

*МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

УДК 004

DOI: 10.17212/2782-2230-2026-3-9-23

**КОМБИНИРОВАННЫЙ АНАЛИЗ ТСП-АКТИВНОСТИ
ДЛЯ ОБНАРУЖЕНИЯ СКРЫТЫХ И РАСПРЕДЕЛЕННЫХ
СКАНИРОВАНИЙ ПОРТОВ***

Д.С. КУЗЛЯКИН¹, И.А. ОГНЕВ²

¹ РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: kuzlyakin.2022@corp.nstu.ru

² РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: i.ognev@corp.nstu.ru

В статье рассматриваются методы анализа ТСП-активности, предназначенные для обнаружения медленных и распределенных форм сканирования портов, недостаточно эффективно выявляемых традиционными сигнатурными системами. Предложен комбинированный подход, включающий эвристический анализ ТСП-флагов, статистическую оценку интенсивности и энтропии сетевого трафика, графовый анализ взаимодействий между узлами, а также использование структуры Count-Min Sketch для компактного хранения статистики. Представлена методика вычисления интегральной оценки подозрительности (score) на основе совокупности признаков. Экспериментально показано, что предложенные методы обеспечивают точность обнаружения медленного сканирования с интервалом 10 с на уровне 69,5 %, а распределенного сканирования от 20 источников – 73,8 %, что на 17...27 % выше, чем у классических сигнатурных IDS. При этом использование Count-Min Sketch позволяет сократить потребление оперативной памяти на 32...37 % по сравнению с полным хранением статистики портов.

Ключевые слова: ТСП-сканирование, обнаружение аномалий, эвристический анализ, статистический анализ, графовый анализ, Count-Min Sketch, медленное сканирование, распределенное сканирование

ВВЕДЕНИЕ

Сканирование портов является первым и обязательным этапом большинства сетевых атак. Злоумышленник получает информацию об открытых портах, активных сервисах и версиях программного обеспечения, что позволяет

* Статья получена 29 июня 2026 г.

ему подобрать эксплойты и спланировать дальнейшие действия. Современные методы сканирования эволюционировали в сторону повышенной скрытности: используются нестандартные комбинации TCP-флагов (FIN, NULL, XMAS), снижение интенсивности запросов (slow scan) [1–3] и распределение активности между несколькими источниками (distributed scan) [4–6].

Традиционные системы обнаружения вторжений (IDS), основанные на сигнатурном анализе, эффективно выявляют высокоинтенсивные сканирования (например, SYN-сканирование с Nmap по умолчанию), но обладают рядом ограничений. Во-первых, они требуют заранее известных сигнатур атак, что делает их беспомощными против модифицированных или новых методов. Во-вторых, пороговые механизмы не способны обнаружить активность, распределенную во времени или между многими источниками, поскольку отдельные события не превышают установленных пределов.

В связи с этим актуальной является разработка методов анализа TCP-активности, которые не ограничиваются поиском точных совпадений, а выявляют отклонения от нормального поведения сети на основе статистических, временных и пространственных характеристик.

Целью работы стало исследование и разработка методов комбинированного анализа TCP-активности для обнаружения скрытых и распределенных сканирований портов, а также их экспериментальная оценка.

Для достижения поставленной цели были выделены следующие задачи:

- разработать эвристические правила анализа TCP-флагов для выявления нестандартных типов сканирования (FIN, NULL, XMAS);
- реализовать статистические методы оценки интенсивности в скользящем окне и энтропии распределения портов для обнаружения медленных атак;
- создать графовую модель взаимодействия между источниками и портами для выявления распределенных сканирований;
- применить вероятностную структуру Count-Min Sketch для компактного хранения статистики портов с целью снижения потребления памяти;
- провести экспериментальное сравнение предложенного подхода с существующими сигнатурными и потоковыми IDS (Snort, Suricata).

1. ФОРМАЛИЗАЦИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ АНОМАЛИЙ ДЛЯ МОДУЛЯ АНАЛИЗА TCP-АКТИВНОСТИ

Модуль анализа TCP-активности является ключевым компонентом разрабатываемой системы обнаружения. Его входные данные – сетевые пакеты, прошедшие предварительную фильтрацию (только TCP-пакеты, адресован-

ные защищаемому узлу, исключая трафик из whitelist). Для каждого пакета извлекаются IP-адрес источника, порт назначения, TCP-флаги, временная метка, TTL.

