

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.169.85 EDN: LCONGD

МЕТОД ПРОФИЛИРОВАНИЯ СЕТЕВЫХ АНОМАЛИЙ НА ОСНОВЕ ТЕРНАРНОГО ЗНАКОВОГО ПРЕДСТАВЛЕНИЯ И АВТОМАТИЧЕСКОГО ЖИЗНЕННОГО ЦИКЛА ПРОФИЛЕЙ

Научная статья

Колесников Н.Д.[1, *]
[1] ORCID : 0009-0008-6299-9733;
[1] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (nezgzokd[at]gmail.com)

Предложена: 28.05.2026; Принята: 23.06.2026; Опубликована: 17.07.2026

Аннотация

В статье описан метод профилирования сетевых аномалий. Метод сам строит и поддерживает библиотеку профилей сетевых атак, опираясь на поток аномалий от произвольного базового детектора. В его основе три механизма: тернарное знаковое кодирование наблюдений в пространство {–1, 0, +1}, информационно-взвешенное ядро попарного сходства сигнатур и жизненный цикл профилей из пяти стадий, который сам выбраковывает устаревшие паттерны – без аналитика и без обращения к LLM. Метод проверен на двух открытых наборах данных (CIC-IDS2017 и Gotham-2025) и четырех базовых детекторах разной природы (kNN, COPOD, HBOS, OCSVM). Эксперименты дали ускорение принятия решений в 1.29–1.97 раза благодаря повторному использованию активных профилей. F1-мера базового детектора при этом практически не изменяется.

Ключевые слова: профилирование сетевых атак, обнаружение аномалий, тернарное кодирование, спектральная кластеризация, жизненный цикл профилей, информационная безопасность.

A METHOD FOR PROFILING NETWORK ANOMALIES BASED ON TERNARY SIGN REPRESENTATION AND AN AUTOMATIC PROFILE LIFE CYCLE

Research article

Kolesnikov N.D.[1, *]
[1] ORCID : 0009-0008-6299-9733;
[1] ITMO University, Saint-Petersburg, Russian Federation

* Corresponding author (nezgzokd[at]gmail.com)

Suggested: 28.05.2026; Accepted: 23.06.2026; Published: 17.07.2026

Abstract

The article describes a method for profiling network anomalies. The method automatically builds and maintains a library of network attack profiles, based on a stream of anomalies from an arbitrary base detector. It is built on three mechanisms: ternary sign-coded representation of observations in the space {–1, 0, +1}, an information-weighted kernel for pairwise similarity of signatures, and a five-stage profile lifecycle that automatically discards obsolete patterns — without the need for an analyst or consultation with an LLM. The method has been tested on two public datasets (CIC-IDS2017 and Gotham-2025) and four baseline detectors of different types (kNN, COPOD, HBOS, OCSVM). The experiments demonstrated a 1.29–1.97-fold acceleration in decision-making due to the reuse of active profiles. The F1 score of the baseline detector remains virtually unchanged.

Keywords: network attack profiling, anomaly detection, ternary coding, spectral clustering, profile lifecycle, information security.

Введение

Корпоративная инфраструктура сегодня практически целиком построена на сетевом взаимодействии различных узлов в эту инфраструктуру входящих. Из-за этого обнаружение сетевых атак стало одной из ключевых задач защиты информации. Вопрос о необходимости обнаружения сетевых атак подтверждает и статистика, так, по данным Check Point Research [1], только за второй квартал 2025 года число атак на организации в Европе выросло на 21%. В России, по отчету Red Security [2], за 2024 год количество инцидентов выросло в 2.5 раза. Меняется и сам периметр: согласно IoT Analytics [3] и Palo Alto Networks [4], доля IoT-устройств и управляемой инфраструктуры в корпоративных сетях уже превысила 70%.

Из этого вытекают две связанные между собой проблемы. Первая — нагрузка на детекторы атак растет быстрее, чем железо организаций успевает за ней, задача ускорения принятия решений становится как никогда актуальной. Вторая — атаки меняются, и любой жестко зафиксированный набор сигнатур стареет за считанные месяцы. Отсюда нужен метод, который одновременно накапливает актуальную библиотеку профилей атак сам и использует ее для ускорения работы на повторяющемся трафике.

