УДК 004.023
DOI: 10.26102/2310-6018/2026.57.6.006

Метод обнаружения аномалий сетевого трафика в малых информационных системах на основе поведенческих микропрофилей

З.М. Альбекова, А.Ф. Околелова✉, М.А. Шапетин, П.В. Егоров, А.А. Бакунов

Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация

Резюме. Малые информационные системы – корпоративные сети малого и среднего бизнеса, ведомственные локальные сети, специализированные автоматизированные системы управления – уязвимы к автоматизированным атакам подбора учетных данных по протоколам FTP и SSH, поскольку располагают ограниченными вычислительными ресурсами и кадровым потенциалом для развертывания полноценных средств защиты. В работе предложен частично надзорный метод обнаружения аномалий сетевого трафика с минимальными требованиями к разметке, моделирующий нормальное поведение пользователей через поведенческие микропрофили – робастные статистические описания типовых режимов сетевой активности, получаемые адаптивной кластеризацией TCP-потоков алгоритмом K-Means. Каждый профиль задается парой «медиана – масштабированное медианное абсолютное отклонение», а аномальность нового потока оценивается взвешенным Z-показателем относительно профиля ближайшего кластера. Веса признаков определяются по статистике Колмогорова-Смирнова, число кластеров – по критерию насыщения площади под ROC-кривой. Экспериментальная проверка на общедоступном наборе данных CICIDS2017 для атак FTP-Patator и SSH-Patator показала, что предложенный метод существенно превосходит классические безнадзорные детекторы – Isolation Forest, Local Outlier Factor и One-Class SVM – как по ранжирующей способности, так и по доле истинных тревог. Ключевым практическим результатом является работоспособность метода в режиме развертывания, не требующем разметки на целевой системе, так как отбор признаков выполняется однократно по публично доступным данным об атаках, после чего построение профилей и выбор порога обходятся без меток. В этих условиях метод обнаруживает более трех четвертей попыток перебора учетных данных, тогда как конкурирующие методы в аналогичных условиях практически не срабатывают.

Ключевые слова: обнаружение аномалий, сетевой трафик, поведенческие микропрофили, MAD-статистика, K-Means, брутфорс-атаки, CICIDS2017, малые информационные системы.

Для цитирования: Альбекова З.М., Околелова А.Ф., Шапетин М.А., Егоров П.В., Бакунов А.А. Метод обнаружения аномалий сетевого трафика в малых информационных системах на основе поведенческих микропрофилей. *Моделирование, оптимизация и информационные технологии.* 2026;14(6). URL: https://moitvivt.ru/ru/journal/article?id=2348 DOI: 10.26102/2310-6018/2026.57.6.006

A method for network traffic anomaly detection in small information systems based on behavioral microprofiles

Z.M. Albekova, A.F. Okolelova✉, M.A. Shapetin, P.V. Egorov, A.A. Bakunov

North-Caucasus Federal University, Stavropol, the Russian Federation

Abstract. Small information systems – corporate networks of small and medium-sized enterprises, departmental local area networks, and specialized automated control systems – are vulnerable to automated credential brute-force attacks over FTP and SSH protocols, as they possess limited computational resources and personnel capacity to deploy full-scale security solutions. This paper proposes a semi-supervised network traffic anomaly detection method with minimal labelling requirements, which models normal user behavior through behavioral microprofiles – robust statistical

descriptions of typical network activity modes derived by adaptive K-Means clustering of TCP flows. Each profile is defined by a median and scaled median absolute deviation pair, while the anomaly score of a new flow is computed as a weighted Z-score relative to the profile of its nearest cluster. Feature weights are determined using the Kolmogorov–Smirnov statistic, and the number of clusters is selected by a ROC-curve area saturation criterion. Experimental evaluation on the publicly available CICIDS2017 dataset for FTP-Patator and SSH-Patator attacks demonstrated that the proposed method substantially outperforms classical unsupervised detectors – Isolation Forest, Local Outlier Factor, and One-Class SVM – both in ranking ability and in the proportion of true alarms. The key practical finding is the method's effectiveness in a deployment mode that requires no labelling on the target system: feature selection is performed once using publicly available attack data, after which profile construction and threshold calibration proceed without any labels. Under these conditions, the method detects more than three quarters of credential brute-force attempts, whereas competing methods under identical conditions produce virtually no detections.

Keywords: anomaly detection, network traffic, behavioral microprofiles, MAD statistics, K-Means, brute-force attacks, CICIDS2017, small information systems.