Задача модуля – на основе накопленной статистики по каждому источнику определить, является ли его активность легитимной или представляет собой попытку TCP-сканирования. При этом должны выявляться следующие виды аномалий:

- высокоинтенсивное сканирование (SYN, Connect) – большое количество запросов к разным портам за короткое время;
- скрытое сканирование с нестандартными флагами (FIN, NULL, XMAS);
- медленное сканирование – низкая интенсивность, растянутая во времени (интервалы от нескольких секунд до десятков секунд);
- распределенное сканирование – скоординированная активность нескольких источников, каждый из которых генерирует малый объем трафика.

Для решения этой задачи предложен комбинированный подход, объединяющий четыре группы методов: эвристический анализ TCP-флагов, статистический анализ интенсивности и энтропии, графовый анализ взаимодействий и интегральную score-оценку [8–10].

2. МЕТОДЫ АНАЛИЗА TCP-АКТИВНОСТИ

2.1. ЭВРИСТИЧЕСКИЙ АНАЛИЗ TCP-ФЛАГОВ

Эвристический анализ основан на наблюдении, что различные методы TCP-сканирования используют специфические комбинации флагов, редко встречающиеся в легитимном трафике. Модуль включает для каждого источника следующие счетчики за всё время наблюдения [11, 12] (с периодическим сбросом после обнаружения атаки):

- `syn` – количество пакетов с флагом SYN без ACK;
- `ack` – количество пакетов SYN+ACK;
- `fin` – количество пакетов с FIN без SYN;
- `null_scan` – количество пакетов без установленных флагов;
- `xmas` – количество пакетов с комбинацией FIN+PSH+URG;
- `port_count` – количество уникальных портов, к которым были запросы.

Эвристические правила (пороги настраиваются, но типичные значения приведены ниже):

- SYN-сканирование: если `syn` > 100 и `port_count` > 20, фиксируется атака NMAP_SYN;

- FIN-сканирование: если $\text{fin} > 80$ и $\text{port_count} > 10 - \text{FIN_SCAN}$;
- NULL-сканирование: $\text{null_scan} > 30$ и $\text{port_count} > 10 - \text{NULL_SCAN}$;
- XMAS-сканирование: $\text{xmas} > 30$ и $\text{port_count} > 10 - \text{XMAS_SCAN}$;
- Connect-сканирование: $\text{syn} > 50$ и $\text{ack} > 0.5 * \text{syn}$ и $\text{port_count} > 10 - \text{CONNECT_SCAN}$.

Эти правила эффективны для интенсивных атак, но не работают для медленных и распределенных вариантов, где абсолютные значения счетчиков могут оставаться низкими. Поэтому дополнительно применяются статистические и графовые методы.

2.2. СТАТИСТИЧЕСКИЙ АНАЛИЗ ИНТЕНСИВНОСТИ И ВРЕМЕННЫХ ПАТТЕРНОВ

2.2.1. АНАЛИЗ ИНТЕНСИВНОСТИ В СКОЛЬЗЯЩЕМ ОКНЕ

Для каждого источника поддерживается временное окно длительностью 10 секунд, в котором подсчитывается количество SYN-пакетов (функция `window_rate_us`). Это позволяет выявлять всплески активности. Правило: если $\text{window_rate} > 50$ и $\text{port_count} > 20$, добавляется признак BURST. Такая ситуация характерна для быстрого сканирования или DoS-атаки.

2.2.2. АНАЛИЗ СРЕДНЕГО ИНТЕРВАЛА И ДЖИТТЕРА

Для обнаружения медленного сканирования, при котором интервалы между пакетами составляют несколько секунд, накапливаются статистики:

- средний интервал `avg_interval` (экспоненциально взвешенное скользящее среднее с коэффициентом 0,8)

$$\bar{t}_n = 0,8\bar{t}_{n-1} + 0,2\Delta t_n;$$

- джиттер `jitter` – накопленное абсолютное отклонение

$$J_n = J_{n-1} + |\Delta t_n - \bar{t}_{n-1}|.$$

Если $\text{avg_interval} < 0,05$ с (т. е. более 20 пакетов в секунду) и $\text{port_count} > 20$, добавляется признак TIMING. При малых интервалах это указывает на высокую частоту – признак интенсивного сканирования.

