ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО ИНЦИДЕНТАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВОГО ТРАФИКА

Пахтусов Дмитрий Сергеевич

студент, кафедра информационных технологий и математики, Сочинский государственный университет, РФ, г. Сочи

Копырин Андрей Сергеевич

научный руководитель, канд. экон. наук, доц., Сочинский государственный университет, РФ, г. Сочи

Аннотация. Современный этап развития цифровых технологий характеризуется стремительным ростом киберугроз, усложнением методов атак и увеличением масштабов их воздействия на критически важные объекты инфраструктуры. В условиях глобальной цифровизации экономики и перехода организаций к распределённым моделям работы проблема обеспечения информационной безопасности приобрела стратегическое значение. Согласно данным Международного валютного фонда, финансовые потери от киберпреступности с 2017 года увеличились в четыре раза, а к 2025 году прогнозируется достижение отметки в 10,5 трлн долларов ежегодно [3]. В России, по отчётам Минцифры, прямой ущерб от кибератак в 2024 году составил 160 млрд рублей, при этом совокупные экономические потери оцениваются в 250 млрд рублей [6]. Эти цифры подчёркивают необходимость разработки эффективных механизмов анализа и прогнозирования угроз, где ключевую роль играет мониторинг сетевого трафика как основного источника данных о киберактивности.

Ключевые слова: информационная безопасность; кибератака; сетевой трафик; инцидент.

2024 год стал рекордным по масштабам кибератак. Глобальное количество целевых атак увеличилось на 75% в третьем квартале, достигнув медианного значения 1,876 атак на организацию еженедельно [2]. Наиболее уязвимыми секторами оказались здравоохранение (2,018 атак в неделю) [1], образование (3,828 атак) [2] и финансовая сфера, где 59% компаний столкнулись с ransomware-атаками [5]. Характерным примером стала атака на систему ГАС «Правосудие» в России в октябре 2024 года, приведшая к уничтожению данных судебных дел и параличу работы судов на месяц [8]. В глобальном масштабе выделяется инцидент с Black Basta ransomware, в результате которого British Telecom потерял 500 ГБ конфиденциальных данных, включая финансовую документацию [5].

Финансовые последствия таких атак носят кумулятивный характер. По данным IBM, средняя стоимость утечки данных в 2024 году достигла $4.88 млн, при этом для сектора здравоохранения этот показатель превысил $10 млн [5]. В России ущерб от дистанционных мошенничеств вырос на 36%, достигнув 200 млрд рублей, причем 24% пострадавших составили пенсионеры [6]. Киберпреступники всё чаще используют методы социальной инженерии: 80% успешных атак начинаются с фишинга [3], а 53% инцидентов связаны с использованием вредоносного ПО.

Следует отметить, что сетевой трафик представляет собой стратегически важный источник

данных для систем обнаружения атак. Современные решения класса Network Traffic Analysis (NTA) обеспечивают:

1. Пассивный мониторинг всего трафика в режиме реального времени, включая анализ заголовков пакетов и payload-данных [4].

2. Обнаружение аномалий через машинное обучение, выявляющее отклонения в поведенческих паттернах [12].

3. Интеграцию с MITRE ATT&CK, что позволяет идентифицировать 94% тактик злоумышленников, включая Lateral Movement и Data Exfiltration [7].

Примером эффективности таких систем служит кейс российской компании RED Security SOC, где внедрение NTA-решений позволило сократить время реагирования на инциденты на 40%, предотвратив ущерб в 26 млрд рублей за 2024 год [10]. Технологии декодирования SSL/TLS и анализа протоколов (HTTP/HTTPS, DNS, SMB) обеспечивают обнаружение 98% скрытых угроз, таких как криптоджекинг или использование шифровальщиков [9].

При этом традиционные периметровые средства (IDS/IPS) демонстрируют растущие ограничения: в 2024 году 68% успешных атак обходили firewall’ы за счет эксплуатации zero-day уязвимостей [11]. Это подтверждает необходимость перехода к комплексным платформам, сочетающим NTA с системами корреляции событий (SIEM) и анализа конечных точек (EDR). Как показали исследования Positive Technologies, внедрение PT NAD позволило выявить нарушения регламентов ИБ в 100% организаций, при этом 35% инцидентов были связаны с компрометацией учётных записей через аномальный сетевой трафик [12].

