис. 6 показаны зафиксированные системой события, которые произошли из-за проведения этой атаки.

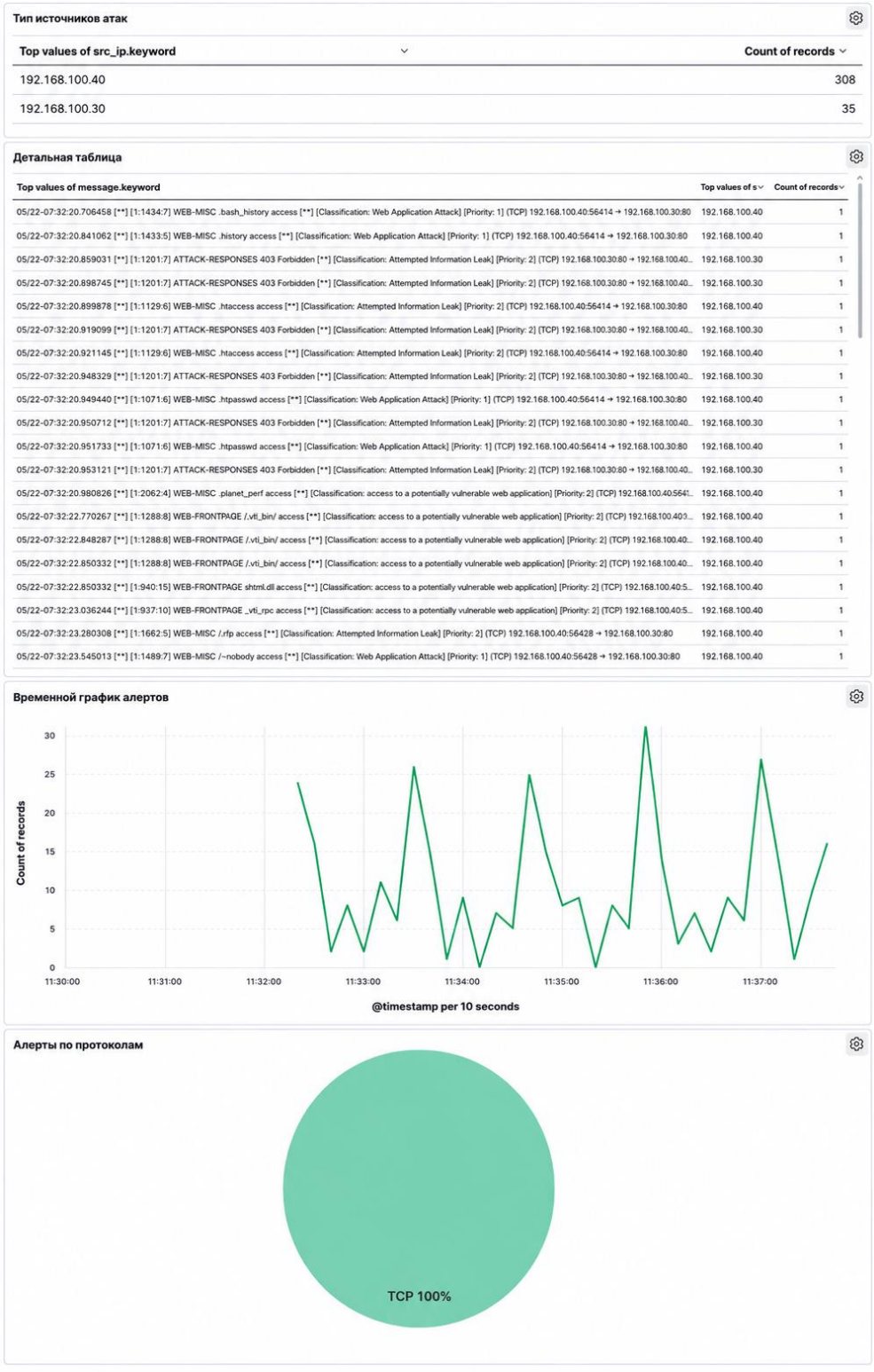

Рис. 6. Изменения дашбордов после проведения атаки с использованием сканера уязвимостей

Е. Атаки на аутентификацию

Были проведены тестовые атаки на аутентификацию методом грубой силы на SSH и FTP сервисы с использованием инструментов для подбора паролей методом грубой силы – Hydra и Medusa.

hydra -l annonymous -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

Дашборд демонстрирует изменения после проведения атак: появились алерты "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 (Рис. 7).