For citation: Albekova Z.M., Okolelova A.F., Shapetin M.A., Egorov P.V., Bakunov A.A. A method for network traffic anomaly detection in small information systems based on behavioral microprofiles. *Modeling, Optimization and Information Technology*. 2026;14(6). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2348 DOI: 10.26102/2310-6018/2026.57.6.006

Введение

Малые информационные системы – сети малого и среднего бизнеса, ведомственные сегменты, специализированные автоматизированные системы управления – составляют наиболее многочисленную и при этом наименее защищенную часть цифровой инфраструктуры. Спектр угроз для них практически не отличается от угроз крупным корпоративным сетям, тогда как доступные ресурсы для защиты – вычислительные мощности, бюджеты и квалификация персонала – несопоставимо скромнее [1, 2]. Особое место среди актуальных угроз занимают атаки автоматизированного подбора учетных данных по протоколам SSH и FTP – они остаются одним из наиболее массовых векторов первичной компрометации в малых сетях [3], а успешный перебор пароля открывает злоумышленнику легитимный канал доступа, после чего выявление последующей вредоносной активности принципиально усложняется. Вместе с тем малые системы обладают структурной особенностью, которую можно обратить в преимущество, так нормальный трафик здесь формируется ограниченным и предсказуемым кругом источников, каждый из которых демонстрирует устойчивый и повторяющийся профиль сетевого поведения. Это делает малые системы естественной областью применения поведенческого моделирования нормы.

Существующие подходы к обнаружению аномалий решают задачу лишь частично. Методы с учителем способны выявлять новые разновидности атак, однако требуют репрезентативной размеченной выборки, получение которой в условиях одной организации, как правило, нереализуемо [4]. Безнадзорные детекторы – Isolation Forest, Local Outlier Factor, One-Class SVM – снимают требование разметки, но имеют два существенных ограничения [5, 6]. Во-первых, их оценочные шкалы привязаны к геометрии обучающего множества и при изменении распределения трафика теряют предсказательную силу. Во-вторых, не улавливаются отклонения, которые незначительны в масштабе всей выборки, но аномальны внутри конкретного режима поведения.

Цель настоящей работы – разработать вычислительно легкий, интерпретируемый метод обнаружения аномалий сетевого трафика с минимальными требованиями к разметке, где отбор признаков выполняется по публичным данным об атаках однократно

и не привязан к конкретной защищаемой системе, а построение профилей нормального поведения пользователей не требует разметки. Ключевая идея метода состоит в построении поведенческих микропрофилей – компактных статистических описаний типовых режимов сетевой активности, выделяемых кластеризацией K-Means.

Материалы и методы

Экспериментальная проверка метода проведена на открытом наборе данных CICIDS2017, подготовленном Канадским институтом кибербезопасности и являющемся одним из общепринятых эталонных корпусов для задач обнаружения сетевых вторжений [7]. В качестве моделируемых атак выбраны два класса – FTP-Patator и SSH-Patator, относящиеся к категории брутфорс и зафиксированные в подмножестве «Bruteforce-Tuesday». Для построения профилей нормального поведения использовался трафик понедельника «Benign-Monday», не содержащий атак. После очистки данных от пропусков и бесконечных значений выборка нормальных TCP-потоков случайным образом разбивалась в пропорции 80/20 на обучающее множество X_fit и валидационное множество X_val. Тестовое множество составили все TCP-потоки вторника – 199 527 записей. Структура и объемы подмножеств приведены в Таблице 1.

Таблица 1 – Структура выборки TCP-потоков на наборе данных CICIDS2017
Table 1 – TCP flow sampling structure on the CICIDS2017 dataset

Подмножество	Назначение выбора	Число потоков
X_fit (Monday TCP, 80 %)	построение микропрофилей	198 732
X_val (Monday TCP, 20 %)	выбор числа кластеров	49 683
Tuesday Benign (TCP)	тест, нормальный класс	190 377
Tuesday FTP-Patator	тест, атака подбора FTP	5 931
Tuesday SSH-Patator	тест, атака подбора SSH	3 219

Признаковое пространство формировалось из числовых характеристик потоков используемого набора данных. Помимо основных имеющихся признаков – были выделены производные признаки, отражающие асимметрию направлений обмена, а именно:

– признак ratio_fwd, вычисляющий долю пакетов клиента по формуле (1);

– признак log_ratio_act_bwd, вычисляющий логарифмический баланс активных данных и обратных пакетов по формуле (2);

– признак log_ratio_bytes, вычисляющий логарифмический баланс байтового объема пакетов по формуле (3).

Введение этих признаков обусловлено физической природой брутфорс-атак, так как в ходе автоматизированного перебора клиент отправляет короткие команды USER/PASS либо инициирующие пакеты SSH-рукопожатия, тогда как ответ сервера, как правило, существенно меньше по объему, чем при нормальной работе.

$$ratio\_fwd = \frac{N_{fwd}}{(N_{fwd} + N_{bwd})}, \quad (1)$$

$$log\_ratio\_act\_bwd = ln(N_{act} + 1) - ln(N_{bwd} + 1), \quad (2)$$

$$log\_ratio\_bytes = ln(B_{fwd} + 1) - ln(B_{bwd} + 1), \quad (3)$$

где N_{fwd} – число пакетов в прямом направлении; N_{bwd} – число пакетов в обратном направлении; N_{act} – число пакетов с полезной нагрузкой в прямом направлении; B_{fwd} – суммарный объем передаваемых байтов в прямом направлении; B_{bwd} – суммарный объем передаваемых байтов в обратном направлении.