Анализ предметной области

Анализ работ по профилированию сетевых атак показывает, что существующие решения делятся на три ключевых семейства, и у каждого есть свои ограничения:

1) подходы с участием оператора. Типичный пример — DEEPCASE [5], связка рекуррентной нейронной сети и DBSCAN-кластеризации событий безопасности с однократной разметкой аналитиком. Главная слабость подхода — статичность разметки. Атаки постепенно эволюционируют, а метки остаются прежними. В итоге со временем система начинает копить и пропуски атак, и ложные срабатывания;

2) подходы с автоматической инкрементальной кластеризацией. Сюда относятся AECID [6] и ITL-IDS [7]. Эти решения строят профили автоматически, без аналитика, но накапливают их без какой-либо процедуры выбраковки. Чем больше становится библиотека, тем хуже качество совпадений: устаревшие профили продолжают влиять на решения. К этому же семейству относятся работы по поведенческому извлечению паттернов сетевого трафика [9], по кластеризации аномалий на наборе CIC-IDS-2017 алгоритмом Birch [10], а также классические работы по неконтролируемому обнаружению атак без априорных знаний [11]. Все они страдают от той же общей проблемы — у них нет встроенного механизма выбраковки выделенных ими паттернов аномального поведения.

3) подходы на основе больших языковых моделей (LLM). Свежий пример — Argos [8], где LLM-агенты автономно генерируют правила обнаружения. Гибкость такого решения высока, но и плата за нее немалая: к языковой модели нужно обращаться постоянно — и для генерации, и для сопровождения правил. Для высоконагруженных корпоративных сетей это вычислительно затратно, а для закрытых инфраструктур — попросту неприменимо.

4) ещё один смежный класс работ — поведенческое профилирование с фокусом на неизвестные ранее атаки. В первую группу таких работ можно отнести контекстно-зависимую поведенческую аномалию для обнаружения ранее не наблюдавшихся атак [12], дискретизацию признакового пространства и анализ решающих границ для unknown-attack detection [13], а также reinforcement zero-shot learning для новых сетевых атак [14]. Во вторую группу попадают работы по обнаружению ранее неизвестных атак на уровне сигнатур [15] и правила обнаружения новых атак в IoT-сегменте сети [16]. Эти работы решают близкую задачу — формирование описаний для ещё не встречавшихся паттернов трафика, — однако ни одна из них все также не включает валидацию выявляемых профилей вследствие чего они могут быть низкого качества (давать посредственный результат при обнаружении сетевых атак).

Анализ показал, что ни один из существующих подходов не сочетает сразу двух желаемых свойств: компактного масштабно-инвариантного представления аномалий и автоматической выбраковки устаревших профилей без аналитика и необходимости обращения к ресурсоемким языковым моделям. Именно отсюда и возникла задача разработать метод, обладающий всеми этими свойствами разом.

Метод профилирования сетевых аномалий на основе тернарного знакового представления и автоматического жизненного цикла профилей

Разработанный метод сам выделяет, оценивает и держит в актуальном состоянии библиотеку профилей сетевых атак. От рассмотренных в разделе 2 решений он отличается тем, что не требует ни ручной разметки, ни LLM. Метод не привязан к конкретному базовому детектору: на вход ему достаточно предоставить вектор признаков, бинарную отметку об аномальности и оценку аномальности.

Общая схема метода такая:

1) на вход поступают результаты работы базового детектора аномалий: 35-мерный вектор признаков сетевого трафика, бинарное решение об аномальности и оценка аномальности;

2) наблюдение проходит через тернарное знаковое кодирование относительно скользящего benign-эталона;

3) полученная сигнатура сравнивается с библиотекой профилей через информационно-взвешенное ядро;

4) если набралось достаточно несвязанных сигнатур, запускается спектральная кластеризация и в библиотеку добавляются новые кандидаты;

5) по результатам совпадений и согласованности с другими активными профилями каждый профиль автоматически меняет состояние в жизненном цикле;

6) арбитр и вето-движок принимают итоговое решение об аномальности с учетом найденных профилей.

Подробнее остановимся на этапах 2–6 — они составляют суть метода.

Этап 2. Тернарное знаковое кодирование. Метод использует скользящие оценки среднего μ_f и стандартного отклонения σ_f. Для каждого признака f строится тернарная сигнатура наблюдения по формуле (1):

$$s_f(x) = \begin{cases} +1, \text{ если } \frac{x_f - \mu_f}{\sigma_f} > k \\ -1, \text{ если } \frac{x_f - \mu_f}{\sigma_f} < -k \\ 0, \text{ иначе.} \end{cases} \quad (1)$$

где k = 1.5 — пороговый коэффициент.