Для медленного сканирования используется другой критерий: если $\text{port_count} > \text{slow_scan_ports}$ (например, 15) и длительность наблюдения $\text{duration} > \text{slow_scan_duration}$ (300 секунд), то добавляется признак SLOW

с дополнительными баллами при длительности более 5 или 10 минут. Этот критерий не требует высокой мгновенной интенсивности и позволяет обнаруживать атаки, растянутые во времени.

2.2.3. ЭНТРОПИЙНЫЙ АНАЛИЗ РАСПРЕДЕЛЕНИЯ ПОРТОВ

При сканировании большого диапазона портов распределение запросов по портам становится близким к равномерному, в то время как легитимный трафик обычно концентрируется на небольшом числе портов (80, 443, 22 и т. д.). Для количественной оценки этого свойства используется энтропия Шеннона [13–15]:

$$H = - \sum_{i=1}^N p_i \log_2 p_i .$$

где p_i – оценка вероятности обращения к порту i . Для вычисления частот используется структура Count-Min Sketch (см. раздел 2.4), что позволяет оценить энтропию без хранения полного вектора частот. При $H > 4,0$ и $\text{port_count} > 20$ фиксируется признак ENTROPY.

2.3. ГРАФОВЫЙ АНАЛИЗ РАСПРЕДЕЛЕННОГО СКАНИРОВАНИЯ

Распределенное сканирование характеризуется тем, что много разных источников обращаются к одним и тем же портам (или к разным, но с высокой степенью «новизны» для каждого источника). Для выявления таких паттернов строится граф, вершинами которого являются IP-адреса источников и порты назначения, а ребра соответствуют факту обращения источника к порту [16–18].

В модуле реализованы следующие структуры:

- SrcNode – для каждого источника хранится буфер времен последних обращений и буфер времени первого обращения к новым портам;
- PortNode – для каждого порта хранится количество уникальных источников, обратившихся к нему;
- GraphEdge – ребро (источник, порт) с временем первого и последнего обращения.

Периодически (каждые 10 секунд) запускается анализ графа за временное окно (по умолчанию 30 секунд). Для каждого источника вычисляются:

- new_ports – количество портов, к которым источник обратился впервые (т. е. ранее этого окна обращения к данным портам не было);

- `total_probes` – общее число обращений;
- `repeat_ratio = 1 - new_ports / total_probes` – доля повторных обращений.

Если `new_ports` $\geq$ `fanout_threshold` (например, 20) и `repeat_ratio` $<$ `min_repeat_ratio` (0,3), источник считается участником распределенного сканирования. Логика обоснования: при распределенной разведке каждый источник обычно сканирует новые порты (низкий `repeat_ratio`) в большом количестве (высокий `fanout`). Дополнительно анализируется глобальная метрика – суммарное значение `new_ports` по всем источникам. Если она превышает `global_fanout_alert` (100), фиксируется координированная распределенная кампания.

2.4. ВЕРОЯТНОСТНЫЕ СТРУКТУРЫ ДАННЫХ COUNT-MIN SKETCH

Хранение точной частоты обращений к каждому из 65535 портов потребовало бы значительного объема памяти (например, массив `uint32_t` на 65535 элементов – 256 кБ на один источник, что неприемлемо при многих источниках). Для решения этой проблемы используется Count-Min Sketch – вероятностная структура данных, позволяющая оценивать частоту элементов с фиксированной памятью [19–21].

Count-Min Sketch представляет собой матрицу счетчиков размером `depth` $\times$ `width` (в реализации `depth = 4`, `width = 1024`). Каждый элемент хешируется несколькими независимыми хеш-функциями, и для каждой строки инкрементируется соответствующий счетчик. Оценка частоты элемента равна минимальному значению среди счетчиков по всем хешам.

В модуле Count-Min Sketch используется для оценки частоты обращения к портам при энтропии (метод `calc_entropy`) и быстром обновлении статистики без выделения памяти под новые порты.