Построение модели нормального поведения включает четыре последовательных шага. На первом шаге выполняется отбор информативных признаков методом Колмогорова-Смирнова, где для каждого признака-кандидата вычисляется D-статистика между его распределением на нормальных потоках и на каждом из двух классов атак, а затем признаку приписывается вес w_k как полусумма двух D-значений. В признаковый набор включаются переменные с $w_k > 0{,}5$, а из оставшихся попарно коррелированных признаков ($|r| > 0{,}95$) удаляется менее информативный. Данный шаг опирается на метки атак и соответствует офлайн-калибровке на исторически накопленном трафике [8], на следующих шагах построения профилей метки не используются.

На втором шаге все базовые признаки подвергаются логарифмическому преобразованию $\ln(x+1)$ для подавления правосторонней асимметрии распределений, а к производным признакам оно не применяется, поскольку они уже сформированы в логарифмической шкале. В результате каждый поток представляется вектором x_{log}.

На третьем шаге векторы x_{log} масштабируются преобразованием StandardScaler, обученным исключительно на данных X_fit, и по масштабированным представлениям выполняется адаптивная кластеризация алгоритмом MiniBatchKMeans с нахождением оптимального числа кластеров C. Масштабирование необходимо, поскольку K-Means использует евклидову метрику и чувствителен к разбросу признаков, для вычисления самих профилей на следующем шаге используются исходные логарифмические значения x_{log}, а не нормированные.

На четвертом шаге каждый кластер c получает поведенческий микропрофиль – компактное статистическое описание одного типового режима сетевой активности. Под режимом понимается устойчивый сценарий использования сети конкретным источником трафика. В малой системе таких режимов немного, тогда как их совокупность стабильна и предсказуема, что делает оправданным описание всей нормы малым числом локальных моделей вместо единой глобальной. Для каждого кластера c из C кластеров строился микропрофиль – вектор робастных оценок $(\tilde{\mu}_k, \tilde{\sigma}_k)$ по всем k признакам, где в качестве $\tilde{\mu}_k$ использовались медиана, и масштабированное медианное абсолютное отклонение $\tilde{\sigma}_k$, обладающие максимальной точкой пробоя 50 % и нечувствительные к выбросам обучающей выборки [9], вычислялись по формулам:

$$\tilde{\mu}_k = median(\{x_{\{k,i\}}\}), \quad (4)$$

$$MAD(x_k) = median(|x_{\{k,i\}} - \tilde{\mu}_k|), \quad (5)$$

$$\tilde{\sigma}_k = max(1{,}4826 \cdot MAD(x_k);\ \sigma_{min}), \quad (6)$$

где $x_{\{k,i\}}$ – логарифмированное значение признака k для i-го потока кластера c* из X_fit.

Нижняя граница σ_{min} устраняет деление на ноль для признаков с вырожденно малым разбросом внутри кластера, в эксперименте использовалось $\sigma_{min} = 0{,}10$ для объёмных признаков и $\sigma_{min} = 0{,}02$ для ratio-признаков. Аномальность нового потока оценивается взвешенным Z-показателем $S_w(x)$ относительно профиля ближайшего кластера c*. При этом новый поток сначала преобразуется в вектор x_{sc} (StandardScaler, обученный на X_fit), который подается на вход K-Means для назначения кластера c*. Чем больше значение $S_w(x)$, тем сильнее поведение потока отклоняется от типового режима, описываемого кластером c*. Оценка неотрицательна по построению (используются абсолютные значения) и равна нулю только для потока, в точности совпадающего с медианным профилем по всем признакам, вычисляется по формуле:

$$S_w(x) = \Sigma_k\, w_k \cdot \frac{|x_{\{log,k\}} - \tilde{\mu}_k|}{\tilde{\sigma}_k}, \quad (7)$$

где $x_{\{log,k\}}$ – логарифмированное значение признака k нового потока; $\tilde{\mu}_k$ и $\tilde{\sigma}_k$ – параметры профиля кластера c*.

Число кластеров C подбиралось на сетке {5, 7, …, 39} по критерию насыщения средней площади под ROC-кривой, усредненной по 5 случайным инициализациям K-Means – выбиралось наименьшее C, при котором одновременно выполняются условия:

$$AUC_{mean}(C) \geq max(AUC_{stable}) - 0{,}005;\ \sigma(AUC, C) < 0{,}03, \quad (8)$$

где C – проверяемое число кластеров; $AUC_{mean}(C)$ – среднее значение площади под ROC-кривой по 5 случайным инициализациям K-Means при данном C; $\sigma(AUC, C)$ – стандартное отклонение AUC по тем же 5 инициализациям, характеризующее устойчивость результата к выбору начальных центроидов; AUC_{stable} – множество значений $AUC_{mean}(C)$ для тех C, при которых $\sigma(AUC, C) < 0{,}03$; порог 0,005 задает допустимую потерю качества ранжирования относительно наилучшего стабильного значения.