Получаемый 35-мерный вектор фиксирует отклонения свыше 1.5σ и сохраняет их знак — выше или ниже эталона. Малые отклонения округляются до нуля. У такого представления два полезных свойства. Прежде всего, оно масштабно-инвариантно: зависит только от того, насколько наблюдение отклонилось от benign-эталона относительно собственного шума признака, не от абсолютных величин. Второе свойство — интерпретируемость: ненулевые компоненты прямо говорят аналитику, какие признаки сместились и в какую сторону, что дает интуитивно понятный «портрет» аномалии.

Этап 3. Сравнение через информационно-взвешенное ядро. Сходство двух тернарных сигнатур s_i и s_j считается по формуле (2):

$$K\left(s_i, s_j\right) = \frac{\sum_f w_f \cdot a_f}{\sum_f w_f \cdot e_f} \quad (2)$$

где a_f равен +1 при совпадении ненулевых знаков, -1 при противоположных и 0, если хотя бы один из векторов нулевой в этой позиции; e_f — индикатор того, что хотя бы один вектор ненулевой; w_f — вес признака, пропорциональный его информационному выигрышу.

Ядро возвращает значение из [–1; +1]: K = +1 – это идентичные плотные сигнатуры, K = –1 — противоположные, K = 0 — нет совпадений. Знаменатель в (2) нормирует ядро по «активным» позициям, благодаря чему оценка не зависит от плотности сигнатуры. Важная деталь — одно и то же ядро работает и при поиске в библиотеке (один-к-N), и при кластеризации непознанных сигнатур (N-к-N). Это заметно упрощает программную реализацию метода.

Этап 4. Спектральная кластеризация и формирование кандидатов. Сигнатуры аномалий копятся в буфере. Как только буфер достигает порога (100 сигнатур) или с предыдущего запуска прошло 30 минут, начинается спектральная кластеризация. Из попарных значений ядра строится матрица аффинности A_ij = (K_ij + 1) / 2, после чего считаются собственные значения нормированного лапласиана. Число кластеров определяется автоматически — по эвристике eigengap, то есть по позиции наибольшего разрыва между соседними собственными значениями. Из каждого кластера берется представитель — мажоритарная по позициям сигнатура. Этот представитель добавляется в библиотеку как новый профиль в состоянии «кандидат».

Этап 5. Жизненный цикл профилей. Каждый профиль в библиотеке проходит конечный автомат из пяти состояний. «Кандидат» — только что извлечен из кластеризации, статистики еще нет. «Испытание» — статистика копится, но на решения профиль еще не влияет. «Активный» — участвует в принятии решений. «Пониженный» — деградировал, но может вернуться. «Списан» — окончательно исключен. Сам граф состояний и переходов показан на рисунке 1.

Рисунок 1 - Состояния и переходы жизненного цикла профиля

DOI: https://doi.org/10.60797/IRJ.2026.169.85.1

Переходы между состояниями определяются автоматически по двум показателям: числу совпадений профиля с поступающими сигнатурами и доле «правильных» совпадений, которую метод оценивает через консенсус с другими активными профилями. Профиль уходит из «кандидата» в «испытание» при 10 совпадениях и низком пересечении с benign-эталоном. Из «испытания» в «активный» — при точности 0.9. Из «активного» в «пониженный» — при падении точности ниже 0.7 или трех ложных срабатываниях подряд. Из «пониженного» есть два пути: либо обратно в «активный» при восстановлении точности до 0.75, либо в «списан» — при падении точности ниже 0.4 или возрасте более 100 окон. Такая схема сама убирает устаревшие профили и тем самым снимает главную проблему рассмотренных в разделе 2 аналогов – накопление некачественных шаблонов.

Этап 6. Принятие решения арбитром и вето. Для нового наблюдения сначала считается его тернарная сигнатура, потом ищутся top-K (K = 5) ближайших профилей в библиотеке. Арбитр выносит вердикт по правилу консенсуса. Если совпали два и более активных профиля с близкими метками — высокая уверенность. Один активный профиль – средняя. Только «кандидаты» или «испытание» — низкая. Нет совпадений — помечается потенциально новый паттерн. Параллельно работает вето-движок. Он проверяет два дополнительных условия: разреженность сигнатуры (доля ненулевых компонент менее 0.05) и превышение benign-сходства над максимальным сходством с активными профилями более чем на 0.3. Срабатывание любого из этих условий принудительно меняет итоговое решение на benign — это страховка от ложных срабатываний на пограничных наблюдениях. Когда в библиотеке есть активные профили, метод дополнительно работает в режиме fast-path: при высоком совпадении наблюдения хотя бы с одним из них решение об аномальности выносится сразу, без полного цикла базового детектора. Этот механизм и дает ускорение на знакомом трафике.

