УДК 004.4

АНАЛИЗ ПОВЕДЕНИЯ СЕТЕВОГО ТРАФИКА ПРИ DOS И DDOS АТАКА С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ВИЗУАЛИЗАЦИИ СЕТЕВЫХ АНОМАЛИЙ

Виноградская М.Ю.,

к.пед.н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Анохин В.А.,

магистрант,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация.

В статье рассматривается метод анализа поведения сетевого трафика на основе системы визуализации сетевых аномалий, реализованной в виде веб-приложения. Предложена архитектура информационной системы, обеспечивающая сбор, обработку и визуализацию параметров сетевой активности в режиме реального времени. Реализовано моделирование различных режимов функционирования сети, включая нормальный режим, DoS-атаку, DDoS-атаку и смешанный режим. В конце представлены выводы по проделанной работе.

Ключевые слова: сетевой трафик, DoS-атака, DDoS-атака, информационная безопасность, анализ сетевых данных, визуализация аномалий, веб-приложение, мониторинг сети.

ANALYSIS OF NETWORK TRAFFIC BEHAVIOR IN DOS AND DDOS ATTACKS USING A NETWORK ANOMALY VISUALIZATION SYSTEM

Vinogradskaya M.Y.,
Candidate of Pedagogical Sciences, Associate Professor,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia
Anokhin V. A.,
Master's Student,
K.E. Tsiolkovsky Kaluga State University,
Kaluga, Russia

Annotation.
This article discusses a method for analyzing network traffic behavior based on a network anomaly visualization system implemented as a web application. An information system architecture is proposed that enables the collection, processing, and visualization of network activity parameters in real time. Various network operating modes are simulated, including normal mode, DoS attack, DDoS attack, and mixed mode. Conclusions are presented at the end.
Keywords: network traffic, DoS attack, DDoS attack, information security, network data analysis, anomaly visualization, web application, network monitoring.

Современные информационные системы, обеспечивающие функционирование компьютерных сетей организаций, как правило, включают взаимосвязанные функциональные блоки мониторинга сетевого трафика и анализа сетевых событий. Первый блок обеспечивает сбор статистических данных о состоянии сети, включая количество передаваемых пакетов, задержки передачи данных и загрузку серверных ресурсов. Второй блок ориентирован на выявление сетевых аномалий и обеспечение устойчивости системы к внешним воздействиям, включая атаки типа отказа в обслуживании (DoS) и распределённого отказа в обслуживании (DDoS), при которых значительное

количество запросов приводит к перегрузке сетевых ресурсов и снижению качества обслуживания пользователей [12].

Существующие системы сетевого мониторинга и анализа трафика - Wireshark, Zabbix, Nagios — предоставляют инструменты сбора и анализа статистических данных, однако не всегда обеспечивают удобные средства визуализации динамики сетевых процессов и выявления аномальных состояний в режиме реального времени [12]. Системы анализа безопасности, такие как Snort и Suricata, ориентированы на обнаружение сигнатур известных атак, но требуют дополнительной обработки данных для визуального анализа поведения сети. Это определяет актуальность настоящего исследования, ориентированного на разработку метода анализа поведения сетевого трафика и визуализации сетевых аномалий при моделировании DoS и DDoS-атак. В результате таких воздействий происходит увеличение задержек передачи данных, снижение производительности системы и возможная недоступность сетевых сервисов [3].

Для эффективного анализа поведения сетевого трафика требуется разработка системы, способной выполнять непрерывный мониторинг параметров сетевой активности и выявлять отклонения от нормального режима функционирования сети. К основным параметрам, характеризующим состояние сети, относятся количество передаваемых пакетов, пропускная способность канала, число активных источников запросов, задержка передачи данных и уровень загрузки серверных ресурсов [4].

Задача исследования состоит в разработке метода анализа сетевого трафика, позволяющего выявлять характерные признаки DoS и DDoS-атак на основе визуализации динамики сетевых параметров. Особое внимание уделяется анализу изменения интенсивности трафика и распределения источников запросов во времени, что позволяет выявлять потенциальные угрозы на ранних стадиях их возникновения [2].

Разработанная система анализа сетевого трафика реализована в виде веб-приложения, обеспечивающего сбор, обработку и визуализацию сетевых

параметров в режиме реального времени. Архитектура системы построена по модульному принципу и включает несколько основных компонентов.

