НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2026 Том 26 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2026 Vol. 26 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2026-26-2-315-323
УДК 004.056

Обнаружение сетевых аномалий в среде Интернета вещей с использованием модифицированных статистических критериев и ансамблевых методов

Нуржан Бажаев✉

[1] Евразийский национальный университет имени Л. Н. Гумилёва, Астана, 010008, Казахстан
[2] АО «Государственная техническая служба», Астана, 010017, Казахстан

nurzhan_nfs@hotmail.com✉, https://orcid.org/0009-0009-4820-6132

Аннотация

Введение. Рост числа устройств Интернета вещей (Internet of Things, IoT) сопровождается усложнением угроз безопасности, включая атаки типа Distributed Denial of Service, brute-force авторизации и массовую генерацию пакетов. Традиционные статистические методы обнаружения аномалий показывают низкую устойчивость к шуму и не учитывают динамику трафика. Это приводит к росту числа ложноположительных срабатываний и снижению точности идентификации атак. **Метод.** Предложен гибридный подход к обнаружению аномалий в IoT-трафике, включающий три этапа: предварительную фильтрацию подозрительных пакетов с использованием модифицированной *Z*-оценки с учетом размера выборки; адаптивную вероятностную оценку риска атаки на основе байесовского классификатора с весовой функцией, усиливающей влияние значимых отклонений; финальную классификацию с применением ансамбля моделей (Random Forest, Support Vector Machine и Long Short-Term Memory), обеспечивающего устойчивость к шуму и выявление нелинейных зависимостей в данных. **Основные результаты.** Экспериментальная проверка на наборе данных UNSW-NB15, содержащем как нормальный трафик, так и различные типы атак, показала, что предложенный метод достигает Precision = 89,1 %, Recall = 90,3 % и F1-score = 89,9 %. Наилучшие результаты отмечены при анализе временных интервалов сообщений (до 92 % точности), что подтверждает эффективность временных признаков. Метод превзошел классические алгоритмы (Rosner Test, Holt-Winters) и сопоставим по точности с autoencoder, но требует меньших вычислительных ресурсов. **Обсуждение.** Гибридная архитектура позволяет адаптироваться к различным типам атак и снижает количество ложных тревог за счет сочетания статистической фильтрации и ансамблевой классификации. Устойчивость к шуму и низкая вычислительная сложность делают метод применимым в условиях ограниченных ресурсов IoT-устройств. Перспективы дальнейших исследований будут направлены на интеграцию федеративного обучения для децентрализованного анализа и использования самоподстраивающихся нейросетевых архитектур для прогнозирования сложных сценариев атак.

Ключевые слова

информационная безопасность, сети Интернета вещей, обнаружение аномалий, выявление атак, модифицированная *Z*-оценка, байесовский классификатор, ансамблевое обучение, машинное обучение, мониторинг трафика

Благодарность

Работа выполнена при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (грант № AP25794699).

Ссылка для цитирования: Бажаев Н. Обнаружение сетевых аномалий в среде Интернета вещей с использованием модифицированных статистических критериев и ансамблевых методов // Научно-технический вестник информационных технологий, механики и оптики. 2026. Т. 26, № 2. С. 315–323. doi: 10.17586/2226-1494-2026-26-2-315-323

Detection of network anomalies in the Internet of Things environment using modified statistical criteria and ensemble methods

Nurzhan Bazhayev✉

[1] L.N. Gumilyov Eurasian National University, Astana, 010008, Kazakhstan
[2] Joint Stock Company "State Technical Service", Astana, 010017, Kazakhstan

