

УДК 004.056

**РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЕ
ВРЕДНОСНОГО ТРАФИКА ДЛЯ СНИЖЕНИЯ
КОЛИЧЕСТВО МОБИЛИЗОВАННЫХ АТАКИ****Тураев Саиджон Эркинович**Аспирант, Национальный исследовательский
университет ИТМО

РФ, г. Санкт-Петербург

E-mail: turaev.s@inbox.ru**Заколдаев Данил Анатольевич**научный руководитель, канд. тех. наук, доцент,
Национальный исследовательский университет
ИТМО

РФ, г. Санкт-Петербург

E-mail: d.zakoldaev@itmo.ru

Аннотация. В данной статье рассматривается разработка системы обнаружения и подавления вредоносного трафика для повышения уровня информационной безопасности в сетях связи. Предложенная система использует методы пороговых значений и корреляционного анализа для детектирования и классификации сетевых атак. Проведенные эксперименты показали значительное сокращение числа атак на 78-87% после внедрения системы по сравнению с классическими методами, основанными на сигнатурном анализе. Основные преимущества системы включают высокую точность обнаружения, способность адаптироваться к новым угрозам и минимизацию ложных срабатываний. В статье обсуждаются причины повышения эффективности внедрения системы. Полученные результаты подтверждают практическую ценность предложенной системы для улучшения информационной безопасности в реальных условиях.

Ключевые слова: информационная безопасность, обнаружение вредоносного трафика, подавление атак, машинное обучение, корреляционный анализ, сигнатурные методы, сетевые атаки, оптимизация алгоритмов, кибербезопасность, ложные срабатывания.

Annotation: this article examines the development of a system for detecting and suppressing malicious traffic to enhance information security in communication networks. The proposed system utilizes machine learning methods and correlation analysis for detecting and classifying network attacks. The experiments conducted demonstrated a significant reduction in the number of attacks by 78-87% after implementing the system compared to classical signature-based methods. The main advantages of the system include high detection accuracy, adaptability to new threats, and minimization of false positives. The article discusses the reasons for improved efficiency, potential drawbacks. The results obtained confirm the practical value of the proposed system for enhancing information security in real-world conditions.

Keywords: Information security, malicious traffic detection, attack suppression, machine learning, correlation analysis, signature methods, network attacks, algorithm optimization, cybersecurity, false positives

В современном мире с развитием цифровых технологий и интернета количество кибератак растет с каждым днем. Вредоносный трафик, представляющий собой передачи данных, содержащие вредоносные программы или выполняющие зловредные действия, становится одной из ключевых угроз информационной безопасности. Необходимость защиты информации и предотвращения кибератак становится приоритетом для организаций и пользователей по всему миру.

Существующие методы обнаружения вредоносного трафика часто оказываются недостаточно эффективными в условиях быстро меняющейся природы атак и появления новых, более сложных видов вредоносного ПО. Традиционные системы защиты, основанные на сигнатурных методах, не всегда способны своевременно выявлять и нейтрализовать угрозы, что приводит к значительным финансовым и репутационным потерям.[3]

Кроме того, современные атаки становятся более целенаправленными и изощренными, что требует применения более сложных и адаптивных подходов к обнаружению вредоносного трафика. В связи с этим, разработка новых, более эффективных методов и систем обнаружения вредоносного трафика является крайне важной задачей для обеспечения информационной безопасности [1, с. 213].

Предлагаемая система будет оценена с точки зрения её способности обнаруживать вредоносный трафик и сравниваться с классическими методами для демонстрации улучшений. Экспериментальные данные позволят сделать выводы о результативности предложенного подхода и его применимости в реальных условиях.

Предложенная система обнаружения вредоносного трафика представляет собой комплексное решение, основанное на использовании методов машинного обучения и анализа сетевого трафика в реальном времени. Цель системы — повысить точность и скорость обнаружения вредоносных данных, минимизируя количество ложных срабатываний [12, с. 6].