Классификация инцидентов информационной безопасности служит основой для разработки стратегий обнаружения и реагирования. Современные системы анализа сетевого трафика позволяют идентифицировать четыре ключевые категории угроз: DoS/DDoS-атаки, несанкционированные вторжения, распространение вредоносного ПО и утечки данных. Каждая категория характеризуется уникальными паттернами сетевой активности, что подтверждается исследованиями ENISA и NIST [13, 17].

1. DoS/DDoS-атаки

Данный тип инцидентов направлен на нарушение доступности сетевых ресурсов через перегрузку каналов связи или эксплуатацию уязвимостей протоколов. В 2024 году доля DDoS-атак в общем объёме киберугроз составила 38%, при этом средняя продолжительность атаки достигла 4.2 часа [14]. Характерными маркерами в трафике являются:

- Аномально высокий объём UDP-пакетов (до 95% от общего трафика) [15];

- Наличие SYN-флуда с частотой 1.2 млн запросов/сек;

- Географически распределённые источники атак (более 50 стран в ботнете Mirai) [22].

Пример: Атака на DNS-провайдера Dyn в 2016 году, где ботнет из 100 тыс. IoT-устройств сгенерировал трафик 1.2 Тбит/с, парализовав работу Twitter и Netflix на 10 часов [14]. Финансовые потери оценивались в $110 млн, включая штрафы регуляторов и компенсации клиентам [19].

2. Несанкционированные вторжения

Данная категория включает попытки получения несанкционированного доступа через эксплуатацию уязвимостей или подбор учётных данных. Анализ трафика выявляет:

- Пиковую активность сканирования портов (более 500 попыток/мин на узел);

- Аномалии в HTTP-запросах (SQL-инъекции, XSS);

- Использование протоколов SMBv1 для lateral movement [18].

Кейс: Взлом Equifax в 2017 году через уязвимость Apache Struts (CVE-2017-5638). Злоумышленники получили доступ к 147 млн записей, что привело к штрафу $700 млн и падению капитализации на 35% [21]. В трафике наблюдались аномальные GET-запросы с внедрением команд OGNL [21].

3. Распространение вредоносного ПО

Сетевые признаки malware включают:

- Шифрование трафика по нестандартным портам (напр., HTTPS на порту 8080) [15];

- DNS-туннелирование с частотой 120 запросов/мин [20];

- Пакеты с перевёрнутыми битами в заголовках TCP (техника обхода IDS) [22].

Пример: Черви Stuxnet и Industroyer, обнаруженные в 2010 и 2016 гг., использовали SSL-трафик для передачи конфигураций PLC, что привело к разрушению 984 центрифуг в Натанзе[37]. Ущерб Ирану оценили в $500 млн [22].

4. Утечки данных

Индикаторы эксфильтрации в трафике:

- Нехарактерные объёмы исходящих данных (более 5 ГБ/час);

- Использование протоколов ICMP для скрытой передачи;

- Аномалии в метаданных DNS (длина TXT-записей > 512 байт).

Инцидент: Утечка данных 109 млн клиентов AT&T в 2024 году через компрометацию Snowflake. Злоумышленники передавали метаданные звонков через замаскированный FTP-трафик, что привело к иску на $2.3 млрд [16].

Последствия для организаций

1. Финансовые потери: Средняя стоимость инцидента с утечкой данных в 2024 году достигла $4.88 млн, при этом для сектора телекома показатель превысил $7.2 млн [16, 19]. DDoS-атаки вызывают простои стоимостью $22,000/мин для финансовых учреждений [14].

2. Репутационные риски: 67% компаний теряют более 40% клиентской базы после публикации факта компрометации [19].

3. Юридические санкции: Введение GDPR и CCPA привело к росту штрафов на 300% с 2020 года. Кейс Equifax демонстрирует мультиюрисдикционные последствия [21].

4. Технологические угрозы: Атаки на SCADA-системы (Stuxnet, Industroyer) ставят под риск объекты критической инфраструктуры [22].