Детальная таблица

Top values of message.keyword	Top values of src_ip.keyword	Count of records
12/07-10:23:29.579984 [**] [1:491:8] INFO FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.30:21 → 192.168.100.40:34616	192.168.100.30	1
12/07-10:23:29.579984 [**] [1:491:8] INFO FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.30:21 → 192.168.100.40:34628	192.168.100.30	1
12/07-10:23:33.236749 [**] [1:491:8] INFO FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.30:21 → 192.168.100.40:34616	192.168.100.30	1
12/07-10:23:33.356766 [**] [1:491:8] INFO FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.30:21 → 192.168.100.40:34628	192.168.100.30	1
12/07-10:23:36.526254 [**] [1:491:8] INFO FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.30:21 → 192.168.100.40:34616	192.168.100.30	1
12/07-10:23:36.653649 [**] [1:491:8] INFO FTP Bad login [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.30:21 → 192.168.100.40:34628	192.168.100.30	1

Рис. 7. Изменения дашбордов после проведения атаки на аутентификацию

VII. АНАЛИЗ РЕЗУЛЬТАТОВ И ВЫВОДЫ

Анализ результатов тестирования продемонстрировал высокую эффективность обнаружения различных типов атак разработанной системой. Все запланированные тестовые атаки были успешно обнаружены с минимальным временем задержки между началом атаки и появлением соответствующего оповещения в платформе визуализации данных Kibana. Временные характеристики системы варьировались в зависимости от типа атаки – простые атаки сканирования обнаруживались практически мгновенно, в то время как сложные многоэтапные атаки требовали накопления статистики для срабатывания пороговых правил.

Точность срабатывания правил оказалась исключительно высокой – все кастомные правила, разработанные в рамках проекта, продемонстрировали корректную работу.

ЗАКЛЮЧЕНИЕ

Практическая значимость проведенного исследования заключается в создании работоспособного прототипа системы мониторинга информационной безопасности, который может быть развернут в организациях с ограниченными финансовыми ресурсами без потери функциональности. Предложенная архитектура легко масштабируется за счет добавления дополнительных сенсоров Snort в различные сегменты сети, а гибкость набора инструментов ELK Stack позволяет подключать новые источники событий безопасности без существенной модификации существующей конфигурации.

ЛИТЕРАТУРА

[1] Академия Selectel – IPS/IDS — системы обнаружения и предотвращения вторжений [Электронный ресурс] – Режим доступа: https://selectel.ru/blog/ips-and-ids/, свободный (дата обращения: 13.02.2026).

[2] Академия Selectel – Что такое SIEM [Электронный ресурс] – Режим доступа: https://selectel.ru/blog/what-is-siem/, свободный (дата обращения: 13.02.2026).

[3] ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности».

[4] 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».

[5] Приказ ФСТЭК России от 11 апреля 2025 г. №117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

[6] Информационное письмо ФСТЭК России «Об утверждении требований к системам обнаружения вторжений».

[7] Snort – Network Intrusion Detection & Prevention System [Электронный ресурс] – Режим доступа: https://snort.org, свободный (дата обращения: 10.02.2026). Kaspersky SecureList Статистика [Электронный ресурс] – Режим доступа: https://statistics.securelist.com/ru/intrusion-detection-scan/day, свободный (дата обращения: 13.02.2026).

[8] ELK Stack – Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash | Elastic [Электронный ресурс] – Режим доступа: https://www.elastic.co/elastic-stack, свободный (дата обращения: 10.02.2026).