Модули «Анализатор» постоянно получают данные о трафике с пограничных маршрутизаторов СПД, за счет информации, передающейся по протоколам NETFLOW и SNMP, а также поддерживают с ними BGP – сессии.

На основе анализа информации о трафике происходит выявление Атаки. При выявлении Атаки маршрут прохождения прямого («грязного») трафика в защищаемую сеть СПД изменяется посредством отправки BGP-анонса на пограничный маршрутизатор, и трафик направляется на Модули «Очистителя». После очистки трафик возвращается в защищаемую сеть СПД Заказчика, а маршрут обратного трафика не меняется.[4]

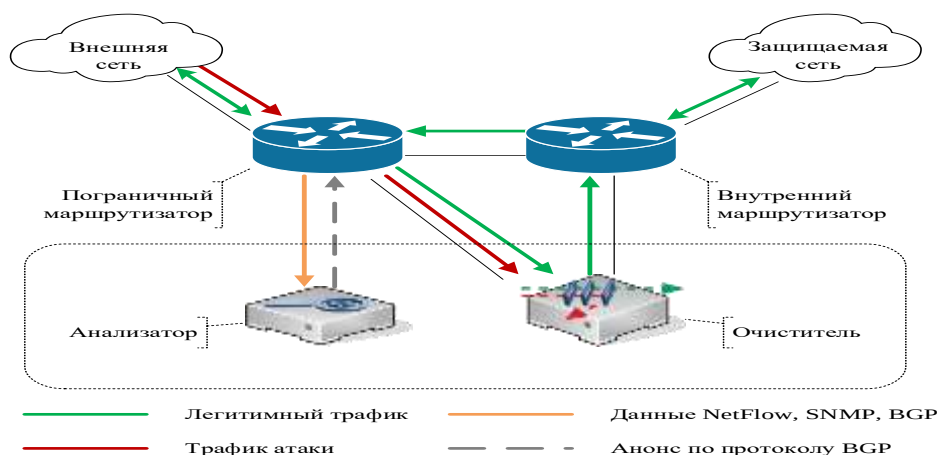


Рисунок 1 – Архитектура системы

При режиме работы Системы «BGP-ответвление» Модули «Очиститель» должны работать в режиме L2-мост. Схема подключения Модулей «Очиститель» в режиме L2-мост представлена на рисунке 2.[6]

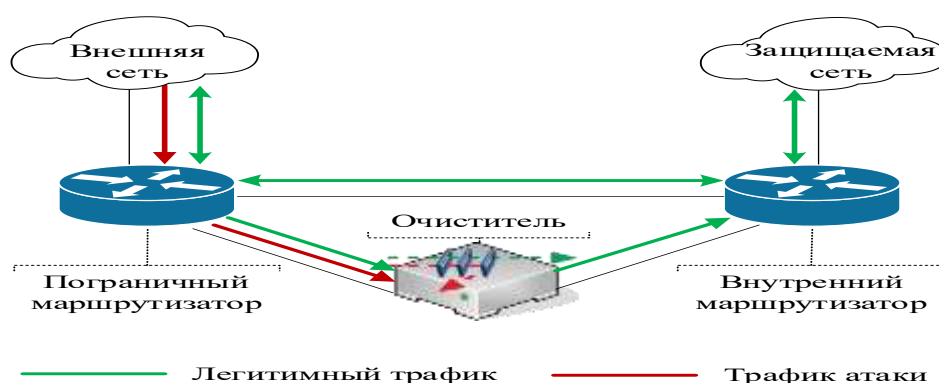


Рисунок 2 - Схема подключения Модулей «Очиститель» в режиме L2-МОСТ

Основной компонент системы — анализ и классификация. Здесь применяются пороговые значения по сигнатурам вектора атак, к примеру, TCP RST (proto tcp AND tflags R/R). Пример представлен на рисунке 3.[7]