Первым компонентом является модуль сбора данных, обеспечивающий регистрацию параметров сетевого трафика, включая количество пакетов, число активных IP-адресов и задержки передачи данных. Полученные данные передаются в модуль анализа [7].

Вторым компонентом является модуль анализа сетевого трафика, предназначенный для выявления аномальных состояний сети на основе сравнения текущих параметров с нормальными значениями. При обнаружении отклонений система фиксирует возможные признаки атаки.

Третьим компонентом является модуль визуализации, отображающий состояние сети в графической форме. Визуализация реализована в виде интерактивных панелей, отображающих динамику сетевых параметров и распределение источников запросов.

В нормальном режиме функционирования сети параметры трафика изменяются плавно и находятся в допустимых пределах. Количество пакетов остаётся стабильным, задержка передачи данных минимальна, а уровень загрузки серверных ресурсов соответствует рабочему состоянию системы.

На рисунке 1 представлен интерфейс системы мониторинга сетевого трафика в нормальном режиме функционирования сети.

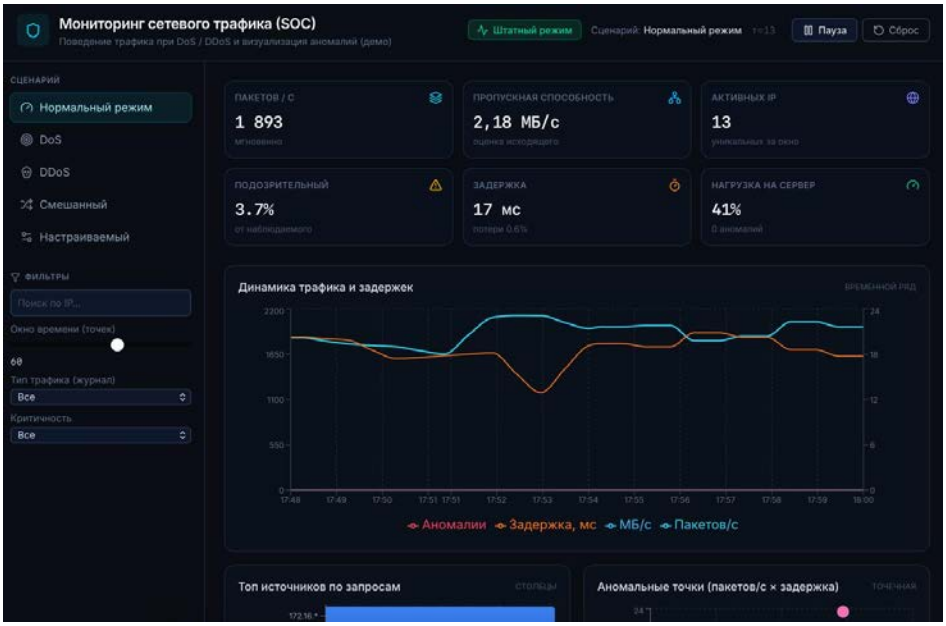

Рис. 1 - Интерфейс системы мониторинга сетевого трафика в нормальном режиме (составлено авторами)

Анализ показывает стабильные значения сетевых параметров без резких скачков нагрузки. Распределение источников запросов остаётся равномерным, а загрузка серверных ресурсов не превышает допустимые значения.

При моделировании DoS-атаки наблюдается резкое увеличение интенсивности сетевого трафика от ограниченного числа источников, что приводит к росту задержек передачи данных и увеличению нагрузки на сервер [5]. На рисунке 2 представлен интерфейс системы мониторинга при моделировании DoS-атаки.

Рис. 2 - Поведение сетевого трафика при DoS-атаке (составлено авторами)

В ходе анализа выявлено значительное увеличение количества пакетов и задержек передачи данных при относительно небольшом числе активных IP-адресов. Распределённые DDoS-атаки характеризуются большим числом источников запросов, одновременно создающих нагрузку на сеть. Это приводит к росту количества активных IP-адресов и увеличению общей нагрузки на сервер [3].

На рисунке 3 представлен интерфейс системы при моделировании DDoS-атаки. Анализ показывает значительное увеличение числа источников трафика и устойчивый рост задержек передачи данных. Нагрузка на сервер достигает критических значений, что свидетельствует о высокой вероятности отказа системы.