IDEF0-диаграмма метода показана на рисунке 2.

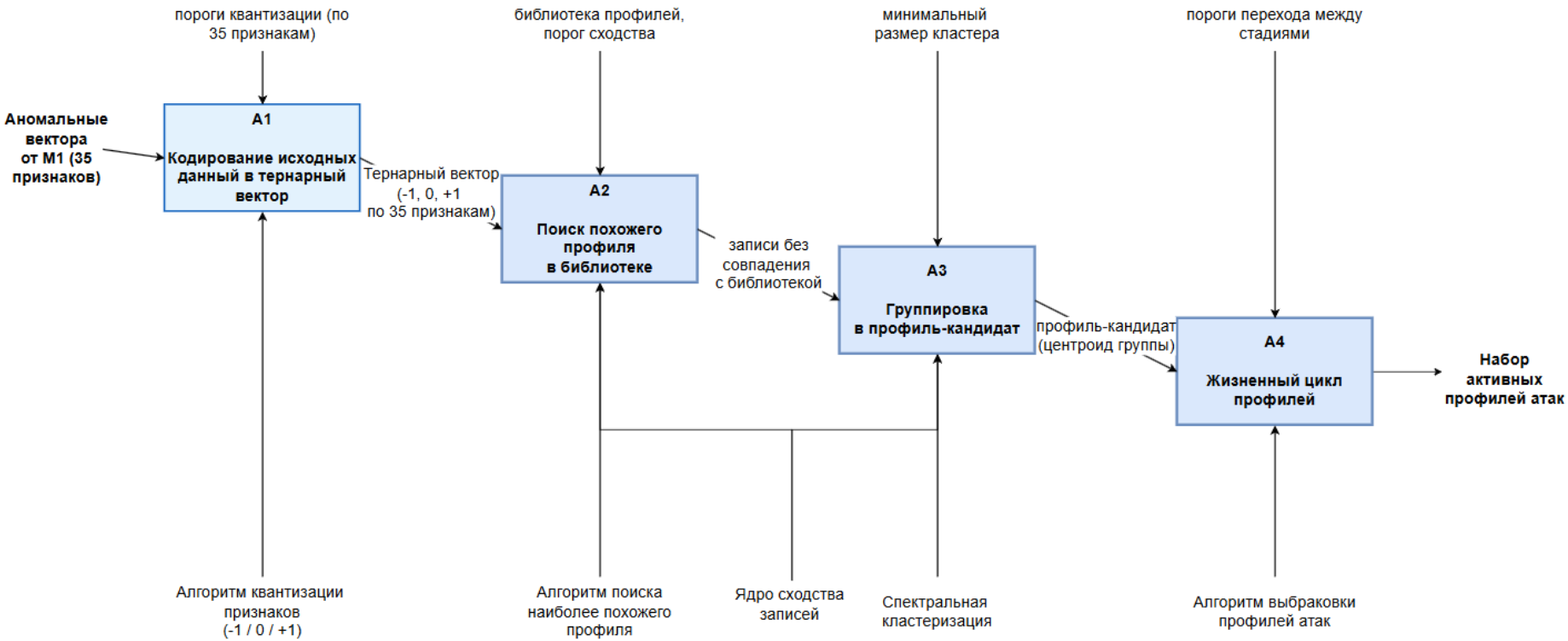

Рисунок 2 - IDEF0-диаграмма метода профилирования сетевых аномалий
DOI: https://doi.org/10.60797/IRJ.2026.169.85.2

Экспериментальное исследование

4.1. Выбор и разработка программных инструментов

Программная реализация метода написана на Python 3.10. Из библиотек задействованы numpy и scipy (численные расчеты и линейная алгебра), scikit-learn (спектральная кластеризация и базовые детекторы), pyod (расширенные реализации COPOD и HBOS).

4.2. Эксперимент

4.2.1. Используемые наборы данных

Для проверки метода взяты два эталонных набора данных, охватывающих разные сегменты сетевой инфраструктуры:

1) CIC-IDS2017 [18] — классический эталон для оценки систем обнаружения сетевых атак на корпоративном трафике; в наборе 2.83 млн записей с соотношением benign к атакам 80:20. Ранее в литературе [17] были задокументированы отдельные ограничения этого набора, которые в настоящем эксперименте учтены при предобработке;

2) Gotham-2025 [19] — современный набор для IoT-сегмента сети; содержит 3,13 млн записей с соотношением 35:65 и охватывает специфику IoT-ботнетов.