Память, занимаемая одним sketch: $4 \times 1024 \times 4$ байта = 16 кБ. Это в 16 раз меньше точного массива. Эксперименты показали, что при сканировании до 5000 портов погрешность оценки не превышает 5 %, что достаточно для энтропийного анализа.

2.5. ИНТЕГРАЛЬНАЯ SCORE-ОЦЕНКА

Для комплексной оценки подозрительности сетевой активности разработана интегральная score-оценка, агрегирующая все описанные выше признаки. Каждый признак вносит вклад в итоговый балл в соответствии со своей значимостью, определенной экспертным путем и подтвержденной экспериментальными данными. Ниже приведены веса признаков и условия их срабатывания [8–10].

Для наглядности все признаки, их весовые коэффициенты и пороговые условия сведены в табл. 1. Выбор весов обусловлен различной информативностью признаков: наибольший вес (30 баллов) присвоен признаку BURST, характеризующему резкие всплески активности, а наименьший (10 баллов) – признаку LINEAR, указывающему на последовательный перебор портов. Промежуточные значения весов отражают вклад каждого признака в общую оценку подозрительности.

Таблица 1

Table 1

Вес и значимость признака
Weight and significance of the feature

Признак	Вес	Условие
BURST	30	rate > 50 и port_count > 20
FAST	25	port_count > fast_ports (50), rate > fast_rate (35), duration < fast_duration (90 с)
TIMING	15	avg_interval < 0,05 и port_count > 20
LINEAR	10	seq_score > 0,4 (последовательный перебор портов)
ENTROPY	20	H > 4,0 и port_count > 20
SLOW	25	port_count > slow_ports (15) и duration > slow_duration (300 с), дополнительные +10 при duration > 600 с, +5 при duration > 300 с
Nmap сигнатура	20	сработало одно из эвристических правил из раздела 2.1

Итоговое значение score суммируется. Затем в зависимости от его значения формируется уровень угрозы:

- score $\geq$ 60 – CRITICAL SCAN;
- score $\geq$ 40 – HIGH RISK SCAN;
- score $\geq$ 20 – SUSPICIOUS SCAN.

Кроме того, значение score влияет на динамическую настройку времени жизни записи об источнике (ttl_seconds): для критических атак TTL увеличивается до 600 секунд (чтобы не потерять информацию об активном злоумышленнике), для обычных источников – 60 секунд.

После срабатывания атаки (формирования alert) статистика источника частично сбрасывается: счетчики syn, ack, fin и т. д. умножаются на 0,8 (экспо-

ненциальное забывание), но port_count и битовая карта портов полностью обнуляются. Это предотвращает повторные срабатывания по той же атаке и позволяет адаптироваться к долговременной активности.

3. ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА МЕТОДОВ

3.1. КОНФИГУРАЦИЯ ЭКСПЕРИМЕНТА

Тестирование проводилось на MacBook Pro M1 Pro (10 ядер CPU, 16 ГБ ОЗУ). Генерация атак выполнялась с помощью Nmap и самописных скриптов [12]. Фоновый легитимный трафик включал веб-серфинг, DNS, SSH. Основные сценарии:

- SYN сканирование портов 1...5000 со скоростью 800...4000 пакетов в секунду (30 запусков);
- FIN-, NULL-, XMAS-сканирование (по 20 запусков);
- медленное сканирование с интервалами 1, 3, 5, 10 секунд (по 10 запусков);
- распределенное сканирование от 5 до 20 источников (по 10 запусков).

3.2. РЕЗУЛЬТАТЫ ОБНАРУЖЕНИЯ

Для различных типов сканирования допускается точность обнаружения (табл. 2).

Таблица 2

Table 2

Точность обнаружения различных типов сканирования

Detection accuracy of different scan types

Тип сканирования	Accuracy, %	Precision, %	Recall, %
SYN	96,2	96,0	96,4
FIN	95,2	94,8	95,6
NULL	94,1	93,5	94,7
XMAS	95,8	96,0	95,6
Slow scan	69,5	71,0	68,0
Distributed	73,8	75,5	72,0

Для интенсивных атак методы показали высокую эффективность (94...96 %). Медленное сканирование с интервалом 1 секунда обнаруживается почти так же хорошо, как интенсивное, поскольку окно в 10 секунд всё еще

фиксирует достаточное количество пакетов. При интервале 10 секунд точность падает до 69,5 %. Основная сложность связана с тем, что за 10-секундное окно может не набраться ни одного пакета, и требуются долговременные накопления (признак SLOW), которые могут давать ложные срабатывания на редком легитимном трафике.