Рис. 3 - Поведение сетевого трафика при DDoS-атаке (составлено авторами)

Для оценки эффективности разработанной системы визуализации был проведён сравнительный анализ поведения сетевого трафика при последовательной смене режимов функционирования сети: нормальный режим, режим DoS-атаки и режим DDoS-атаки. На рисунках представлены изменения распределения источников запросов, количества аномальных точек, уровня

загрузки целевого сервера и структуры сетевого потока при переходе между режимами работы [10].

В нормальном режиме работы (рисунок 4) наблюдается равномерное распределение сетевых запросов между источниками. На диаграмме «Топ источников запросов» фиксируется умеренная активность отдельных IP-адресов без резкого превышения нагрузки. Количество аномальных точек незначительно и соответствует допустимым значениям параметров сети.

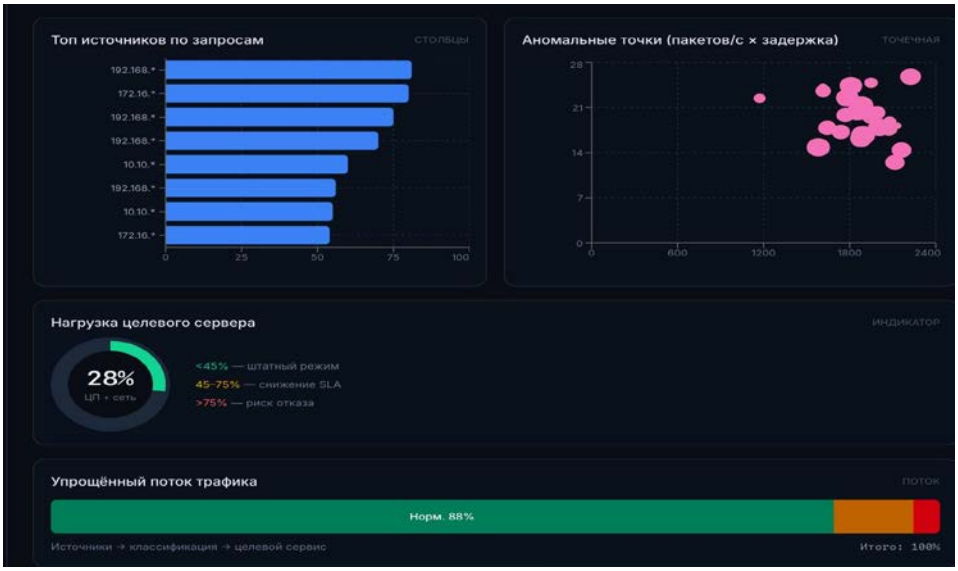

Рис. 4 — Показатели сетевого трафика в нормальном режиме работы (составлено авторами)

При переходе в режим DoS-атаки (рисунок 5) наблюдаются существенные изменения структуры сетевого трафика. Основная нагрузка начинает формироваться ограниченным числом источников, среди которых выделяется один доминирующий IP-адрес, генерирующий значительно большее количество запросов по сравнению с остальными. Количество аномальных точек увеличивается, формируя устойчивые группы отклонений по параметрам «пакеты в секунду» и «задержка передачи данных» [4].

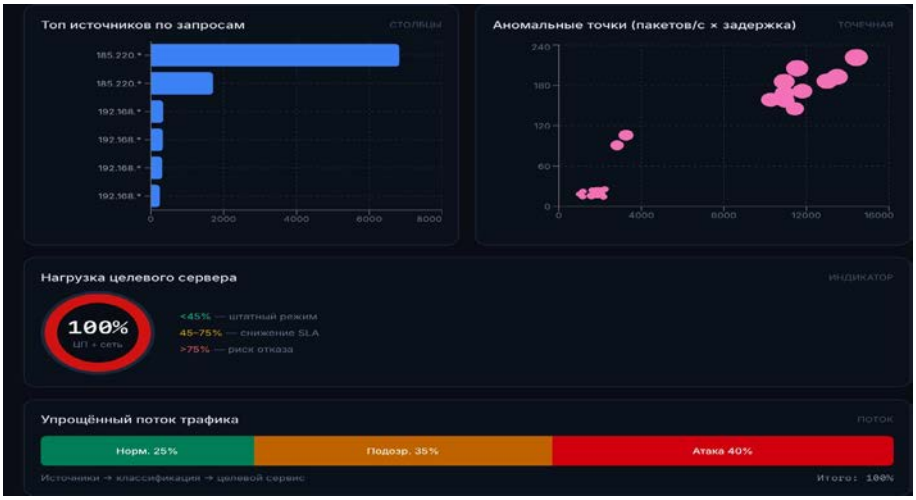

Рис. 5 — Показатели сетевого трафика при моделировании DoS-атаки (составлено авторами)