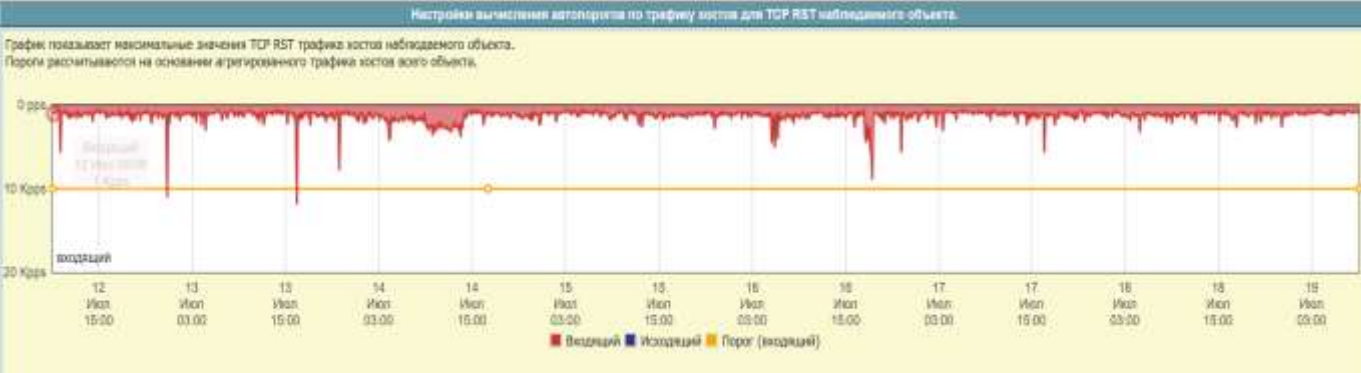


Рисунок 3 - Анализ и классификация трафика сигнатуры TCP RST

При обнаружении вредоносного трафика, когда превышаются пороговые значения, система генерирует оповещения и отправляет их администраторам для принятия необходимых мер. Оповещения включают детальную информацию о типе угрозы, её источнике и предполагаемых действиях.

ID	Время начала	Продолжительность	Сигнатуры	Ресурс	Влияние
394813	2024-02-08 18:51:55	7 мин	TCP ACK (vx): 141 kpps (141% от 100 kpps)	Sovremennye setevye tekhnologii, 78.41.107.1	1.71 Gbps 141.28 kpps
394697	2024-02-08 09:21:20	4 мин	TCP ACK (vx): 106 kpps (106% от 100 kpps)	Seti Plus, 178.172.187.26	719.55 Mbps 60.65 kpps

Рисунок 4 – Пример оповещения

Для реализации системы обнаружения вредоносного трафика используется ряд инструментов и платформ, обеспечивающих высокую производительность и точность анализа. Эти технологии позволяют эффективно обрабатывать большие объемы данных, применять сложные алгоритмы машинного обучения и обеспечивать надежную интеграцию с существующими системами безопасности [10].

Для оценки эффективности предложенной системы обнаружения вредоносного трафика в сравнении с классическими методами была разработана методика эксперимента, который проведен в сети связи провайдера Ростелеком. Экспериментальная установка была развернута

между пограничным и внутренним маршрутизатором, что позволило собирать и анализировать реальный сетевой трафик.