Такая пара наборов нужна, чтобы проверить метод и в традиционных корпоративных сетях, и в сетях с IoT-устройствами.

4.2.2. Базовые детекторы аномалий

Поток аномалий в метод поставляли четыре базовых детектора разной природы:

1) kNN — метрический подход на основе ближайших соседей;

2) COPOD (Copula-Based Outlier Detection) — непараметрический метод на копульных функциях;

3) HBOS (Histogram-Based Outlier Score) — быстрый метод на гистограммах в предположении независимости признаков;

4) OCSVM (One-Class Support Vector Machine) — классический ядровой метод в одноклассовой постановке.

Эти четыре детектора покрывают четыре непохожих семейства подходов к обнаружению аномалий — метрические, статистические, плотностные и ядровые. Такой набор дает жесткую проверку независимости метода от реализации базового детектора.

4.2.3. Оценка качества выделения профилей

На первом этапе проверялось, насколько корректно метод выделяет профили атак из потока аномалий. Для каждой пары «базовый детектор + набор данных» фиксировались две вещи: распределение профилей по состояниям жизненного цикла на момент окончания эксперимента и изменение F1-меры базового детектора при подключении метода. Сводные числа — в таблице 1.

Таблица 1 - Распределение профилей по состояниям жизненного цикла

DOI: https://doi.org/10.60797/IRJ.2026.169.85.3

Детектор + Датасет	Всего	Кандидаты	Испытание	Активные	Реплей, %	ΔF1
OCSVM + CIC-IDS2017	23	8	2	13	64,8	+0,0021
OCSVM + Gotham-2025	64	21	6	37	68,7	0,0000
kNN + CIC-IDS2017	23	4	6	13	54,5	−0,0143
COPOD + CIC-IDS2017	10	5	0	5	49,7	+0,0043
HBOS + CIC-IDS2017	12	3	5	4	40,1	0,0000
COPOD + Gotham-2025	55	12	26	17	22,5	−0,0188
kNN + Gotham-2025	71	19	51	0	0	0,0000
HBOS + Gotham-2025	73	20	52	0	0	0,0000

Из таблицы 1 видно несколько закономерностей. Начнем с того, что далеко не все профили доходят до состояния «активный»: в среднем 35–65% остаются в «кандидате» или «испытании». Это и есть консервативность жизненного цикла — на решения метод выпускает только те профили, у которых есть статистика совпадений и согласованность с другими активными профилями. Например, в сценариях kNN + Gotham-2025 и HBOS + Gotham-2025 ни один профиль

не дошел до активного состояния. Причина в том, что эти детекторы на данном наборе дают слабо стабильные аномалии: разрозненные срабатывания не образуют устойчивых кластеров, и метод корректно отказывается двигать соответствующие профили дальше по жизненному циклу. Следующее, что бросается в глаза: по всем восьми сценариям абсолютное изменение F1-меры базового детектора не превышает 0,02 — это укладывается в статистический шум (малую значимость такого отклонения). Иначе говоря, подключение метода не роняет качество базового детектора, а кое-где даже минимально улучшает его — благодаря согласованным решениям активных профилей.

4.2.4. Оценка ускорения принятия решений

На втором этапе оценивалось ускорение принятия решений благодаря режиму fast-path. Для каждой пары измерялось две величины: среднее время полного цикла принятия решения базовым детектором (t_детектор) и среднее время принятия решения при включенном методе (T_с_профилями). Результаты сведены в таблицу 2.

Таблица 2 - Ускорение принятия решений через fast-path по библиотеке профилей

DOI: https://doi.org/10.60797/IRJ.2026.169.85.4

Детектор + Датасет	Активные	Реплей, %	t_детектор, мкс	T_с_профилями, мкс	Ускорение
COPOD + CIC-IDS2017	5	49,7	6 226	3 156	x1,97
COPOD + Gotham-2025	17	22,5	21 875	16 984	x1,29
HBOS + CIC-IDS2017	4	40,1	264	182	x1,45
kNN + CIC-IDS2017	13	54,5	388	204	x1,90
OCSVM + CIC-IDS2017	13	64,8	110	65	x1,69
OCSVM + Gotham-2025	37	68,7	115	65	x1,76

Полученные значения ускорения лежат в диапазоне 1,29–1,97 раза и хорошо коррелируют с долей повторяющихся паттернов (реплея) в каждом сценарии. Чем больше наблюдений попадает в уже сформированные активные профили, тем больший выигрыш дает fast-path. Отдельно отметим случай COPOD + CIC-IDS2017: при доле реплея около 50% удалось достичь практически двукратного ускорения, а исходное время детектора там — 6,2 мс. Для продуктивных систем с высокой интенсивностью потока данных это значит, что метод способен почти удвоить пропускную способность подсистемы обнаружения — при той же точности, что и была в базовой реализации (без применения метода).