При переходе к режиму распределённой DDoS-атаки (рисунок 6) фиксируются наиболее значительные изменения параметров сети. В отличие от DoS-атаки, активность распределяется между большим числом источников, каждый из которых генерирует значительный объём запросов. На диаграмме «Топ источников запросов» наблюдается высокая активность множества IP-адресов, что является характерным признаком распределённой атаки. Количество аномальных точек существенно возрастает, формируя плотные группы отклонений в области высоких значений интенсивности трафика.

Рис. 6 — Показатели сетевого трафика при моделировании DDoS-атаки (составлено авторами)

Сравнение полученных результатов показывает, что при последовательной смене режимов функционирования сети наблюдается устойчивый рост количества аномальных точек, увеличение нагрузки на сервер и изменение структуры распределения источников запросов. Если в нормальном режиме источники распределены равномерно, то при DoS-атаке доминирует один основной источник, а при DDoS-атаке активность распределяется между множеством источников.

Полученные результаты подтверждают, что визуализация распределения источников запросов, аномальных точек и серверной нагрузки позволяет эффективно выявлять признаки сетевых атак и отслеживать динамику изменения параметров сети при переходе между различными режимами её функционирования. Использование подобных методов визуального анализа повышает наглядность мониторинга сетевых процессов и способствует своевременному обнаружению потенциальных угроз информационной безопасности.

В ходе выполнения исследования был разработан и реализован метод анализа поведения сетевого трафика при DoS и DDoS-атаках с использованием системы визуализации сетевых аномалий. Предложенный подход основан на сборе и визуальном отображении статистических параметров трафика, включая распределение источников запросов, уровень нагрузки на сервер и области аномальной активности. Проведённое моделирование различных режимов работы сети показало, что при переходе от нормального режима к режимам DoS и DDoS-атак наблюдается увеличение количества аномальных точек, изменение структуры источников запросов и рост нагрузки на сервер до критических значений, что позволяет своевременно выявлять признаки атакующего воздействия.

Практическая значимость разработанного решения заключается в возможности его применения в системах мониторинга информационной безопасности, учебных и исследовательских проектах. В качестве направлений

дальнейшего развития рассматриваются внедрение алгоритмов автоматического обнаружения сетевых атак, расширение средств визуализации сетевых параметров и интеграция разработанной системы с существующими инструментами мониторинга сетевой инфраструктуры.

Библиографический список:

1. Баранов, В.В. Компьютерные сети и телекоммуникации : учебник / В.В. Баранов. - Москва : Академия. - 2020. — 352 с.
2. Бевингтон, Р. Защита от сетевых атак и DDoS-угроз / Р. Бевингтон ; пер. с англ.-Москва : ДМК Пресс. - 2020. — 320 с.
3. Кулябов, Д.С. Основы информационной безопасности : учебник / Д.С. Кулябов. -Москва : Академия. - 2019. — 256 с.
4. Лапонина, О.Р. Анализ сетевого трафика и обнаружение вторжений / О.Р. Лапонина. -Москва : ДМК Пресс. - 2021. — 368 с.
5. Назарио, Х. DDoS-атаки и методы защиты от них / Х. Назарио ; пер. с англ. - Москва : ДМК Пресс. - 2018. — 280 с.
6. Назаров, А.Н. Сетевые технологии и протоколы передачи данных : учебное пособие / А.Н. Назаров. -Москва : Юрайт. - 2022. — 300 с.
7. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. -Санкт-Петербург : Питер. - 2021. — 992 с.
8. Официальная документация PostgreSQL [Электронный ресурс]. — Режим доступа: https://www.postgresql.org/docs/ (дата обращения: 24.06.2026).
9. Официальная документация Python [Электронный ресурс]. — Режим доступа: https://docs.python.org/ (дата обращения: 24.06.2026).
10. Смирнов, А. А. Методы обнаружения сетевых атак : учебное пособие / А.А. Смирнов. -Москва : Горячая линия – Телеком. - 2018. — 280 с.
11. Столлингс, У. Криптография и защита сетей : принципы и практика / У. Столлингс ; пер. с англ. -Москва : Вильямс. - 2019. — 768 с.

12. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. - Москва : ФОРУМ. - 2020. — 416 с.