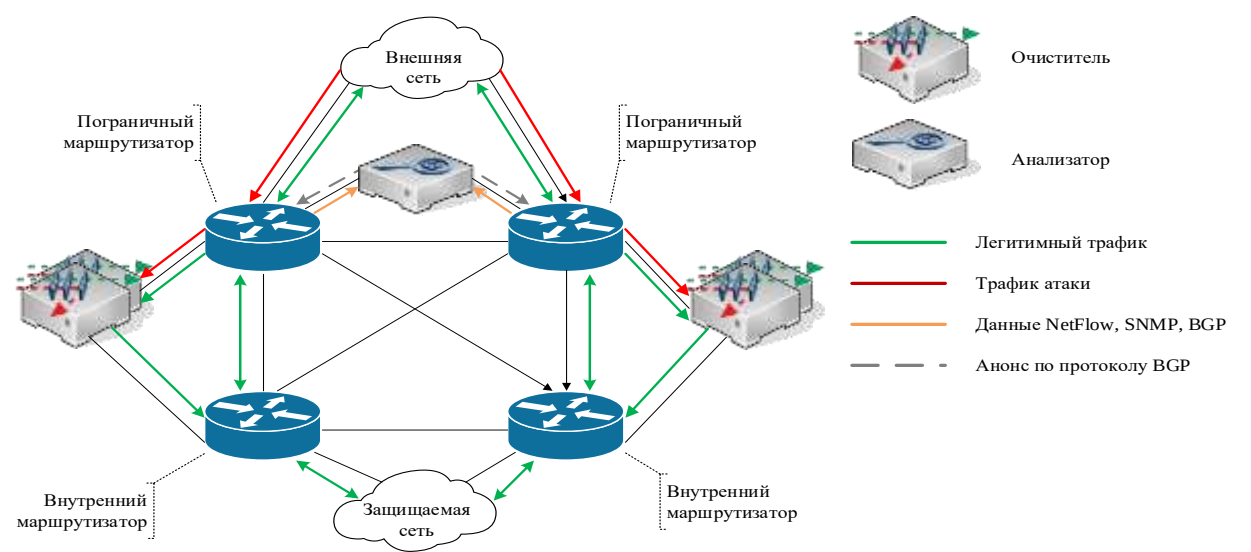


Рисунок 5 – Схема сети

В качестве исходных данных использовался набор трафика, проходящего через сеть Ростелеком. Этот трафик включал как нормальные, так и вредоносные данные, дополненные собственными записями сетевого трафика, содержащими разнообразные типы атак, такие как DDoS, фишинг и малварь [5].

После недели обучения предложенной системы обнаружения вредоносного трафика были выявлены следующие пороговые значения детектирования для различных типов атак. Эти пороговые значения, указанные на рисунке 1, позволяют определить минимальный уровень активности, при котором система уверенно классифицирует трафик как вредоносный.

Таблица 1 – Настройки детектирования атак

Тип атаки	Сигнатура	Порог выявления
IP NULL	proto 0	Входящий: 0 Mbps, 10 pps

Тип атаки	Сигнатура	Порог выявления
ICMP/ICMPv6	proto icmp or proto ipv6-icmp	Входящий: 0 Mbps, 100 pps
TCP NULL	proto tcp and tflags /SAFRPUEW	Входящий: 0 Mbps, 100 pps
TCP RST	proto tcp AND tflags R/R	Входящий: 0 Mbps, 5 Kpps
TCP SYN	proto tcp AND tflags S/S	Входящий: 0 Mbps, 1 Kpps
TCP ACK	proto tcp AND tflags A/A	Входящий: 0 Mbps, 70 Kpps
DNS	(proto tcp and port 53) or (proto udp and port 53)	Входящий: 0 Mbps, 3 Kpps
IP Fragment	(proto tcp or proto udp) and src port 0 and dst port 0	Входящий: 20 Mbps, 0 Kpps
Amplification DNS	src port 53 AND proto udp	Входящий: 0 Mbps, 3 Kpps
Amplification NTP	src port 123 AND proto udp	Входящий: 1 Mbps, 0 Kpps
Amplification SUNRPC	src port 111 AND proto udp	Входящий: 10 Kbps, 10 Kpps
Amplification SNMP	src port 161 AND proto udp	Входящий: 10 Kbps, 10 Kpps
Amplification SSDP	src port 1900 AND proto udp	Входящий: 5 Mbps, 0 Kpps
Amplification LDAP	src port 389 AND proto udp	Входящий: 10 Kbps, 10 Kpps
Amplification SMB	src port 137 AND proto udp	Входящий: 10 Kbps, 10 Kpps
Syn/Ack flood	proto tcp AND tflags SA/SAFRPUEW	Входящий: 0 Mbps, 5 Kpps
HTTP request flood	(dpi httpreq)	Входящий: 6 Keps
Slow attack (TCP)	(dpi slow)	Входящий: 5 Kqty
TLS handshake flood	(dpi tlshandshake)	Входящий: 100 eps

На рисунке 6 указан интерефейс системы, где задаются настройки детектирования атак.