nurzhan_nfs@hotmail.com✉, https://orcid.org/0009-0009-4820-6132

Abstract

The rapid growth of Internet of Things (IoT) devices is accompanied by increasingly sophisticated security threats, including DDoS attacks, brute-force authentication attempts, and large-scale packet flooding. Traditional statistical methods for anomaly detection exhibit low robustness to noise and fail to account for the dynamic nature of IoT traffic. This results in a higher rate of false positives and reduced accuracy in attack identification. This paper proposes a hybrid approach to IoT traffic anomaly detection consisting of three stages: preliminary filtering of suspicious packets using a modified *Z*-score adjusted for sample size; adaptive probabilistic attack risk assessment based on a Bayesian classifier with a weighting function that amplifies the impact of significant deviations; final classification using an ensemble of models (Random Forest, SVM, and LSTM), which ensures robustness to noise and enables the identification of nonlinear dependencies in the data. Experimental evaluation on the UNSW-NB15 dataset, which includes both normal traffic and diverse attack scenarios, demonstrated that the proposed method achieved Precision = 89.1 %, Recall = 90.3 %, and F1-score = 89.9 %. The best results were observed in the analysis of message interval anomalies (up to 92 % accuracy), confirming the effectiveness of temporal features. The method outperformed classical algorithms (Rosner Test, Holt-Winters) and achieved comparable accuracy to autoencoder while requiring significantly fewer computational resources. The hybrid architecture enables adaptation to diverse attack types and reduces false alarms through the combination of statistical filtering and ensemble classification. Its noise resilience and low computational complexity make the method suitable for deployment in resource-constrained IoT environments. Future research directions include the integration of federated learning for decentralized anomaly detection and the use of self-adaptive neural architectures for predicting complex attack scenarios.

Keywords

information security, IoT security, IoT networks, anomaly detection, intrusion detection, modified *Z*-score, Bayesian classifier, ensemble learning, machine learning, traffic monitoring

Acknowledgements

This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP25794699).

For citation: Bazhayev N. Detection of network anomalies in the Internet of Things environment using modified statistical criteria and ensemble methods. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2026, vol. 26, no. 2, pp. 315–323 (in Russian). doi: 10.17586/2226-1494-2026-26-2-315-323

Введение

Мир стремительно погружается в эпоху Интернета вещей (Internet of Things, IoT), количество подключенных устройств к 2025 году, по прогнозам, превысит 75 млрд. Такой масштабный рост сопровождается увеличением числа атак: только в 2024 году зафиксировано более 90 млн инцидентов, что на 40 % выше показателей 2023 года. Ботнеты семейства Mirai, Mozi и новые варианты вредоносных программ активно эксплуатируют уязвимости IoT-устройств для организации распределенных атак типа Distributed Denial of Service (DDoS), хищения данных и промышленного шпионажа, что представляет серьезную угрозу для критической инфраструктуры и «умных» городов, и является одной из ключевых проблем информационной безопасности.

Традиционные методы защиты оказываются малоэффективными в условиях динамически изменяющегося IoT-трафика, где наблюдаются значительные колебания в объемах пакетов и активности узлов. Это требует разработки новых алгоритмов, способных адаптироваться к поведению устройств в реальном времени и снижать вероятность ложных срабатываний.

В последние годы наблюдается активное развитие методов обнаружения аномалий в IoT-сетях. Среди них можно выделить как классические статистические подходы, так и глубинные модели машинного обучения.

Например, в работе [1] предложена модифицированная *Z*-оценка в сочетании с энтропийным анализом параметров пакетов, что позволило достичь точности свыше 95 %. В [2] представлен ансамбль autoencoders и случайных лесов (Random Forest, RF), демонстрирующий F1-score 96 % при низкой задержке. В работе [3] отмечено, что RF, Support Vector Machine (SVM) и autoencoder остаются основой для систем обнаружения вторжений (Intrusion Detection System, IDS), однако дальнейшее развитие методов направлено на использование гибридных и ансамблевых решений. В [4] показана эффективность федеративного обучения (RFW-модели) для выявления локальных и глобальных аномалий без централизованного сбора данных. В работе [5] подчеркнута роль глубинного ансамбля Convolutional Neural Network и Long Short-Term Memory (CNN-LSTM) в сочетании с классическими методами, достигающими точность 98 %, однако ограниченных высокой вычислительной сложностью.

Несмотря на значительный прогресс, известные решения имеют ряд недостатков: высокая вычислительная нагрузка при глубоком обучении, ограничивающая их применение на пограничных IoT-узлах; чувствительность моделей к шуму и нестабильным временным

паттернам; ограниченная способность к обнаружению ранее неизвестных (zero-day) атак из-за зависимости от размеченных данных.

Эти ограничения определяют необходимость разработки метода, сочетающего точность ансамблевых алгоритмов с вычислительной эффективностью статистических подходов.