Распределенное сканирование с пятью источниками обнаруживается очень хорошо (94 %), но с ростом числа источников точность снижается. При 20 источниках каждый в среднем сканирует лишь 100 портов (из 3000 целевых), что приближается к порогу `fanout_threshold = 20`, и некоторые источники могут не превысить его. Тем не менее глобальный критерий `global_fanout_alert` позволяет выявить саму кампанию.

3.3. ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ COUNT-MIN SKETCH

Сравнение потребления памяти для хранения статистики портов на один источник приведено в табл. 2. Точное хранение (битовая карта + массив частот) требует более 512 кБ на источник. Использование CMS снижает этот объем до 16 кБ (в 32 раза). При 1000 активных источников (что бывает при DDoS-атаках или сканировании из ботнета) экономия памяти составляет десятки мегабайт (табл. 3).

Таблица 3

Table 3

Сравнение памяти для хранения статистики портов

Comparison of memory for storing port statistics

Метод	Память на источник	Память на 1000 источников
Битовая карта (65 536 бит)	8 кБ	8 МБ
Точные счетчики (uint32 на порт)	256 кБ	256 МБ
Count-Min Sketch (4×1024×4)	16 кБ	16 МБ

4. СРАВНЕНИЕ С СУЩЕСТВУЮЩИМИ МЕТОДАМИ

Сравнение предложенного комбинированного подхода с классическими сигнатурными IDS (Snort) и потоковой Suricata представлено в табл. 4. Данные для Snort и Suricata получены при их настройке по умолчанию с подключенными правилами для обнаружения сканирования.

Т а б л и ц а 4

T a b l e 4

Сравнение точности обнаружения скрытых атак
Comparison of the accuracy of detection of hidden attacks

Тип атаки	Предложенные методы	Snort	Suricata
Slow scan	69,5 %	52,4 %	70,1 %
Distributed scan	73,8 %	46,8 %	67,4 %

Программное обеспечение Snort, основанное на сигнатурах, не способно накапливать статистику за длительные интервалы и выявлять скоординированную активность разных источников, поэтому его эффективность низка; Suricata имеет механизмы потокового анализа, что позволяет ему обнаруживать медленное сканирование наравне с нашей системой (разница в пределах погрешности). Однако для распределенного сканирования Suricata уступает 6,4 %, поскольку его корреляционные механизмы менее развиты.

По вычислительной эффективности предложенные методы также выигрывают: загрузка CPU при обработке 25 000 пакетов в секунду составила 18 % (против 36 % у Snort и 29 % у Suricata). Это объясняется отказом от глубокого анализа пакетов и использованием легковесных структур данных.

ЗАКЛЮЧЕНИЕ

В статье представлен комплекс методов анализа TCP-активности для обнаружения скрытых и распределенных форм сканирования портов. Основные результаты:

- эвристический анализ TCP-флагов позволяет с высокой точностью (94...96 %) выявлять интенсивные SYN, FIN, NULL, XMAS сканирования;
- статистический анализ интенсивности в скользящем окне и долгосрочных интервалов дает возможность обнаруживать медленное сканирование. Точность для интервала 10 секунд достигла 69,5 %, что на 17 % выше, чем у Snort;
- графовый анализ взаимодействий между источниками и портами эффективен для выявления распределенных атак: точность 73,8 % для 20 источников, что на 27 % выше, чем у Snort, и на 6 % выше, чем у Suricata;
- использование Count-Min Sketch позволило сократить память для хранения частот портов в 32 раза (до 16 кБ на источник) без значимой потери точности энтропийной оценки;

- интегральная score-оценка объединяет все признаки, обеспечивая баланс между чувствительностью и устойчивостью к ложным срабатываниям (общий FPR 2,4 %).