Решающее правило формируется сравнением $S_w(x)$ с порогом θ. В работе исследованы два сценария выбора порога. Порог θ_J соответствует точке J индекса Юдена на ROC-кривой и обеспечивает максимальную сбалансированную чувствительность [10], определяется по формуле:

$$J = TPR - FPR, \quad (9)$$

где TPR – доля верных срабатываний к общему числу срабатываний, FPR – доля ложных срабатываний к общему числу срабатываний.

Несмещенный контаминационный порог θ_c определяется как (1 − ĉ)-квантиль распределения S_w на валидационном множестве X_val, где ĉ – априорная оценка доли аномалий, задаваемая оператором безопасности на основании экспертных знаний или исторической статистики инцидентов. В реальном развертывании эта величина неизвестна и требует оценки; в настоящем эксперименте для воспроизводимости использовалось значение ĉ = 0,0459, соответствующее фактической доле атакующего трафика в тестовой выборке. Чувствительность метода к выбору ĉ является самостоятельным направлением дальнейшего исследования.

Эффективность методов оценивалась по стандартному набору метрик бинарной классификации, рассчитываемых из матрицы ошибок, состоящего из точности (Precision), полноты (Recall), гармонического среднего точности и полноты (F1). Точность определяет долю реальных атак среди всех тревог и характеризует нагрузку на оператора безопасности. Полнота показывает, какую долю фактически произошедших атак метод обнаружил. F1-мера объединяет оба показателя в одну оценку, что особенно важно при сильном дисбалансе классов, характерном для задач обнаружения аномалий.

$$Precision = \frac{TP}{TP + FP}, \quad (10)$$

$$Recall = \frac{TP}{TP + FN}, \quad (11)$$

$$F1 = \frac{2 \cdot TP}{2 \cdot TP + FP + FN}, \quad (12)$$

где TP – верно обнаруженные атаки, FP – ложные тревоги на нормальном трафике, TN – верно пропущенные нормальные потоки, FN – пропущенные атаки.

Также, важной метрикой оценки построенной модели метода является ROC-AUC. Площадь под ROC-кривой AUC характеризует ранжирующую способность метода независимо от выбранного порога, где значение AUC = 1 соответствует идеальному ранжированию, AUC = 0,5 – случайному. Именно AUC является основным

сравнительным показателем для неконтролируемых детекторов, поскольку не зависит от конкретной точки применения. Полная архитектура предлагаемого метода обнаружений аномалий, включающая все описанные этапы исследования, представлена на Рисунке 1.

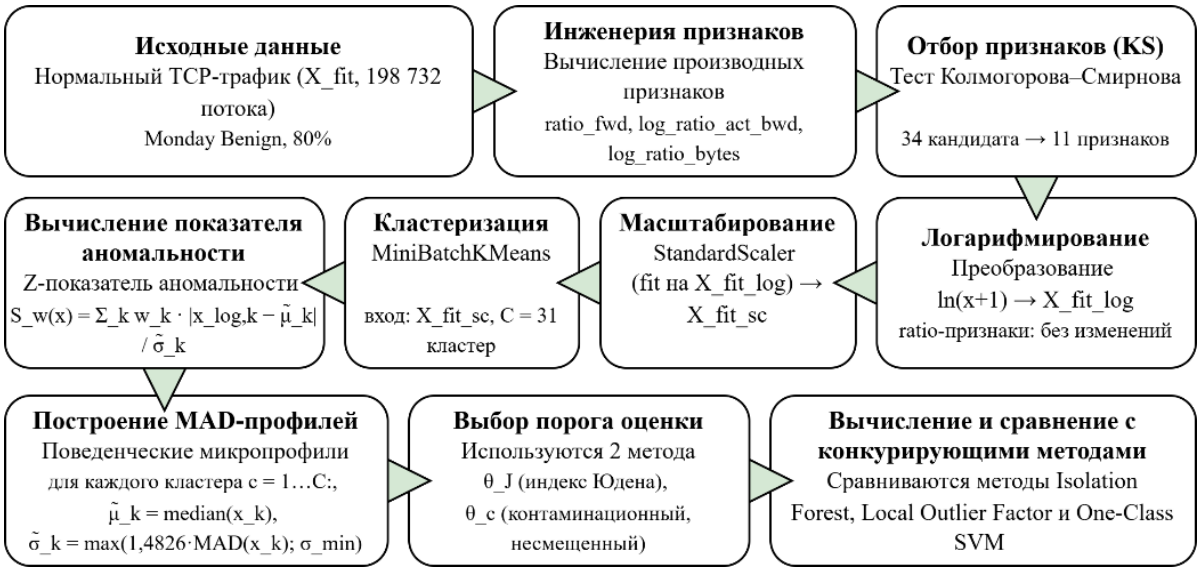

Рисунок 1 – Архитектура метода обнаружения аномалий на основе поведенческих микропрофилей

Figure 1 – Architecture of the microprofile-based anomaly detection method

Результаты

Процедура отбора признаков сократила исходное пространство с 34 кандидатов до 11 переменных. Среди отобранных – один производный признак (ratio_fwd), характеристики длины пакетов в прямом направлении, межпакетные интервалы и параметры начального TCP-окна. При переборе числа кластеров на сетке {5, 7, …, 39} стабильные решения с $\sigma < 0{,}02$ были получены при $C = 31$ и $C = 35$. Значение $C = 31$ выбрано как наименьшее из устойчивых, удовлетворяющее критерию насыщения AUC, т. к. дальнейшее увеличение числа кластеров не дает статистически значимого прироста качества ранжирования.