Методология ряда исследований [6–17] предполагает использование различных моделей глубокого обучения (Generative Adversarial Networks (GAN), CNN-LSTM, autoencoder), а также их ансамблей в сочетании с классическими классификаторами, такими как RF. Эксперименты показывают, что комбинации алгоритмов CNN + LSTM + RF достигают точности до 98 %, обеспечивая при этом наименьшие показатели ложных тревог.

В промышленной IoT-среде активно исследуются сценарии обнаружения аномалий оборудования (например, датчиков, контроллеров, шлюзов), где ансамбли с autoencoders и статистической предобработкой (методов быстрого преобразования Фурье и главных компонент) демонстрируют высокую эффективность, но требуют значительных вычислительных ресурсов.

Кроме того, применяются стохастические модели, имитирующие DDoS-атаки, что позволяет более точно оценивать устойчивость IDS и эффективность интеграции с технологиями машинного обучения.

В работе [18] отмечена перспективность использования отрицательной энтропии как регуляризатора для повышения устойчивости к высокоизменчивым паттернам трафика.

Выполненный анализ показал: статистические методы (энтропия, модифицированные *Z*-оценки) остаются востребованными для легких и вычислительно экономичных решений; ансамблевые модели (RF, SVM, XGBoost, CNN-LSTM) обеспечивают баланс между точностью и устойчивостью; глубокие нейросетевые подходы (autoencoder, GAN, CNN-LSTM) достигают точности свыше 98 %, но ограничены вычислительной сложностью; распределенные и стохастические методы (Federated Learning, RFW) становятся перспективными направлениями для защиты IoT-сетей.

Цель работы — разработка гибридного метода обнаружения сетевых аномалий в IoT-трафике для задач информационной безопасности, основанного на модифицированной *Z*-оценке, адаптивном байесовском классификаторе и ансамбле моделей RF-SVM-LSTM, обеспечивающий: снижение числа ложноположительных срабатываний; адаптацию к различным типам IoT-атак; применимость на ресурсно-ограниченных устройствах.

Описание предлагаемого метода

Разработан гибридный метод обнаружения аномалий в IoT-трафике, объединяющий преимущества статистического и машинного подходов. Метод включает три последовательных этапа.

Этап 1. Первичная фильтрация подозрительных событий с помощью модифицированной *Z*-оценки.

Этап 2. Вероятностная оценка степени аномальности посредством байесовского классификатора с весовой функцией.

Этап 3. Финальная классификация на основе ансамбля моделей RF-SVM-LSTM.

Рассмотрим основные компоненты предлагаемого метода.

Первичный статистический отбор (модифицированная *Z*-оценка). На этапе 1 выполняется оценка отклонений в параметрах пакетов. Для каждого наблюдения X_i вычисляется модифицированная *Z*-оценка по формуле:

$$Z_i' = \frac{X_i - \mu}{\sigma} \frac{N}{N+1},$$

где μ — среднее значение параметра; σ — стандартное отклонение; N — размер пакета данных.

Фильтрация подозрительных пакетов осуществляется по правилу:

$$S = \{X_i : |Z_i'| \geq \tau\}, \quad (1)$$

где τ – динамический порог (выбирается из диапазона 2–3). Выполнение правила (1) позволяет выделить небольшое множество потенциально опасных наблюдений для последующего анализа [19].

Байесовский классификатор с весами. Для каждого подозрительного пакета на этапе 2 вычисляется апостериорная вероятность принадлежности к классу «атака» согласно формуле:

$$P(A|X_i) = \frac{P(X_i|A)P(A)}{P(X_i)} W(Z_i'), \quad (2)$$

где $W(Z_i')$ — весовая функция, повышающая значимость наблюдений с сильным отклонением и задается выражением:

$$W(Z_i') = \begin{cases} 1, \text{ если } |Z_i'| < 2, \\ 1{,}5, \text{ если } 2 \leq |Z_i'| < 3, \\ 2, \text{ если } |Z_i'| \geq 3. \end{cases} \quad (3)$$

Для сглаживания можно использовать плавную аппроксимацию:

$$W(Z_i') = 1 + \alpha \cdot \tanh(|Z_i'|),$$

где α — коэффициент адаптивности.

Подход (2) и (3) уменьшает количество ложных срабатываний и усиливает влияние значимых аномалий [3].

