УДК 004.56: 65.011.56

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФФИКЕ

И.А. ТРЕТЬЯКОВ, М.Г. ЧУМАЧЕНКО

Донецкий государственный университет, Российская Федерация

Поступила в редакцию 01 апреля 2025

Аннотация. В настоящей работе разработана автоматизированная система оповещения о потенциальных атаках на сетевой траффик. Система способна в реальном времени анализировать траффик на предмет наличия аномалий, характерных для различных видов атак, что значительно повышает уровень информационной безопасности в условиях постоянно растущей угрозы сетевых атак.

Ключевые слова: информационная безопасность, аномалия, сетевая атака, траффик, автоматизированная система, машинное обучение, python.

Введение

В современном мире, где объёмы передаваемых данных постоянно растут, и сетевые технологии становятся всё более сложными и многофункциональными, вопросы информационной безопасности занимают одно из центральных мест в повестке дня многих организаций и индивидуальных пользователей. Среди многочисленных аспектов информационной безопасности особое внимание привлекают атаки на сетевой траффик [1-3], способные нарушить нормальное функционирование информационных систем, привести к утечке или потере данных, а также к существенным финансовым потерям. Предотвращение таких угроз информационной безопасности невозможно без разработки и внедрения специализированных автоматизированных систем на основе методов и средств машинного обучения [4-6].

Архитектура разрабатываемой системы

Автоматизированная система обнаружения аномалий в сетевом траффике реализована на высокоуровневом языке программирования общего назначения Python и представляет собой комплексное решение, способное в режиме реального времени анализировать траффик на предмет наличия потенциальных атак и аномальных действий. Архитектура системы разрабатывалась с учетом необходимости обеспечения высокой производительности, масштабируемости и гибкости в интеграции с существующими сетевыми инфраструктурами.

Компоненты автоматизированной системы обнаружения аномалий в сетевом траффике:

1. Модуль захвата данных отвечает за перехват сетевых пакетов посредством библиотеки Scapy. Scapy позволяет детально анализировать структуру каждого пакета, что является критически важным для последующего выявления аномалий.

2. Модуль предварительной обработки преобразует сырые данные пакетов в структурированный формат, подготавливая их к анализу. Включает в себя фильтрацию и валидацию данных, обеспечивая, что только релевантная информация будет передана на следующий этап.

3. Модуль машинного обучения анализирует обработанные данные на предмет выявления аномальных шаблонов основываясь на алгоритмах кластеризации (KMeans). Использование

библиотеки Sklearn позволяет эффективно применять сложные алгоритмы машинного обучения для определения потенциальных угроз.

4. Модуль логирования записывает все действия и события в системе, обеспечивая возможность последующего анализа и аудита безопасности.

5. Пользовательский интерфейс реализован посредством библиотеки Tkinter и приведен на рис. 1. Интерфейс предоставляет пользователям легкий доступ к функционалу системы, включая запуск анализа, просмотр результатов и конфигурацию настроек.

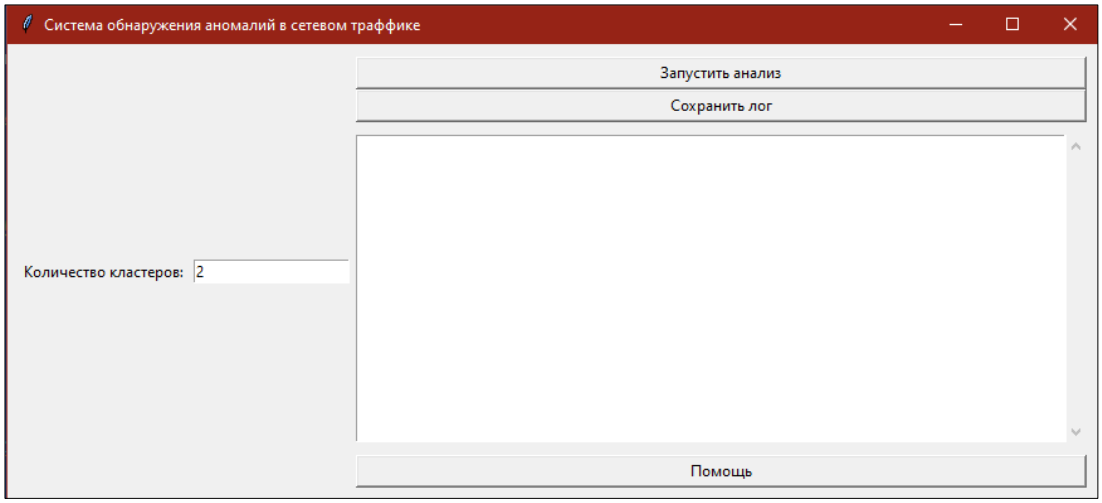

Рис. 1. Пользовательский интерфейс

Каждый компонент автоматизированной системы обнаружения аномалий в сетевом траффике спроектирован так, чтобы обеспечить максимальную эффективность и точность при идентификации потенциальных угроз. Важной частью системы является проверка корректности IP-адресов и портов, которые вводит пользователь. Валидация этих входных данных выполняется с использованием регулярных выражений и дополнительных проверок на диапазон значений, чтобы гарантировать, что анализ будет выполнен только с корректными параметрами. На рис. 2 представлены две функции, реализующие валидацию IP-адресов и портов.

```python
def validate_ip(ip_address):
    """Проверяет, является ли введенный IP-адрес валидным IPv4 адресом...."""
    ip_pattern = re.compile(r"^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$")
    if not ip_pattern.match(ip_address):
        raise ValueError("Некорректный IP-адрес.")


1 usage
def validate_port(port):
    """Проверяет, является ли введенный порт валидным...."""
    try:
        port_num = int(port)
        if not 1 <= port_num <= 65535:
            raise ValueError("Номер порта должен быть в диапазоне от 1 до 65535.")
    except ValueError:
        raise ValueError("Номер порта должен быть в диапазоне от 1 до 65535.")
```