Разделяющая способность взвешенного Z-показателя S_w наглядно прослеживается по распределениям оценок на тестовой выборке. Для легитимных потоков характерны относительно низкие значения: $\mu = 1{,}43$, $\sigma = 1{,}97$, при этом 99-й перцентиль не превышает 11,0. Иными словами, подавляющее большинство нормальных соединений получает оценку, не выходящую за пределы своего кластерного профиля. Картина для атакующего трафика принципиально иная: потоки FTP-Patator отклоняются от ближайшего профиля в среднем на $S_w = 4{,}70$, потоки SSH-Patator – на $S_w = 5{,}21$, что в 3,3 и 3,6 раза превышает соответствующее среднее для нормального класса. Этот разрыв получен из-за того, что брутфорс-сессии структурно несовместимы с типовыми режимами легитимной активности, зафиксированными в профилях, и потому стабильно попадают в область высоких Z-оценок. Как следствие, детектор уверенно ранжирует атакующий трафик выше нормального на протяжении всего диапазона порогов, что и выражается в итоговом значении AUC = 0,958.

Сравнение предложенного метода с методами-конкурентами – Isolation Forest, Local Outlier Factor и One-Class SVM – проводилось в двух сценариях, различающихся по степени осведомленности о метках атак при выборе порога. В обоих сценариях все методы обучались на одном и том же множестве X_fit (для конкурирующих методов

использовалась случайная подвыборка из 30 000 потоков, что соответствует их типичным практическим режимам), а параметры аномальности задавались равными априорной доле аномалий ĉ = 0,0459.

Для сценария 1 порог отсечения θ_J для всех методов определялся индексом Юдена по тестовой ROC-кривой. Этот сценарий предполагает наличие размеченных данных об атаках и отражает верхнюю оценку достижимого качества каждого детектора. Сводные результаты приведены в Таблице 2.

Таблица 2 – Сравнение методов обнаружения аномалий с порогом θ_J, индекс Юдена
Table 2 – Comparison of anomaly detection methods with the threshold θ_J, Youden index

Метод / Method	Precision	Recall	F1	AUC
Микропрофиль (предлагаемый) Microprofile (proposed)	0,213	0,961	0,348	0,958
Isolation Forest	0,105	0,968	0,190	0,883
Local Outlier Factor	0,122	0,965	0,216	0,889
One-Class SVM	0,049	0,988	0,093	0,658

По площади под ROC-кривой предложенный метод превосходит ближайшего конкурента – Local Outlier Factor – на 0,069 единицы, Isolation Forest – на 0,075 единицы и One-Class SVM – на 0,3 единицы. Абсолютное значение AUC характерно для задач обнаружения на наборе CICIDS2017 и само по себе не является исключительным [1], а достигнутое ранжирование получено вычислительно лёгким интерпретируемым методом. При выравнивании по Recall (все методы обнаруживают ≈ 96–99 % атак) ключевое преимущество метода микропрофилей состоит в существенно более высокой точности: 0,213 против 0,049–0,122 у конкурентов, то есть доля истинных тревог в 1,7–4,3 раза выше при сопоставимой полноте.

Для сценария 2 порог отсечения θ_c каждого метода вычислялся исключительно из распределения его собственных оценок метрик на обучающей подвыборке – как $(1 - \hat{c})$-квантиль, без какого-либо обращения к тестовым меткам. Для предлагаемого метода порог θ_c дополнительно вычислялся по валидационному множеству X_val. Этот сценарий воспроизводит реальные условия развертывания, при которых размеченные атаки заранее недоступны, и является наиболее объективным критерием практической применимости. Сводные результаты приведены в Таблице 3.