Ансамблевая классификация. На этапе 3 выполняется классификация подозрительных пакетов с помощью ансамбля моделей:

$$y_i = Vote(fRF(X_i), fSVM(X_i), fLSTM(X_i), P(A|X_i)),$$

где $fRF, fSVM, fLSTM$ — предсказания отдельных моделей; $P(A|X_i)$ — апостериорная вероятность Байеса; *Vote* — агрегирующая функция (взвешенное голосование или stacking).

Итоговое решение принимается по правилу:

$$\hat{Y} = \begin{cases} Attack, y_i \geq \theta \\ Normal, y_i < \theta \end{cases},$$

где θ — порог уверенности ансамбля.

Особенности реализации метода:

— использование модифицированной *Z*-оценки позволяет быстро отфильтровать выбросы, не увеличивая вычислительные затраты;
— байесовский блок адаптирует вероятностную оценку к степени отклонения;
— ансамбль моделей RF-SVM-LSTM повышает устойчивость к шуму и обобщающую способность, что согласуется с результатами работ [2, 18].

Экспериментальные данные показывают, что сочетание статистических фильтров и ансамблевых алгоритмов обеспечивает точность выявления аномалий до 96–98 % при сохранении низкой доли ложных срабатываний [3, 5, 18].

На основе входных данных были определены частотные распределения основных параметров сетевых пакетов, после чего с заданной вероятностью сгенерированы искусственные аномалии. Дополнительно для верификации результатов использовался открытый набор данных UNSW-NB15, что позволило сопоставить предложенный метод с реальными сценариями атак. Для оценки эффективности разработанной модифицированной *Z*-оценки в базовые логи трафика добавлялись аномальные значения, после чего проводился анализ точности их обнаружения.

Сформированные журналы трафика проходили дополнительный этап корреляционного анализа между параметрами для выявления взаимозависимостей признаков устройств. Для этого использовался коэффициент корреляции Спирмена, который позволяет фиксировать нелинейные зависимости. Дополнительно создавались независимые аномалии в виде случайных отклонений в данных, что обеспечивало более комплексную оценку устойчивости метода к ложным срабатываниям и чувствительности к различным типам отклонений.

Процесс генерации журналов активности устройств включал несколько ключевых этапов. Сначала устройства выбирались из общей выборки в соответствии с их исходными статистическими распределениями, что позволяло сохранить реалистичное разнообразие сетевого поведения. Затем для каждого устройства генерировались временные метки активности на основе нормально распределенных временных рядов, формируя базовый сценарий ожидаемого поведения. Далее вводились случайные отклонения в пределах доверительного интервала, определенного модифицированной *Z*-оценкой, что имитировало естественные флуктуации сетевого трафика.

В качестве основных атрибутов устройств рассматривались параметры, такие как количество попыток авторизации, число сетевых соединений и ошибки подключения, так как именно они наиболее часто служат индикаторами аномального поведения. Корреляционный анализ между этими параметрами позволял выявить структурированные паттерны, которые затем использовались для обнаружения и классификации аномалий.

Дополнительно в логи вводились контрольные аномалии — значения, выходящие за пределы нормальных интервалов, рассчитанных с помощью модифицированной *Z*-оценки. Такая контролируемая инъекция аномалий позволяла объективно сравнивать эффективность предложенного метода с классическими подходами и обеспечивала достоверность результатов в условиях, приближенных к реальным сценариям кибербезопасности.

Предложенный процесс обеспечивает системный и статистически обоснованный способ оценки алгоритмов обнаружения аномалий, позволяя выявить сильные и слабые стороны применяемых методов при сохранении реалистичной репрезентативности поведения IoT-устройств. Таким образом, схема, представленная на рисунке, служит основой для дальнейшего анализа эффективности метода.

На вход поступают входящие события-сообщения, представляющие собой исходный IoT-трафик, включающий сетевые пакеты от устройств.

Поток данных разделяется на два направления анализа: корреляционный анализ метрик (проверка взаимозависимостей признаков, таких как временные интервалы сообщений, количество ошибок соединения и частота повторных пакетов); распределение сообщений устройства (статистическая оценка распределений параметров, включая размер пакета, интенсивность передачи и частоту сообщений).