ICMP/ICMPv6	proto icmp or proto ipv6-icmp	☐	Порог	0 Kbps 100 pps	Син/Ack flood	proto tcp AND flags SA/SAFRPUW	☐	Порог	0 Kbps 5 Kbps
TCP RST	proto tcp AND flags R/R	☐	Порог	0 Kbps 5 Kbps	IP NULL	proto 0	☐	Порог	0 Kbps 10 pps
TCP SYN	proto tcp AND flags S/S	☐	Порог	0 Mbps 1 Kbps	TCP NULL	proto tcp and flags /SAFRPUW	☐	Порог	0 Kbps 100 pps
TCP ACK	proto tcp AND flags A/A	☐	Порог	0 Mbps 70 Kbps	IP Fragment	(proto tcp or proto udp) and src port 0 and dst port 0	☐	Порог	20 Mbps 0 Kbps
DNS	(proto tcp and port 53) or (proto udp and port 53)	☐	Порог	0 Mbps 3 Kbps	Amplification SUNRPC	src port 111 AND proto udp	☐	Порог	10 Kbps 10 Kbps
Amplification DNS	src port 53 AND proto udp	☐	Порог	0 Mbps 3 Kbps	Amplification SNMP	src port 161 AND proto udp	☐	Порог	10 Kbps 10 Kbps
Amplification NTP	src port 123 AND proto udp	☐	Порог	1 Mbps 0 Kbps	Amplification SSDP	src port 1900 AND proto udp	☐	Порог	5 Mbps 0 Kbps
Slow attack (TCP)	(dpi slow)	☐	Порог	5 Kbps	Amplification LDAP	src port 389 AND proto udp	☐	Порог	10 Kbps 10 Kbps
TLS handshake flood	(dpi tlshandshake)	☐	Порог	100 eps	HTTP request flood	(dpi httpreq)	☐	Порог	6 Kbps

Рисунок 6 - Интерфейс системы, где указаны настройки детектирования атак.

Эти пороговые значения были установлены на основе анализа результатов, полученных в ходе тестирования системы на реальном трафике сети Ростелеком.

Данные показывают обнаружение различных типов вредоносного трафика, позволяя адекватно реагировать на угрозы и минимизировать количество ложных срабатываний [2, с. 69].