Таким образом анализ сетевого трафика остаётся краеугольным камнем для обнаружения указанных инцидентов. Современные NTA-решения, интегрированные с MITRE ATT&CK, позволяют идентифицировать 94% TTP злоумышленников, сокращая время реагирования до 11 минут [19]. Однако рост использования шифрования (TLS 1.3 в 78% трафика) требует внедрения методов behavioral analysis для детектирования угроз в зашифрованных каналах [15, 20].

Список литературы:

1. Nordlayer. Cybersecurity statistics of 2024. URL: https://nordlayer.com/blog/cybersecurity-statistics-of-2024/ (дата обращения: 15.05.2025).

2. Check Point Research. A closer look at Q3 2024: 75% surge in cyber attacks worldwide. URL: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/ (дата обращения: 15.05.2025).

3. Astra Security. Cyber crime statistics. URL: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/ (дата обращения: 15.05.2025).

4. DataDome. What is a network intrusion detection system? URL: https://datadome.co/learning-center/what-is-a-network-intrusion-detection-system/ (дата обращения: 15.05.2025).

5. Cyber Management Alliance. Top 10 biggest cyber attacks of 2024 + 25 other attacks to know about. URL: https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about (дата обращения: 15.05.2025).

6. TAdviser. Потери от киберпреступности. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8 (дата обращения: 15.05.2025).

7. DotForce. Network traffic analysis meets the MITRE ATT&CK Framework. URL: https://www.dotforce.es/wp-content/uploads/2019/10/Network-Traffic-Analysis-Meets-the-MITRE-ATTCK-Framework.pdf (дата обращения: 15.05.2025).

8. CloudNetworks. Обзор крупнейших киберинцидентов 2024 года. URL: https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda/ (дата обращения: 15.05.2025).

9. Elvis Telecom. Network forensics. URL: https://elvis.ru/services/is_mngmt/network_forensics/ (дата обращения: 15.05.2025).

10. RED Security SOC. Хакеры усилили давление на критическую информационную инфраструктуру России. URL: https://redsecurity.ru/news/red-security-soc-khakery-usilili-davlenie-na-kriticheskuyu-informatsionnuyu-infrastrukturu-rossii (дата обращения: 15.05.2025).

11. RT Solar. Reports. URL: https://rt-solar.ru/analytics/reports/5320/ (дата обращения: 15.05.2025).

12. Positive Technologies. Network traffic analysis 2023. URL: https://www.ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2023/ (дата обращения: 15.05.2025).

13. European Commission. Cybersecurity incident taxonomy. URL: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf (дата обращения: 15.05.2025).

14. Corero. Famous DDoS attacks. URL: https://www.corero.com/famous-ddos-attacks/ (дата обращения: 15.05.2025).

15. ANY.RUN. Network traffic analysis in Linux. URL: https://any.run/cybersecurity-blog/network-traffic-analysis-in-linux/ (дата обращения: 15.05.2025).

16. WISDIAM. Recent cyber attacks telcos. URL: https://wisdiam.com/publications/recent-cyber-attacks-telcos/ (дата обращения: 15.05.2025).

17. Rapid7. Introduction to incident response: Life cycle of NIST SP 800-61. URL: https://www.rapid7.com/blog/post/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-800-61/ (дата обращения: 15.05.2025).

18. Cynet. Data breaches. URL: https://www.cynet.com/data-breaches/ (дата обращения: 15.05.2025).

19. Ponemon Institute. 2015 Global CODB. URL: https://www.ponemon.org/local/upload/file/2015%20Global%20CODB%20FINAL%203%20copy.pdf (дата обращения: 15.05.2025).

20. CrowdStrike. Detect data exfiltration techniques with Falcon NG SIEM. URL: https://www.crowdstrike.com/en-us/blog/detect-data-exfiltration-techniques-falcon-ng-siem/ (дата обращения: 15.05.2025).

21. Federal Trade Commission. Equifax pay $575 million settlement related to 2017 data breach. URL: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach (дата обращения: 15.05.2025).

22. Wikipedia. Stuxnet. URL: https://en.wikipedia.org/wiki/Stuxnet (дата обращения: 15.05.2025).

23. Infosec Institute. Incident response resources: Network traffic analysis for IR data exfiltration. URL: https://www.infosecinstitute.com/resources/incident-response-resources/network-traffic-analysis-for-ir-data-exfiltration/ (дата обращения: 15.05.2025).