Информация об авторах

Зимнюкова Вероника Дмитриевна, студентка четвертого курса, учебной группы б2-ИФБС-41, направления 10.03.01 «Информационная безопасность», Саратовского государственного

технического университета имени Гагарина Ю.А., г. Саратов, Россия, veronikazimnukova@gmail.com

Ершов Алексей Сергеевич, доцент кафедры ИБС, к.т.н., Саратовского государственного технического университета, имени Гагарина Ю.А., г. Саратов, Россия, ershovas@sstu.ru.

Design of the network attacks detection system based on Snort and ELK Stack

Veronika Zimnyukova, Alexey Ershov

Yuri Gagarin Saratov State Technical University, Saratov, Russia

***Abstract* – The article discusses the process of designing and practical implementation of an integrated network attack detection system based on open-source solutions – Snort and ELK Stack. The analysis of modern approaches to monitoring of information security is carried out, the requirements of regulatory documents of the FSTEC of Russia and Russian legislation to intrusion detection systems and management of security events are investigated. The architecture of a laboratory stand is described, including four virtual machines with role distribution: Snort IDS sensor, ELK Stack server, target server-victim and machine of the attacker. The article demonstrates the process of configuring log forwarding, developing detection rules, and creating visualizations in Kibana. The article presents the results of testing the system during various types of attacks, including network scanning, DoS attacks, web attacks, credential harvesting, and vulnerability scanning. The analysis of the system's effectiveness confirms its high accuracy.**

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

REFERENCES

[1] Akademiya Selectel – IPS/IDS — sistemy obnaruzheniya i predotvrashcheniya vtorzhenij [Elektronnyj resurs] – Rezhim dostupa: https://selectel.ru/blog/ips-and-ids/, svobodnyj (data obrashcheniya: 13.02.2026).

[2] Akademiya Selectel – Chto takoe SIEM [Elektronnyj resurs] – Rezhim dostupa: https://selectel.ru/blog/what-is-siem/, svobodnyj (data obrashcheniya: 13.02.2026).

[3] GOST R 59547-2021 «Zashchita informacii. Monitoring informacionnoj bezopasnosti».

[4] Prikaz FSTEK Rossii ot 18 fevralya 2013 g. №21 «Ob utverzhdenii sostava i soderzhaniya organizacionnyh i tekhnicheskih mer po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh».

[5] Prikaz FSTEK Rossii ot 11 aprelya 2025 g. №117 «Ob utverzhdenii trebovanij o zashchite informacii, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah, inyh informacionnyh sistemah gosudarstvennyh organov, gosudarstvennyh unitarnyh predpriyatij, gosudarstvennyh uchrezhdenij».

[6] Informacionnoe pis'mo FSTEK Rossii «Ob utverzhdenii trebovanij k sistemam obnaruzheniya vtorzhenij».

[7] Snort – Network Intrusion Detection & Prevention System [Elektronnyj resurs] – Rezhim dostupa: https://snort.org, svobodnyj (data obrashcheniya: 10.02.2026). Kaspersky SecureList Statistika [Elektronnyj resurs] – Rezhim dostupa: https://statistics.securelist.com/ru/intrusion-detection-scan/day, svobodnyj (data obrashcheniya: 13.02.2026).

[8] ELK Stack – Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash | Elastic [Elektronnyj resurs] – Rezhim dostupa: https://www.elastic.co/elastic-stack, svobodnyj (data obrashcheniya: 10.02.2026).

Information about the authors

Zimnyukova Veronika Dmitrievna, fourth-year student, study group b2-IFBS-41, direction 10.03.01 "Information Security", Yuri Gagarin State Technical University of Saratov, Saratov, Russia, veronikazimnukova@gmail.com

Ershov Alexey Sergeevich, Associate professor of the Department of Information Security, Candidate of Technical Sciences, Yuri Gagarin State Technical University of Saratov, Saratov, Russia, ershovas@sstu.ru.