Рис. 2. Пример реализации кода по валидации IP адреса и порта

Функция validate_ip(ip_address) предназначена для проверки является ли введенная строка корректным IPv4 адресом. Функция validate_port(port) проверяет, находится ли введенное значение порта в допустимом диапазоне (от 1 до 65535). Эти функции являются ключевыми компонентами системы валидации входных данных, обеспечивая базовую безопасность и корректность данных, используемых в дальнейших операциях системы.

После проверки корректности IP-адресов и портов, которые вводит пользователь, система начинает свою работу с захвата траффика, который проходит через сетевой интерфейс. После захвата пакеты проходят через этап предварительной обработки, где осуществляется их фильтрация и стандартизация. Далее обработанные данные направляются в модуль машинного обучения, где происходит анализ на предмет классификации трафика на нормальный и аномальный. В случае обнаружения аномалии система фиксирует событие в логах и через пользовательский интерфейс оповещает об этом администратора (рис. 3).

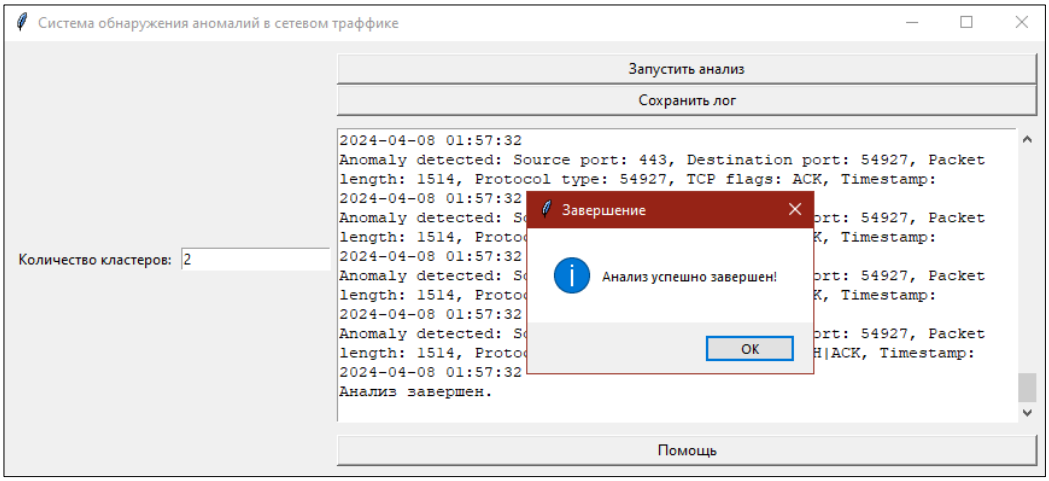

Рис. 3. Визуализация результатов анализа

Заключение

Таким образом, разработанная автоматизированная система обнаружения аномалий в сетевом траффике представляет собой мощный инструмент для обеспечения сетевой безопасности, способный оперативно реагировать на угрозы и предотвращать возможные атаки в реальном времени.

AUTOMATED SYSTEM OF ANOMALY DETECTION IN NETWORK TRAFFIC

I.A. TRETIAKOV, M.G. CHUMACHENKO

Abstract. In this paper, we have developed an automated system of notification for potential attacks on network traffic. The system is able to analyze traffic in real time for the presence of anomalies characteristic of various types of attacks, which significantly increases the level of information security in the face of an ever-growing threat of network attacks.

Keywords: information security, anomaly, network attack, traffic, automated system, machine learning, python.

Список литературы

1. Третьяков И.А., Кожекина Е.Н., Лебедев К.Е. Выявление проблем безопасности веб-сайтов посредством DoS-атаки // Вестник Донецкого национального университета. Серия Г: Технические науки. 2022. № 1. – С. 19-32. EDN UOSGY.
2. Чаругин В.В., Чесалин А.Н. Анализ и формирование наборов данных сетевого трафика для обнаружения компьютерных атак // International Journal of Open Information Technologies. 2023. Т. 11, № 6. С. 100-106. EDN HZDNHW.
3. Лаута О.С., Скоробогатов С.Ю., Перов Р.А., Привалов А.А. Разработка модели обнаружения компьютерных атак на программно-конфигурируемые сети // Известия Тульского государственного университета. Технические науки. 2023. № 5. С. 181-193. EDN GJPBPF.

4. Кажемский М.А., Шелухин О.И. Многоклассовая классификация сетевых атак на информационные ресурсы методами машинного обучения // Труды учебных заведений связи. 2019. Т. 5, № 1. С. 107-115. EDN JARTWC.
5. Мулюха В.А., Лабошин Л.Ю., Лукашин А.А., Нашивочников Н.В. Машинное обучение для анализа и классификации шифрованного сетевого трафика // Международная конференция по мягким вычислениям и измерениям. 2020. Т. 1. С. 238-241. EDN XYQCZP.
6. Бабичева М.В., Третьяков И.А. Применение методов машинного обучения для автоматизированного обнаружения сетевых вторжений // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50, № 1. С. 53-61. EDN MGBAGF.