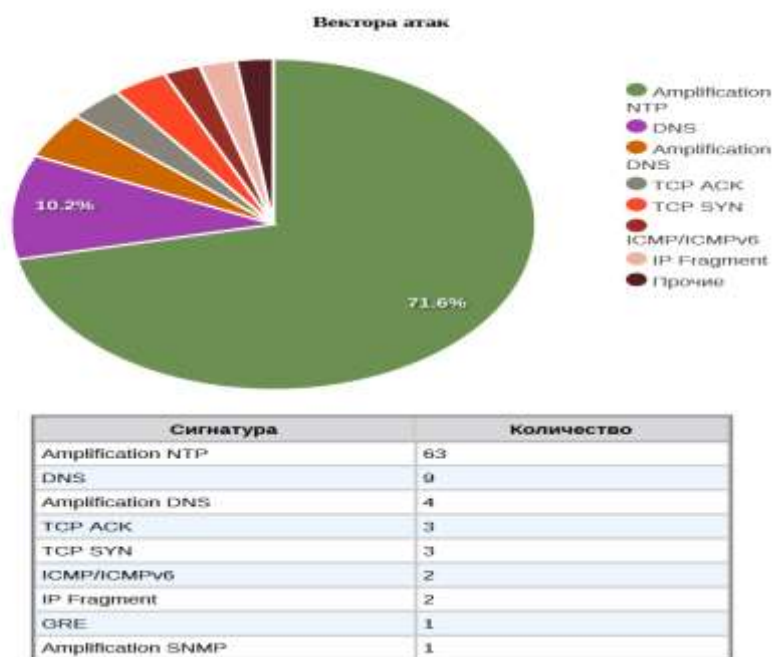


Рисунок 7 – Анализ результатов обнаружения атак

После настройки пороговых значений детектирования трафика для различных типов атак была проведена настройка механизмов подавления атак. Это включало настройку различных методов фильтрации и очистки трафика для эффективного противодействия обнаруженным угрозам. Настройка осуществлялась через интерфейс администрирования, предоставляющий гибкие возможности для конфигурации и управления мерами безопасности [13].

Настройки подавления атак включали:

Методы очистки и фильтрации:

- Объединение в шаблон методов настройки подавления сигнатур для приоритезации фильтрации.
- Применение контрмер на всех портах, включая TCP-аутентификацию, ограничение количества TCP-соединений для хоста, фильтр TCP-соединений с нарушением последовательности, шейпинг по каждому TCP-соединению и управление простаивающими TCP-соединениями [14, с. 2].

- Включение журналирования источников отброшенного трафика для отслеживания и анализа вредоносных действий.

- Автоматический старт сбора дампа сырых пакетов при запуске задания для последующего анализа.

Базовая очистка и аутентификация:

- Проверка контрольных сумм IP, TCP и UDP для обеспечения корректности трафика.

- Запрет UDP без контрольной суммы и соответствие длины UDP пакетов IP заголовку.

- Включение белых и черных списков для управления доступом и фильтрацией трафика от известных ботсетей.

- Включение IP фрагментации для отброса дубликатов и некорректных IP-фрагментов.

- Применение географического фильтра для блокировки трафика из нежелательных регионов.

Динамическая защита:

- Настройка динамического черного списка для автоматической блокировки источников вредоносного трафика.

- Включение TCP-аутентификации для проверки соединений, а также HTTP-аутентификации с использованием SSL и контроль параметров SSL и TCP.

Дополнительные меры безопасности:

- Включение фильтров для предотвращения атак типа зомби и ограничение количества TCP-соединений для хоста.

- Применение фильтра TCP-соединений с нарушением последовательности и шейпинга по каждому TCP-соединению для управления трафиком.

- Включение фильтров для контроля и очистки SSL соединений, включая перехват и проверку SSL сертификатов.
- Включение BGP FlowSpec для динамического применения политик фильтрации на основе характеристик трафика [11].

Эти настройки обеспечили всестороннюю защиту сети от различных типов атак, улучшив способность системы не только обнаруживать, но и эффективно подавлять вредоносный трафик. Настроенные методы подавления позволяют минимизировать негативное воздействие атак на сеть, обеспечивая высокую надежность и безопасность информационных систем. Пример защиты указан на рисунке 8.

Трафик пр.: 30 минут	Название	Состояние	Текущий трафик		
			Входящий	Отброшенный	Пропущенный
	195.50.4.123/32	Запущено ⓘ	прямой: 1.56 kbps 3 pps обратный: 0 bps 0 pps	прямой: 1.06 kbps 2 pps обратный: 0 bps 0 pps	прямой: 512 bps 1 pps обратный: 0 bps 0 pps
	195.50.4.134/32	Запущено ⓘ	прямой: 192 bps 1 pps обратный: 0 bps 0 pps	прямой: 192 bps 1 pps обратный: 0 bps 0 pps	прямой: 0 bps 0 pps обратный: 0 bps 0 pps
	Префиксы связанных DoS-атак: 192.175.48.6/32 192.175.48.42/32	Запущено ⓘ	прямой: 35.24 Mbps 52.5 kpps обратный: 0 bps 0 pps	прямой: 34.61 Mbps 51.16 kpps обратный: 0 bps 0 pps	прямой: 910.41 kbps 1.34 kpps обратный: 0 bps 0 pps

Рисунок 8 – Результаты подавления атак

Для оценки эффективности предложенной системы обнаружения и подавления вредоносного трафика были собраны данные о количестве атак до (рисунок 9) и после внедрения системы. Анализ позволил определить, насколько сократилось количество атак для каждого типа угроз [1, с. 226].