4.3. Сравнительный анализ

Чтобы сопоставить разработанный метод с известными решениями, проведено сравнение с двумя подходами: ITL-IDS на инкрементальной кластеризации [7] и AECID на многоплоскостных отпечатках [6]. Сравнение шло на тех же базовых детекторах, что и в основном эксперименте; фиксировалось итоговое изменение F1-меры при подключении каждого профайлера. Сводные результаты — в таблице 3.

Таблица 3 - Сравнение с существующими методами профилирования по изменению F1

DOI: https://doi.org/10.60797/IRJ.2026.169.85.5

Детектор + Датасет	Предложенный метод	Mahdavi и др. [7]	Landauer и др. [6]
OCSVM + CIC-IDS2017	+0.0021	−0,0612	−0,0612
OCSVM + Gotham-2025	0.0000	−0,1248	−0,1248
COPOD + CIC-IDS2017	+0.0043	−0,0078	−0,0078
COPOD + Gotham-2025	−0.0188	−0,1215	−0,1215

Из таблицы 3 видно: известные подходы к профилированию заметно роняют F1 базового детектора — вплоть до 0.125 в зависимости от пары «детектор + набор». А разработанный метод держит точность в пределах статистического шума. Разница объясняется автоматической выбраковкой: в предложенном решении устаревшие и нестабильные профили выводятся из эксплуатации до того, как успевают повлиять на итоговый вердикт. В [6] и [7] такие профили продолжают участвовать в принятии решений и тянут качество вниз.

Итого, метод одновременно ускоряет принятие решений на знакомом трафике и держит точность на уровне базового детектора. Ни один из рассмотренных аналогов этого вместе не делает.

Заключение

В работе разработан метод профилирования сетевых аномалий со следующими преимуществами:

1) метод сам строит, оценивает и поддерживает библиотеку профилей сетевых атак — без аналитика и без обращения к LLM. Это делает его применимым в закрытых и высоконагруженных корпоративных сетях;

2) тернарное знаковое представление дает масштабную инвариантность относительно различий между сегментами сети;

3) автоматический жизненный цикл из пяти стадий сам выбраковывает устаревшие профили и потому не дает библиотеке деградировать во времени;

4) метод не зависит от конкретной реализации базового детектора аномалий. Это подтверждено экспериментально на четырех детекторах разной природы.

Эксперименты на двух эталонных наборах данных (CIC-IDS2017 и Gotham-2025) и четырех базовых детекторах (kNN, COPOD, HBOS, OCSVM) показали ускорение принятия решений в 1.29–1.97 раза благодаря повторному использованию активных профилей. F1-мера базового детектора при этом меняется в пределах 0.02 — это статистический шум одного запуска. На фоне известных методов профилирования [6], [7] разработанное решение дает заметно меньшую деградацию точности — за счет автоматической выбраковки.

В дальнейшем планируется расширить охватываемые методом классы атак за пределы сетевой разведки, рассмотренной здесь, а также применить тот же жизненный цикл к профилированию событий безопасности на уровне приложения.

Конфликт интересов

Не указан.

Рецензия

Яковлев И.В., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.169.85.6

Conflict of Interest

None declared.

Review

Iakovlev I.V., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.169.85.6

Список литературы / References

1. Check Point Research. Global Cyber Attacks Surge 21% in Q2 2025: Europe Experiences the Highest Increase of all Regions // Check Point Blog. — 2025. — 17 July. — URL: https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/ (accessed: 13.03.2026).

2. Red Security. Отчет SOC: в 2024 году число инцидентов ИБ выросло в 2.5 раза. — 2024. — URL: https://tadviser.com/index.php/Company:RED_Security (дата обращения: 13.03.2026).

3. Sinha S. Number of connected IoT devices / S. Sinha // IoT Analytics. — 2024. — URL: https://iot-analytics.com/number-connected-iot-devices/ (дата обращения: 13.03.2026).

4. Palo Alto Networks. The 2024 IoT SPalo Alto Networks. The 2024 IoT Security Benchmark Report // Palo Alto Networks. — 2024. — URL: https://www.paloaltonetworks.com/resources/research/the-2024-benchmark-report-on-iot-security (accessed: 13.03.2026).ecurity Benchmark Report. — 2024.