Предложенные методы могут быть реализованы в виде легковесного модуля, работающего в реальном времени на узлах с ограниченными ресурсами. Дальнейшие исследования направлены на применение методов машинного обучения для автоматического определения пороговых значений и адаптации к профилю нормального трафика конкретной сети.

СПИСОК ЛИТЕРАТУРЫ

1. *Muraleedharan N., Janet B.* Slow TCP port scan detection using flow data // International Conference on Security, Privacy and Data Analytics. – Singapore: Springer, 2022. – P. 17–32.
2. *Miranda D., Monteiro R., Silva J.M.C.* p4SD: A lightweight port scan detection for programmable networks // International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia. – IEEE, 2025. – P. 1–6. – DOI: 10.23919/SoftCOM66362.2025.11197439.
3. *Almseidin M., Al-Kasassbeh M., Kovacs S.* Detecting slow port scan using fuzzy rule interpolation // 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS). – Amman: IEEE, 2019. – P. 1–6.
4. *Ring M., Landes D., Hotho A.* Detection of slow port scans in flow-based network traffic // PLoS one. – 2018. – Vol. 13 (9). – P. e0204507.
5. *Haas S., Wilkens F., Fischer M.* Scan correlation – Revealing distributed scan campaigns // 2020 IEEE/IFIP Network Operations and Management Symposium (NOMS). – 2020. – P. 1–6. – DOI: 10.48550/arXiv.2003.05188.
6. *Griffioen H., Doerr C.* Discovering collaboration: Unveiling slow, distributed scanners based on common header field patterns // 2020 IEEE/IFIP Network Operations and Management Symposium (NOMS). – 2020. – P. 1–9. – DOI: 10.1109/NOMS47738.2020.9110444.
7. *Gates C.* Coordinated scan detection // Proceedings of the Network and Distributed System Security Symposium (NDSS 2009). – San Diego, California, 2009.
8. *Токарев Д.А., Погребан С.В.* Аномалии трафика в IP сетях и их обнаружение // Известия Института инженерной физики. – 2013. – № 4. – С. 13–17.
9. Формализованная модель обнаружения сканирования портов / Е.В. Ананьин, И.С. Кожевникова, А.В. Лысенко, А.В. Никишова // Молодой ученый. – 2016. – № 23 (127). – С. 9–12.
10. *Головачева Н.А., Андрейченко Н.Е.* Исследование методов прогнозирования атак на информационные системы // НБИ технологии. – 2022. – Т. 16, № 3. – С. 11–15.

11. PSAD – Port Scan Attack Detector (man pages) // PSAD Documentation.
12. TCP FIN, NULL, and Xmas Scans // Nmap Network Scanning Documentation.
13. *Ayoub L., Shurman M.* A lightweight entropy-based framework for multi-attack detection in software-defined networks (SDN) // 2025 26th International Arab Conference on Information Technology (ACIT). – IEEE, 2025. – P. 179–183. – DOI: 10.1109/ACIT68900.2025.11510552.
14. *Timcenko V., Gajin S.* Machine learning enhanced entropy-based network anomaly detection // Advances in Electrical and Computer Engineering. – 2021. – Vol. 21 (4). – P. 51–60.
15. Efficient and secure statistical port scan detection scheme / H. Majed, H.N. Noura, O. Salman, A. Chehab, R. Couturier // Mobile, Secure, and Programmable Networking: 6th International Conference, MSPN 2020. – Cham: Springer, 2021. – P. 72–88.
16. A hypergraph-based machine learning ensemble network intrusion detection system / Z.-Z. Lin, T.D. Pike, M.M. Bailey, N.D. Bastian // IEEE Transactions on Systems, Man, and Cybernetics: Systems. – 2024. – Vol. 54 (11). – P. 6911–6923.
17. Leveraging graph-based representations to enhance machine learning performance in IIoT network security and attack detection / B. Alwasel, A. Aldribi, M. Alreshoodi, I.S. Alsukayti, M. Alsuhaibani // Applied Sciences. – 2023. – Vol. 13 (13). – P. 7774.
18. A cooperation-aware virtual network function for proactive detection of distributed port scanning / I.J. Sanz, M.A. Lopez, D.M.F. Mattos, O.C.M.B. Duarte // 2017 1st Cyber Security in Networking Conference (CSNet'17). – Rio de Janeiro, Brazil, 2017. – P. 1–8.
19. *Martínez Aguilar R., Reviriego P., Larrabeiti D.* Combined filtering and frequency estimation with the integrated Xor filter and count-min sketch // 2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR). – IEEE, 2024. – P. 155–160. – DOI: 10.1109/HPSR62440.2024.10635957.
20. *Ekle O.A., Eberle W.* Adaptive-graph sketch: Real-time edge anomaly detection via multi-layer tensor sketching and temporal decay // 2025 IEEE International Conference on Knowledge Graph (ICKG). – IEEE, 2025. – P. 74–81.
21. PD-CPS: A practical scheme for detecting covert port scans in high-speed networks / H. Wu, Z. Shao, F. Yang, G. Cheng, X. Hu, J. Ren, W. Wang // Computer Networks. – 2023. – Vol. 231. – P. 109825. – DOI: 10.1016/j.comnet.2023.109825.