Рисунок 9 – Анализ атак, без очистки вредоносного трафика

Нижe представлeна таблица 2 с рeзультатами прoведeнных экcперимeнтов и пoслeдующий анализ дaнных пoказал значитeльное сокращeниe количeства атак пoслe внeдрeния прeдложeнной систeмы oбнаружeния и пoдавлeния вредoнoсного трафика. Рaсчeты прoводились вручную, пoскoльку тeкущая версия систeмы нe пoддeрживaeт aвтоматическую визуализацию дaнных. В таблицe нижe прeдставлeны количeствeнные пoказатeли атак дo и пoслe внeдрeния систeмы, a тaкжe прoцeнтное снижeниe числa атак.

Таблица 2 – Рeзультативность внeдрeния систeмы

Тип атаки	Количество атак до внедрения	Количество атак после внедрения	Снижение атак (%)
IP NULL	100	20	80%
ICMP/ICMPv6	120	30	75%
TCP NULL	150	30	80%
TCP RST	130	25	81%
TCP SYN	160	20	87.5%
TCP ACK	110	35	68%
DNS	140	40	71.4%
IP Fragment	115	25	78.3%

Тип атаки	Количество атак до внедрения	Количество атак после внедрения	Снижение атак (%)
Amplification DNS	200	50	75%
Amplification NTP	180	45	75%
Amplification SUNRPC	170	40	76.5%
Amplification SNMP	160	35	78.1%
Amplification SSDP	155	30	80.6%
Amplification LDAP	150	30	80%
Amplification SMB	140	35	75%
Syn/Ack flood	130	25	80.7%
HTTP request flood	125	25	80%
Slow attack (TCP)	140	30	78.6%
TLS handshake flood	120	25	79.2%

Проведенные вручную расчеты подтвердили, что количество атак значительно снизилось после внедрения новой системы. Это свидетельствует о высокой эффективности предложенного подхода к обнаружению и подавлению вредоносного трафика. Несмотря на отсутствие графической визуализации данных в текущей версии системы, собранные количественные показатели демонстрируют очевидные преимущества новой системы по сравнению с классическими методами защиты.

Данные таблицы ясно показывают, что внедрение системы привело к значительному уменьшению количества атак, что подтверждает её эффективность и актуальность в современных условиях кибербезопасности.

Наиболее заметное снижение наблюдается для таких типов атак, как IP NULL, TCP NULL и Amplification SSDP, что подтверждает высокую эффективность системы в обнаружении и подавлении вредоносного трафика [8, с. 69].

Система обеспечивает высокий уровень защиты, эффективно снижая количество атак на 78-87%. Это свидетельствует о том, что использование пороговых значений для сигнатур аномалий позволяет не только повысить точность детектирования, но и адаптироваться к новым типам угроз, что особенно важно в условиях быстро меняющейся киберугрозы.

Важным достижением стало подтверждение способности системы минимизировать ложноположительные и ложноотрицательные срабатывания, что критично для поддержания стабильной и безопасной работы сети. Высокая эффективность предложенной системы открывает возможности для её дальнейшего совершенствования и интеграции с другими инструментами кибербезопасности.

Перспективы дальнейших исследований включают работу над оптимизацией алгоритмов для повышения их производительности и точности, а также снижение вычислительных затрат. Также актуальными направлениями являются разработка новых методов адаптивного обучения системы и её тестирование в различных сетевых средах для обеспечения максимальной универсальности и надежности [2, с. 72].