5. Van Ede T. DEEPCASE: Semi-Supervised Contextual Analysis of Security Events / T. Van Ede, H. Aghakhani, N. Spahn [et al.] // Proceedings of the 2022 IEEE Symposium on Security and Privacy (S&P 2022). — IEEE, 2022. — P. 522–539.

6. Landauer M. AMiner: A Modular Log Data Analysis Pipeline for Anomaly-based Intrusion Detection / M. Landauer, M. Wurzenberger, F. Skopik [et al.] // Digital Threats: Research and Practice. — 2023. — Vol. 4. — № 1. — P. 1–26.

7. Ahmad R. ITL-IDS: Incremental Transfer Learning for Intrusion Detection Systems / R. Ahmad, I. Alsmadi, W. Alhamdan [et al.] // Knowledge-Based Systems. — 2023. — Vol. 282. — P. 111101.

8. Gu Y. Argos: Agentic Time-Series Anomaly Detection with Autonomous Rule Generation via Large Language Models / Y. Gu, Y. Xiong, J. Mace [et al.] // arXiv. — 2025. — arXiv:2501.14170. — DOI: 10.48550/arXiv.2501.14170.

9. Meng Y. Behavior Pattern Mining from Traffic and Its Application to Network Anomaly Detection / Y. Meng, Q. Qian, Z. Liu [et al.] // Security and Communication Networks. — 2022. — P. 9139321.

10. Yin Y. Improving multilayer-perceptron (MLP)-based network anomaly detection with birch clustering on CICIDS-2017 dataset / Y. Yin, J. Jang-Jaccard, W. Xu [et al.] // Proceedings of the 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2023). — IEEE, 2023. — P. 423–431.

11. Casas P. Knowledge-independent traffic monitoring: Unsupervised detection of network attacks / P. Casas, J. Mazel, P. Owezarski [et al.] // IEEE Network. — 2012. — Vol. 26. — № 1. — P. 13–21.

12. Qin Z.Q. Interaction Context-Aware Network Behavior Anomaly Detection for Discovering Unknown Attacks / Z.Q. Qin, X.K. Ma, Y.J. Wang // Security and Communication Networks. — 2022. — P. 3595304.

13. Shin G.Y. Data discretization and decision boundary data point analysis for unknown attack detection / G.Y. Shin, D.W. Kim, M.M. Han // IEEE Access. — 2022. — Vol. 10. — P. 114008–114015.

14. Wang H. Unknown network attack detection method based on reinforcement zero-shot learning / H. Wang, Y. Wang, Y. Guo // Journal of Physics: Conference Series. — IOP Publishing, 2022. — Vol. 2303. — № 1. — P. 012008.

15. Alzubi S. Towards intrusion detection of previously unknown network attacks / S. Alzubi, F. Stahl, M.M. Gaber // Communications of the ECMS. — 2021. — Vol. 35. — № 1. — P. 35–41.

16. Chakraborty S. Detection and classification of novel attacks and anomaly in IoT network using rule based deep learning model / S. Chakraborty, S.R. Krishna, A.K. Pradhan [et al.] // SN Computer Science. — 2024. — Vol. 5. — № 8. — P. 1056.

17. Engelen G. Troubleshooting an Intrusion Detection Dataset: the CICIDS2017 Case Study / G. Engelen, V. Rimmer, W. Joosen // Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW). — IEEE, 2021. — P. 7–12.

18. CIC-IDS-2017 Network Intrusion Dataset // Kaggle. — URL: https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset (accessed: 13.03.2026).

19. Sáez-de-Cámara X. Gotham Testbed: a Reproducible IoT Testbed for Security Experiments and Dataset Generation / X. Sáez-de-Cámara, J.L. Flores, C. Arellano [et al.] // IEEE Transactions on Dependable and Secure Computing. — 2024. — Vol. 21. — № 1. — P. 186–203.

Список литературы на английском языке / References in English

1. Check Point Research. Global Cyber Attacks Surge 21% in Q2 2025: Europe Experiences the Highest Increase of all Regions // Check Point Blog. — 2025. — 17 July. — URL: https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/ (accessed: 13.03.2026).