Таблица 3 – Сравнение методов обнаружения аномалий с порогом θ_c, контаминационный порог
Table 3 – Comparison of anomaly detection methods with the threshold θ_c, contamination threshold

Метод / Method	Precision	Recall	F1
Микропрофиль (предлагаемый) Microprofile (proposed)	0,376	0,758	0,502
Isolation Forest	0,002	0,002	0,002
Local Outlier Factor	0,085	0,212	0,121
One-Class SVM	0,000	0,000	0,000

Результаты сценария 2 требуют пояснения, так как низкие показатели конкурентов не свидетельствуют об их принципиальной непригодности – в сценарии 1 при оптимально подобранном пороге те же методы достигают Recall ≈ 0,96–0,99. Причина отказа в сценарии 2 носит технический характер – шкалы оценок Isolation Forest и One-Class SVM привязаны к геометрии обучающего множества, а не к абсолютной

степени аномальности, и при статистическом смещении трафика между обучающей и тестовой выборками $(1 - \hat{c})$-квантиль от обучающих скоров перестает соответствовать реальной границе аномалии. LOF частично сохраняет работоспособность (F1 = 0,121), поскольку его шкала плотности устойчивее к такому сдвигу. Предлагаемый метод этого недостатка лишен, так как Z-показатель S_w по построению неотрицателен и имеет фиксированный физический смысл – отклонение в единицах MAD от профиля нормального режима, что обеспечивает переносимость порога с данных X_val на тестовую выборку.

Таким образом, сценарий 1 подтверждает превосходство метода по ранжирующей способности (AUC), а сценарий 2 – его уникальную пригодность для развертывания без предварительной разметки атак, что критично именно для малых информационных систем.

ROC-кривые всех рассматриваемых методов по сценарию 1, приведенные на Рисунке 2, позволяют сопоставить их ранжирующую способность визуально. Кривая предлагаемого метода расположена выше кривых всех конкурентов на всем протяжении оси FPR. Наиболее ощутимое расхождение наблюдается в области малых ложноположительных ставок, т. е. при FPR < 0,03 кривые Isolation Forest и Local Outlier Factor практически сливаются с диагональю случайного классификатора, тогда как метод микропрофилей в той же зоне удерживает TPR выше 0,7. Это означает, что при жестком ограничении на ложные тревоги конкурирующие методы фактически теряют способность обнаруживать атаки, тогда как предложенный метод сохраняет приемлемую чувствительность.

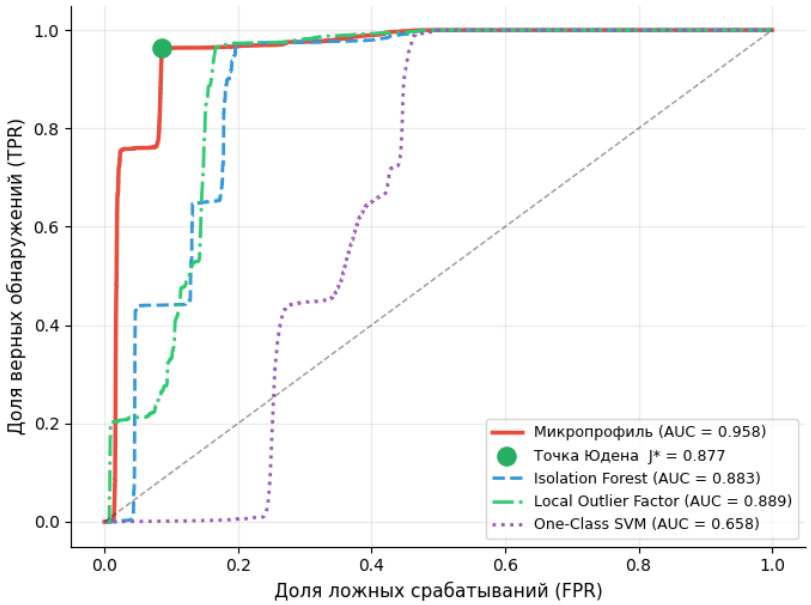

Рисунок 2 – ROC-кривые методов обнаружения аномалий на тестовой выборке CICIDS2017
Figure 2 – ROC curves of anomaly detection methods on the CICIDS2017 test set

Метод One-Class SVM занимает последнее место по площади под кривой, при AUC = 0,658. Столь низкое значение согласуется с поведением метода в сценарии 2, где он практически не дает срабатываний, т. к. модель не формирует шкалы оценок, монотонно связанной с аномальностью, и при смещении распределения трафика между обучающей и тестовой выборками ее разделяющая способность деградирует.

Точка, выбранная по критерию индекса Юдена, отмеченная на кривой метода микропрофилей, соответствует FPR ≈ 0,086 и TPR ≈ 0,961. На практике это означает, что

из каждых 100 атак верно обнаруживаются 96, при этом ошибочно помечая как аномальные менее 9 % легитимных потоков.

Обсуждение

Полученные показатели качества поддаются объяснению через физические свойства исследуемых атак, что подтверждает содержательность предложенного подхода. Потоки FTP-Patator уверенно выявляются в обоих операционных режимах – полнота (Recall) составила 67,5 % при θ_c и 98,6 % при θ_J. Столь высокая детектируемость обусловлена характером протокольного обмена: команды аутентификации USER и PASS занимают порядка 23 байт, тогда как при нормальной работе FTP-клиент передает файлы с полезной нагрузкой 400–1460 байт. После логарифмирования признаков это выражается в контрасте ln(24) ≈ 3,18 против ln(1 461) ≈ 7,29 – отклонение достаточно велико, чтобы Z-показатель фиксировал его относительно байтовых признаков соответствующего профиля.