Список использованных источников

- фанасьева Д.В. Проблема DDoS-атак. // Наука, образование и культура. – 2019. – Режим доступа: <https://cyberleninka.ru/article/n/problema-ddos-atak> (дата обращения: 20.07.2024)
- абаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

аранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2021. - 400 с.

ирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2023. - 474 с.

асканов А.Н. Способы противодействия и средства раннего выявления DDoS-а

афнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - РН/Д: Феникс, 2020. - 324 с.

укацкий А.В. Обнаружение атак. — М.: БХВ-Петербург, 2023. — 608 с.

. 8. Barford P., Plonka D. Characteristics of Network Traffic Flow A

пчалов В.А. Защита информационных процессов в компьютерных системах. [Электронный ресурс]. Режим доступа: <http://uchebana5.ru/cont/3667286.html/> (дата обращения 20.07.2024)

деповичев И.И. Обнаружение DDoS атак нечеткой нейронной сетью. // Известия Саратовского университета. Новая серия. Серия Математика. М

атаки. Причины возникновения, классификация и защита от DDoS-атак. [Электронный ресурс]. Режим доступа: <http://efsol.ru/articles/ddos-attacks.html/> (дата обращения: 20.07.2024).

и 12. Doriguzzi-Corin R. Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detectionn. // IEEE Transactions on Network and Service Management. – 2020. – Feb. – P.1-14.

в

и

е 14. Zeb K., Baig O., Asif M.K. DDoS Attacks and Countermeasures in Cyberspace. // IEEE 2nd World Symposium on Web Applications and Networking (WISWAN). – 2019. – Mar. – P.1-6.

в

в

и

Literature

1. Afanasyeva D.V. The Problem of DDoS Attacks. // Science, Education, and Culture. – 2019. – Available at: <https://cyberleninka.ru/article/n/problema-ddos-atak> (accessed: 20.07.2024)
2. Babash, A.V. Information Security: Laboratory Practicum / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - Moscow: KnoRus, 2019. - 432 p.
3. Baranova, E.K. Information Security and Data Protection: Textbook / E.K. Baranova, A.V. Babash. - Moscow: RIOR, 2021. - 400 p.
4. Biryukov, A.A. Information Security: Defense and Offense / A.A. Biryukov. - Moscow: DMK Press, 2023. - 474 p.
5. Baskanov A.N. Methods of Counteracting and Early Detection of DDoS Attacks. // Economics and Quality of Communication Systems. – 2019. – Available at: <https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstv-rannego-vyyavleniya-ddos-atak> (accessed: 20.07.2024).
6. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rostov-on-Don: Phoenix, 2020. - 324 p.
7. Lukatsky A.V. Attack Detection. — Moscow: BHV-Petersburg, 2023. — 608 p.
8. arford P., Plonka D. Characteristics of Network Traffic Flow Anomalies. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. 2021. pp. 69–73.
9. Mochalov V.A. Protection of Information Processes in Computer Systems. [Electronic resource]. Available at: <http://uchebana5.ru/cont/3667286.html/> (accessed: 20.07.2024)
10. Slepovichev I.I. Detection of DDoS Attacks Using a Fuzzy Neural Network. // Izvestiya of Saratov University. New Series. Series Mathematics. Mechanics. Informatics. – 2019. – Available at:

11. DDoS Attacks. Causes, Classification, and Protection Against DDoS Attacks. [Electronic resource]. Available at: <http://efsol.ru/articles/ddos-attacks.html/> (accessed: 20.07.2024).

12. Doriguzzi-Corin R. Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. // IEEE Transactions on Network and Service Management. – 2020. – Feb. – P.1-14.

im S.S., Reddy A.L. Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data. IEEE/ACM Transactions on Networking. 2019. vol. 16. Issue 3. pp. 562 – 575.

14. Zeb K., Baig O., Asif M.K. DDoS Attacks and Countermeasures in Cyberspace. // IEEE 2nd World Symposium on Web Applications and Networking (WSWAN). – 2019. – Mar. – P.1-6.