2. Red Security. Otchet SOC: v 2024 godu chislo intsidentov IB viroslo v 2.5 raza [Red Security. SOC Report: The number of cybersecurity incidents increased 2.5-fold in 2024]. — 2024. — URL: https://tadviser.com/index.php/Company:RED_Security (accessed: 13.03.2026). [in Russian]

3. Sinha S. Number of connected IoT devices / S. Sinha // IoT Analytics. — 2024. — URL: https://iot-analytics.com/number-connected-iot-devices/ (дата обращения: 13.03.2026).

4. Palo Alto Networks. The 2024 IoT SPalo Alto Networks. The 2024 IoT Security Benchmark Report // Palo Alto Networks. — 2024. — URL: https://www.paloaltonetworks.com/resources/research/the-2024-benchmark-report-on-iot-security (accessed: 13.03.2026).ecurity Benchmark Report. — 2024.

5. Van Ede T. DEEPCASE: Semi-Supervised Contextual Analysis of Security Events / T. Van Ede, H. Aghakhani, N. Spahn [et al.] // Proceedings of the 2022 IEEE Symposium on Security and Privacy (S&P 2022). — IEEE, 2022. — P. 522–539.

6. Landauer M. AMiner: A Modular Log Data Analysis Pipeline for Anomaly-based Intrusion Detection / M. Landauer, M. Wurzenberger, F. Skopik [et al.] // Digital Threats: Research and Practice. — 2023. — Vol. 4. — № 1. — P. 1–26.

7. Ahmad R. ITL-IDS: Incremental Transfer Learning for Intrusion Detection Systems / R. Ahmad, I. Alsmadi, W. Alhamdan [et al.] // Knowledge-Based Systems. — 2023. — Vol. 282. — P. 111101.

8. Gu Y. Argos: Agentic Time-Series Anomaly Detection with Autonomous Rule Generation via Large Language Models / Y. Gu, Y. Xiong, J. Mace [et al.] // arXiv. — 2025. — arXiv:2501.14170. — DOI: 10.48550/arXiv.2501.14170.

9. Meng Y. Behavior Pattern Mining from Traffic and Its Application to Network Anomaly Detection / Y. Meng, Q. Qian, Z. Liu [et al.] // Security and Communication Networks. — 2022. — P. 9139321.

10. Yin Y. Improving multilayer-perceptron (MLP)-based network anomaly detection with birch clustering on CICIDS-2017 dataset / Y. Yin, J. Jang-Jaccard, W. Xu [et al.] // Proceedings of the 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2023). — IEEE, 2023. — P. 423–431.

11. Casas P. Knowledge-independent traffic monitoring: Unsupervised detection of network attacks / P. Casas, J. Mazel, P. Owezarski [et al.] // IEEE Network. — 2012. — Vol. 26. — № 1. — P. 13–21.

12. Qin Z.Q. Interaction Context-Aware Network Behavior Anomaly Detection for Discovering Unknown Attacks / Z.Q. Qin, X.K. Ma, Y.J. Wang // Security and Communication Networks. — 2022. — P. 3595304.

13. Shin G.Y. Data discretization and decision boundary data point analysis for unknown attack detection / G.Y. Shin, D.W. Kim, M.M. Han // IEEE Access. — 2022. — Vol. 10. — P. 114008–114015.

14. Wang H. Unknown network attack detection method based on reinforcement zero-shot learning / H. Wang, Y. Wang, Y. Guo // Journal of Physics: Conference Series. — IOP Publishing, 2022. — Vol. 2303. — № 1. — P. 012008.

15. Alzubi S. Towards intrusion detection of previously unknown network attacks / S. Alzubi, F. Stahl, M.M. Gaber // Communications of the ECMS. — 2021. — Vol. 35. — № 1. — P. 35–41.

16. Chakraborty S. Detection and classification of novel attacks and anomaly in IoT network using rule based deep learning model / S. Chakraborty, S.R. Krishna, A.K. Pradhan [et al.] // SN Computer Science. — 2024. — Vol. 5. — № 8. — P. 1056.

17. Engelen G. Troubleshooting an Intrusion Detection Dataset: the CICIDS2017 Case Study / G. Engelen, V. Rimmer, W. Joosen // Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW). — IEEE, 2021. — P. 7–12.

18. CIC-IDS-2017 Network Intrusion Dataset // Kaggle. — URL: https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset (accessed: 13.03.2026).

19. Sáez-de-Cámara X. Gotham Testbed: a Reproducible IoT Testbed for Security Experiments and Dataset Generation / X. Sáez-de-Cámara, J.L. Flores, C. Arellano [et al.] // IEEE Transactions on Dependable and Secure Computing. — 2024. — Vol. 21. — № 1. — P. 186–203.