Иначе обстоит дело с потоками SSH-Patator, где полнота обнаружения составила 91,6 % при θ_J и 91,2 % при θ_c. Это объясняется тем, что детекция в данном случае опирается прежде всего на признак направленности трафика ratio_fwd, который мало чувствителен к сдвигу порога. Несколько более низкая полнота по сравнению с FTP-Patator при θ_J связана со структурными особенностями протокола SSH, т. к. фаза согласования ключей порождает пакеты объёмом 600 – 1 400 байт, что частично совпадает с диапазоном нормальных интерактивных сессий. Здесь проявляется фундаментальное ограничение поточного анализа без инспекции содержимого – отсевающие метаданные потока не позволяют разграничить рукопожатие при легитимной аутентификации и рукопожатие в ходе перебора паролей.

Преимущество метода поведенческих микропрофилей перед остальными детекторами объясняется иным принципом моделирования нормы. Разбиение трафика на кластеры выделяет гомогенные группы потоков со схожим поведением, и внутри каждой такой группы разброс признаков заметно ниже, чем по всей обучающей выборке. За счет этого Z-показатель оказывается чувствительным к локальным отклонениям, которые на фоне всей выборки выглядят незначительными, но явно аномальны внутри конкретного кластера. Методы Isolation Forest и Local Outlier Factor оценивают аномальность относительно глобальной структуры данных и при оптимально подобранном пороге в сценарии 1 они достигают сравнимой полноты обнаружения, однако это сопровождается существенно большим числом ложных тревог – т. е. методы находят атаки, но одновременно помечают как подозрительную значительную долю стандартного трафика.

Результаты сценария 2 выявляют принципиальное различие между предложенным методом и конкурентами в части свойств шкал аномальности. Функции решения Isolation Forest и One-Class SVM призваны к геометрии обучающего множества, оба представления теряют предсказательную силу при изменении статистических характеристик трафика между обучением и тестированием. Переход с трафика понедельника на трафик вторника представляет именно такой сдвиг – тестовая выборка содержит атакующие потоки, отсутствовавшие при построении модели, что приводит к нарушению соответствия между обученной шкалой и реальной степенью аномальности потока. В режиме θ_c, не требующем разметки атак, предлагаемый метод обнаруживает более трех четвертей попыток подбора учетных данных при точности (Precision) = 0,376. Конкурирующие методы в этом же режиме либо дают единичные срабатывания (LOF с F1 = 0,121), либо не обнаруживают атак вовсе.

Вместе с тем необходимо обозначить границы применимости полученных результатов. Эксперимент проведен на одном публичном датасете CICIDS2017, известном как относительно простой для задач детекции – классы атак в нем хорошо отделимы от нормального трафика по базовым статистикам потоков [1], что может завышать оценки качества по сравнению с реальными сетевыми средами. Вопрос о том, насколько полученные показатели сохранятся на более сложных наборах данных или в условиях реального трафика, остается открытым и требует отдельной экспериментальной проверки. Проблема переносимости моделей между наборами данных хорошо задокументирована в литературе [4] и требует дополнительного изучения. Кроме того, оба рассмотренных класса атак – FTP-Patator и SSH-Patator – относятся к одному типу угроз, а именно автоматизированному перебору учетных данных. Применение предлагаемого метода при иных сценариях атак в рамках данной работы не рассматривалось.

Заключение

В настоящей работе разработан метод обнаружения аномалий сетевого трафика, в основе которого лежит представление нормального поведения внутри малой информационной системы в виде набора поведенческих микропрофилей. Каждый профиль описывает один устойчивый режим сетевой активности через медиану и масштабированное медианное абсолютное отклонение по 11 информативным признакам TCP-потока, при оптимальном числе профилей $C = 31$, которое определено по критерию насыщения AUC. Аномальность нового потока измеряется взвешенным Z-показателем S_w относительно ближайшего профиля – величиной с фиксированным физическим смыслом, не зависящей от глобальной структуры обучающей выборки. Именно это свойство позволяет обнаруживать отклонения, незначительные в масштабе всего трафика, но выраженные внутри конкретного режима поведения, и сохранять предсказательную силу порога при смене состава трафика.

Проверка на наборе данных CICIDS2017 показала, что Z-оценки атакующего трафика превышают нормальные в 3,3–3,6 раза, что выражается в AUC = 0,958 – результате, типичном для задач на наборе CICIDS2017 [1], однако достигнутом без затрат на обучение с учителем и при вычислительной стоимости инференса, в 2–12 раз ниже, чем у методов-конкурентов. Преимущество над Isolation Forest составило 0,075 единицы, над Local Outlier Factor – 0,069, над One-Class SVM – 0,3. Особую практическую значимость представляет поведение метода в несмещенном режиме, когда порог θ_c задается исключительно по распределению нормального трафика без каких-либо сведений об атаках – при таких условиях метод обнаруживает 75,8 % попыток подбора учетных данных при Precision = 0,376, тогда как Isolation Forest и One-Class SVM в том же режиме дают F1 < 0,002.