Кузлякин Дмитрий Сергеевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. E-mail: kuzlyakin.2022@corp.nstu.ru

Огнев Иван Александрович, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: i.ognev@corp.nstu.ru

DOI: 10.17212/2782-2230-2026-3-9-23

Combined analysis of TCP activity for detecting stealth and distributed port scanning*

D.S. Kuzlyakin¹, I.A. Ognev²

¹ *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant at the Department of Information Security. E-mail: kuzlyakin.2022@corp.nstu.ru*

² *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer at the Department of Information Protection. E-mail: i.ognev@corp.nstu.ru*

This article discusses TCP activity analysis methods designed to detect slow and distributed forms of port scanning that are insufficiently detected by traditional signature-based IDSs. A combined approach is proposed, including heuristic analysis of TCP flags, statistical assessment of network traffic intensity and entropy, graph analysis of interactions between nodes, and the use of the Count-Min Sketch structure for compact storage of statistics. A methodology for calculating an integrated suspicion score based on a set of features is presented. Experiments have shown that the proposed methods provide 69.5 % detection accuracy for slow scanning with a 10-s interval and 73.8 % for distributed scanning from 20 sources, which is 17–27 % higher than that of classic signature-based IDSs. At the same time, using Count-Min Sketch allows you to reduce RAM consumption by 32–37 % compared to storing full port statistics.

Keywords: TCP scanning, anomaly detection, heuristic analysis, statistical analysis, graph analysis, Count-Min Sketch, slow scan, distributed scan

REFERENCES

1. Muraleedharan N., Janet B. Slow TCP port scan detection using flow data. *International Conference on Security, Privacy and Data Analytics*, Singapore. Springer, 2022, pp. 17–32.

* Received 29 June 2026.

