

УДК 004.056.5

В. С. БАРАНОВ, Е. В. МАЛАШЕНКО, В. А. МОИСЕЕНКО (ЭМ-31)
Научный руководитель – канд. физ.-мат. наук *Е. А. ЗАДОРОВНИК*

ПРИНЦИПЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ

Рассмотрена задача выявления нетипичных событий в компьютерных сетях. Проанализированы три категории методов: статистические, сигнатурные и поведенческие. Установлены их сильные и слабые стороны, сформулированы критерии выбора подхода в зависимости от условий эксплуатации сети, обоснована перспективность гибридных решений для практического применения.

По мере роста интенсивности обмена данными инфраструктура передачи информации превращается в первоочередную мишень для деструктивных воздействий. Принципиальным отличием защиты сети от смежных проблем безопасности является необходимость работы в условиях непрерывного потока данных и жестких временных ограничений. Под сетевой аномалией понимается устойчивое отступление наблюдаемых характеристик трафика от базовой линии, указывающее на несанкционированное вмешательство, нештатную ситуацию или отказ узла [1].

Исследования в данной области развиваются по нескольким направлениям. Некоторые авторы сосредоточились на разработке легких моделей, допускающих работу на маршрутизаторах с ограниченными ресурсами [2]. Другое направление связано с применением глубоких нейронных архитектур, позволяющих учитывать долгосрочные временные зависимости в трафике [3]. Вместе с тем проблема совмещения высокой чувствительности детектора с низкой долей ложных тревог остается нерешенной. Настоящая работа ставит целью систематизировать накопленный опыт и провести сравнение ключевых подходов по единым критериям.

Логика обнаружения аномалий определяет принадлежность метода к одной из трех групп: статистической, сигнатурной или поведенческой.

Статистический подход опирается на предположение о стационарности нормального трафика. Для каждого контролируемого показателя формируется базовый профиль, отклонение от которого сверх заданного порога квалифицируется как аномалия. Наиболее распространен метод накопленных сумм (CUSUM). Он реагирует даже на плавный дрейф метрики, недоступный обычным пороговым правилам [1]. Достоинством этого подхода является вычислительная экономичность, а недостатком – неустойчивость к нестационарным условиям. На рисунке 1 показан характерный пример резкого роста трафика при DDoS-воздействии на фоне типичного суточного профиля сети.

Сигнатурные системы обнаружения вторжений (IDS) работают иначе.

Каждый пакет или сессия сопоставляется с каталогом заранее описанных угроз. Высокая точность при известных атаках сочетается с принципиальной неспособностью реагировать на угрозы, отсутствующие в базе данных [2].

Выбросы трафика (Traffic Spikes)

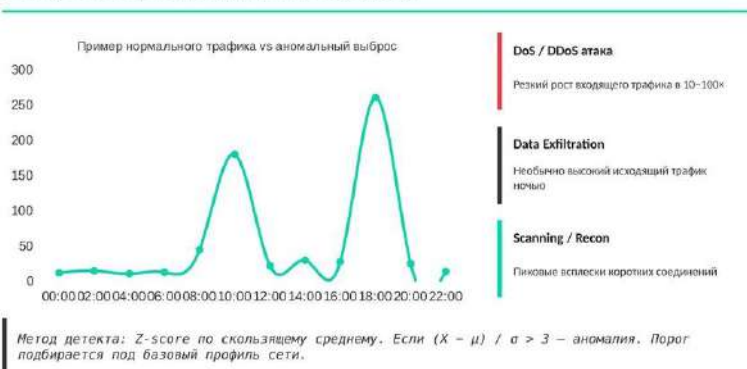


Рисунок 1 – Суточный профиль трафика

Особую сложность представляют скрытые каналы, маскирующиеся под легитимные протоколы в частности DNS-туннелирование, схема которого приведена на рисунке 2.

DNS-туннели

DNS используется как скрытый транспорт для обхода межсетевых экранов — данные кодируются в субдоменах запросов.



Практический пример детекта (без сигнатур):

DNS-запрос к субдомену длиной > 60 байт → подмена XXX.attacker.com → детект как туннель

Правило: `len(query_name) > 60 AND entropy(subdomain) > 3.5 AND NOT is_cdn(domain)`

Признаки DNS-туннеля:

- Необычно длинные имена хостов (>60 байт)
- Высокая энтропия субдомена (base64/hex)
- Большой объем TXT/NULL/CNAME записей
- Высокая частота запросов к одному домену
- Редко встречающиеся домены (молодые домены)

Инструменты: Zeek dns.log + JA3, nfdump, RITA

`zeek -r capture.pcap policy/protocols/dns
nfdump -f 'proto udp and dst port 53' -s dstip/100`

Рисунок 2 – Принцип организации DNS-туннеля как скрытого канала утечки данных

Поведенческие методы формируют модель нормального поведения непосредственно из исторических данных без явного описания угроз. Это качество делает их применимыми к атакам нулевого дня. Среди активно используемых алгоритмов выделяются:

- метод опорных векторов (SVM), обеспечивающий устойчивую клас-

сификацию в пространстве высокой размерности;

- рекуррентные сети LSTM, моделирующие зависимости внутри временных рядов трафика;

- ансамблевые методы, в том числе Isolation Forest, эффективно выделяющий точки-выбросы без явного обучения на аномалиях [3].

Сопоставление подходов по ключевым критериям приведено в таблице 1.

Таблица 1 – Сравнительные характеристики методов обнаружения аномалий

Метод	Точность	Быстродействие	Новые угрозы
Статистические	Средняя	Высокое	Нет
Сигнатурные	Высокая	Высокое	Нет
Интеллектуальные	Высокая	Среднее	Да

Данные таблицы 1 показывают, что ни один из подходов не является универсальным. Статистические методы уместны там, где ресурс обработки ограничен, а угрозы носят количественный характер. Сигнатурные решения целесообразно применять в сегментах с хорошо изученным профилем угроз. Поведенческие методы наиболее предпочтительны в динамичных средах, где перечень возможных атак заранее неизвестен. Гибридная архитектура, объединяющая быстрое статистическое предфильтрование с глубокой нейросетевой классификацией подозрительных сессий, позволяет сбалансировать перечисленные противоречия.

На основании исследования можно сделать следующие выводы. Задача обнаружения сетевых аномалий не имеет единственного оптимального решения. Выбор метода обусловлен характеристиками конкретной инфраструктуры и ожидаемыми классами угроз. Наиболее перспективными являются гибридные системы, способные совмещать скоростное статистическое профилирование трафика с адаптивными моделями машинного обучения. Практическое внедрение таких систем создает предпосылки для своевременного выявления как известных, так и ранее не наблюдававшихся атак, что существенно повышает защищенность сетевой инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1 Шелухин, О. И. Обнаружение аномалий в сетевом трафике на основе теории фракталов и хаоса / О. И. Шелухин, А. В. Осин, С. Б. Смольский. – М. : Горячая линия-Телеком, 2016. – 392 с.

2 Лукацкий, А. В. Обнаружение атак / А. В. Лукацкий. – СПб. : БХВ-Петербург, 2001. – 624 с.

3 Chalapathy, R. Deep Learning for Anomaly Detection: A Survey / R. Chalapathy, S. Chawla // arXiv preprint. – 2019. – URL: <https://arxiv.org/abs/1901.03407> (date of access: 10.04.2026)

Получено 11.06.2026