Полученные результаты относятся к строго определенным условиям эксперимента – набору CICIDS2017 и двум классам брутфорс-атак, – поэтому их распространение на другие сетевые среды и типы угроз требует самостоятельной верификации. Во-первых, апробация на других публичных датасетах позволит оценить переносимость метода за пределы набора данных CICIDS2017. Во-вторых, целесообразно распространить подход на атаки иных классов – DoS, горизонтальное сканирование, веб-эксплойты и т. д. В-третьих, включение временных меток сессий в модель профиля откроет возможность выявления медленных и распределенных кампаний, которые в текущей реализации остаются за пределами наблюдаемого.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Maseer Z.K., Yusof R., Bahaman N., et al. Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. *IEEE Access*. 2021;9:22351–22370. https://doi.org/10.1109/ACCESS.2021.3056614
2. Campazas-Vega A., Crespo-Martínez I.S., Guerrero-Higueras Á.M., et al. Malicious traffic detection on sampled network flow data with novelty-detection-based models. *Scientific Reports*. 2023;13(1):15446. https://doi.org/10.1038/s41598-023-42618-9
3. Alotibi N., Alshammari M. Deep learning-based intrusion detection: A novel approach for identifying brute-force attacks on FTP and SSH protocol. *International Journal of Advanced Computer Science and Applications*. 2023;14(6):107–111. https://doi.org/10.14569/IJACSA.2023.0140612
4. Cantone M., Marrocco C., Bria A. Machine learning in network intrusion detection: A cross-dataset generalization study. *IEEE Access*. 2024;12:144489–144508. https://doi.org/10.1109/ACCESS.2024.3472907
5. Chua W., Pajas A.L.D., Castro C.Sh., et al. Web traffic anomaly detection using Isolation Forest. *Informatics*. 2024;11(4):83. https://doi.org/10.3390/informatics11040083
6. Rabih R., Vahdat-Nejad H., Mansoor W., et al. Highly accurate anomaly based intrusion detection through integration of the local outlier factor and convolutional neural network. *Scientific Reports*. 2025;15(1):21147. https://doi.org/10.1038/s41598-025-08175-z
7. Sharafaldin I., Habibi Lashkari A., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy, 22–24 January 2018, Funchal, Madeira, Portugal.* SciTePress; 2018. P. 108–116. https://doi.org/10.5220/0006639801080116
8. Awad M., Fraihat S. Recursive feature elimination with cross-validation with decision tree: feature selection method for machine learning-based intrusion detection systems. *Journal of Sensor and Actuator Networks*. 2023;12(5):67. https://doi.org/10.3390/jsan12050067
9. Goldstein M., Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PLoS ONE*. 2016;11(4):e0152173. https://doi.org/10.1371/journal.pone.0152173
10. Rai H.M., Yoo J., Agarwal S. The improved network intrusion detection techniques using the feature engineering approach with boosting classifiers. *Mathematics*. 2024;12(24):3909. https://doi.org/10.3390/math12243909

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Альбекова Замира Мухамедалиевна, кандидат педагогических наук, доцент департамента цифровых, робототехнических систем и электроники института перспективной инженерии, Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация.
e-mail: zam.stavscc@mail.ru
ORCID: 0000-0002-7214-8114

Zamira M. Albekova, Candidate of Pedagogical Sciences, Associate Professor at the Department of Digital, Robotic Systems and Electronics, Institute of Advanced Engineering, North-Caucasus Federal University, Stavropol, the Russian Federation.

Околелова Анастасия Федоровна, студентка, Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация.
e-mail: okolelowa.anastasya@yandex.ru
ORCID: 0009-0009-8301-6473

Anastasiia F. Okolelova, Student, North-Caucasus Federal University, Stavropol, the Russian Federation.

Шапетин Максим Алексеевич, студент, Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация.
e-mail: mshapetin@mail.ru
ORCID: 0009-0000-9766-613X

Maxim A. Shapetin, Student, North-Caucasus Federal University, Stavropol, the Russian Federation.

Егоров Павел Валерьевич, студент, Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация.
e-mail: egorovpavel2000@mail.ru
ORCID: 0009-0009-3137-8739

Pavel V. Egorov, Student, North-Caucasus Federal University, Stavropol, the Russian Federation.

Бакунов Артем Андреевич, студент, Северо-Кавказский федеральный университет, Ставрополь, Российская Федерация.
e-mail: aabakunoov@gmail.com
ORCID: 0009-0007-6745-4081

Artem A. Bakunov, Student, North-Caucasus Federal University, Stavropol, the Russian Federation.

Статья поступила в редакцию 20.04.2026; одобрена после рецензирования 05.06.2026; принята к публикации 14.06.2026.

The article was submitted 20.04.2026; approved after reviewing 05.06.2026; accepted for publication 14.06.2026.