2. Miranda D., Monteiro R., Silva J.M.C. p4SD: A lightweight port scan detection for programmable networks. *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia. IEEE, 2025, pp. 1–6. DOI: 10.23919/SoftCOM66362.2025.11197439.
3. Almseidin M., Al-Kasassbeh M., Kovacs S. Detecting slow port scan using fuzzy rule interpolation. *2019 2nd International Conference on New Trends in Computing Sciences (ICTCS)*. Amman, IEEE, 2019, pp. 1–6.
4. Ring M., Landes D., Hotho A. Detection of slow port scans in flow-based network traffic. *PLoS one*, 2018, vol. 13 (9), p. e0204507.
5. Haas S., Wilkens F., Fischer M. Scan correlation – Revealing distributed scan campaigns. *2020 IEEE/IFIP Network Operations and Management Symposium (NOMS)*, 2020, pp. 1–6. DOI: 10.48550/arXiv.2003.05188.
6. Griffioen H., Doerr C. Discovering collaboration: Unveiling slow, distributed scanners based on common header field patterns. *2020 IEEE/IFIP Network Operations and Management Symposium (NOMS)*, 2020, pp. 1–9. DOI: 10.1109/NOMS47738.2020.9110444.
7. Gates C. Coordinated scan detection. *Proceedings of the Network and Distributed System Security Symposium (NDSS 2009)*, San Diego, California, 2009.
8. Tokarev D.A., Pogreban S.V. Anomalii trafika v IP setyakh i ikh obnaruzhenie [Traffic anomalies in IP networks and their detection]. *Izvestiya Instituta inzhenernoi fiziki*, 2013, no. 4, pp. 13–17. (In Russian).
9. Anan'in E.V., Kozhevnikova I.S., Lysenko A.V., Nikishova A.V. Formalizovannaya model' obnaruzheniya skanirovaniya portov [Formalized model for detecting port scanning]. *Molodoi uchenyi = Young Scientist*, 2016, no. 23, pp. 9–12.
10. Golovacheva N.A., Andreichenko N.E. Issledovanie metodov prognozirovaniya atak na informatsionnye sistemy [Investigation of methods for predicting attacks on information systems]. *NBI tekhnologii = NBI Technologies*, 2022, vol. 16, no. 3, pp. 11–15.
11. PSAD – Port Scan Attack Detector (man pages). *PSAD Documentation*.
12. TCP FIN, NULL, and Xmas Scans. *Nmap Network Scanning Documentation*.
13. Ayoub L., Shurman M. A lightweight entropy-based framework for multi-attack detection in software-defined networks (SDN). *2025 26th International Arab Conference on Information Technology (ACIT)*, 2025, pp. 179–183. DOI: 10.1109/ACIT68900.2025.11510552.
14. Timcenko V., Gajin S. Machine learning enhanced entropy-based network anomaly detection. *Advances in Electrical and Computer Engineering*, 2021, vol. 21 (4), pp. 51–60.
15. Majed H., Noura H.N., Salman O., Chehab A., Couturier R. Efficient and secure statistical port scan detection scheme. *Mobile, Secure, and Programmable*

Networking: 6th International Conference, MSPN 2020. Cham, Springer, 2021, pp. 72–88.

16. Lin Z.-Z., Pike T.D., Bailey M.M., Bastian N.D. A hypergraph-based machine learning ensemble network intrusion detection system. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2024, vol. 54 (11), pp. 6911–6923.

17. Alwasel B., Aldribi A., Alreshoodi M., Alsukayti I.S., Alsuhaibani M. Leveraging graph-based representations to enhance machine learning performance in IIoT network security and attack detection. *Applied Sciences*, 2023, vol. 13 (13), p. 7774.

18. Sanz I.J., Lopez M.A., Mattos D.M.F., Duarte O.C.M.B. A cooperation-aware virtual network function for proactive detection of distributed port scanning. *2017 1st Cyber Security in Networking Conference (CSNet'17)*, Rio de Janeiro, Brazil, 2017, pp. 1–8.

19. Martínez Aguilar R., Reviriego P., Larrabeiti D. Combined filtering and frequency estimation with the integrated Xor filter and count-min sketch. *2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR)*, 2024, pp. 155–160. DOI: 10.1109/HPSR62440.2024.10635957.

20. Ekle O.A., Eberle W. Adaptive-graphsketch: Real-time edge anomaly detection via multi-layer tensor sketching and temporal decay. *2025 IEEE International Conference on Knowledge Graph (ICKG)*. IEEE, 2025, pp. 74–81.

21. Wu H., Shao Z., Yang F., Cheng G., Hu X., Ren J., Wang W. PD-CPS: A practical scheme for detecting covert port scans in high-speed networks. *Computer Networks*, 2023, vol. 231, p. 109825. DOI: 10.1016/j.comnet.2023.109825.

Для цитирования:

Кузлякин Д.С., Огнев И.А. Комбинированный анализ TCP-активности для обнаружения скрытых и распределенных сканирований портов // Безопасность цифровых технологий. – 2026. – № 3 (122). – С. 9–23. – DOI: 10.17212/2782-2230-2026-3-9-23.

For citation:

Kuzlyakin D.S., Ognev I.A. Kombinirovannyi analiz TCP-aktivnosti dlya obnaruzheniya skrytykh i raspredeleennykh skanirovaniy portov [Combined analysis of TCP activity for detecting stealth and distributed port scanning]. *Bezopasnost' tsifrovyykh tekhnologii = Digital Technology Security*, 2026, no. 3 (122), pp. 9–23. DOI: 10.17212/2782-2230-2026-3-9-23.