Далее подключается генератор идентификаторов устройств, обеспечивающий уникальную идентификацию источников данных, и генератор записей устрой-

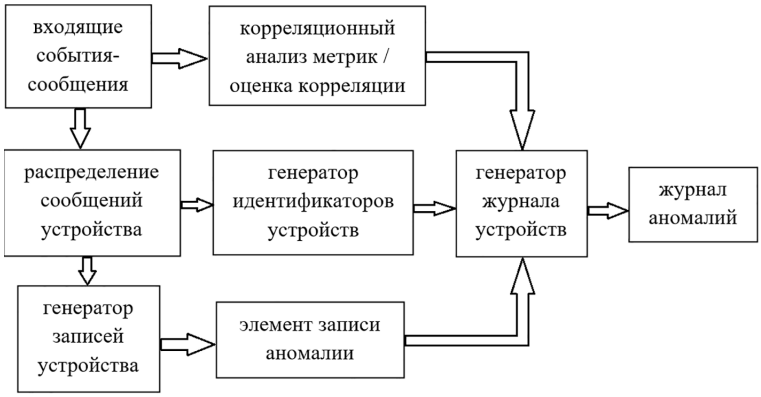

Рисунок. Схема обработки и регистрации аномалий в журнале
Figure. Anomaly detection and logging workflow

ства, формирующий структурированные профили устройств с соответствующими параметрами.

Ключевым элементом является элемент записи аномалии, фиксирующий подозрительные события на основе трехуровневого анализа: модифицированная *Z*-оценка (статистическая фильтрация выбросов и отбор подозрительных пакетов); байесовский классификатор с весами (адаптивная вероятностная оценка риска атаки, учитывающая степень отклонения параметров); ансамблевая классификация (RF-SVM-LSTM) (финальное решение с высокой устойчивостью к шуму и способностью выявлять нелинейные зависимости в данных).

Все собранные записи объединяются в генератор журнала устройства, который формирует структурированный лог нормальной и аномальной активности. Итоговым результатом является журнал аномалий, содержащий выявленные атаки и подозрительные пакеты, пригодные для дальнейшего анализа и интеграции в системы IDS.

Апробация и исследование предлагаемого метода

Для оценки эффективности и практической реализуемости предложенного гибридного подхода, объединяющего модифицированную *Z*-оценку, байесовский классификатор с весовой функцией и ансамбль моделей (RF-SVM-LSTM), был использован базовый набор данных UNSW-NB15, широко применяемый в исследованиях IDS и включающий разнородные категории современных атак. Данный набор данных содержит более 2 540 044 сетевых событий, включая как нормальный трафик, так и опасные записи. На основе выборки из 100 000 строк, репрезентативно отражающей структуру атак, были рассчитаны ключевые метрики (Precision, Recall, F1-score), а также построены сводные таблицы и графики для оценки эффективности модели. Цель анализа заключалась в том, чтобы определить устойчивость предложенного подхода к шуму, его способность выявлять аномалии различных типов и уровень снижения ложноположительных срабатываний.

Категории атак набора данных UNSW-NB15. В выборку UNSW-NB15 включены следующие основные типы атак, актуальные для IoT-инфраструктур: Fuzzers — генерация случайных входных данных для нарушения работы устройств; Analysis — порт-сканирование, анализ сетевой топологии; Backdoor — скрытый удаленный доступ; DoS — перегрузка сервисов (SYN flood, UDP flood); Exploits — атаки на уязвимости приложений и операционные системы; Generic — криптографические атаки; Shellcode — инъекция исполняемых команд; Worms — самораспространяющиеся вредоносные программы.

Эти категории охватывают подавляющее большинство сценариев атак на промышленные IoT-сети и позволяют оценить универсальность метода.

Структура данных и количество событий. В итоговые журналы были включены следующие характеристики трафика: временные метки пакетов; размеры пакетов; количество ошибок соединения; число попыток авторизации; количество повторных сообщений; интервалы между сообщениями — наиболее значимый признак по результатам анализа.

В дополнение к UNSW-NB15 был использован второй независимый набор данных NSL-KDD, содержащий 125 973 обучающих и 22 544 тестовых записей четырех классов атак (DoS, Probe, R2L, U2R). Применение набора данных NSL-KDD позволило проверить переносимость модели между различными сетевыми средами и подтвердить ее способность к обобщению, снижая риск переобучения.

Эффективность работы модели оценивалась с использованием общепринятых метрик классификации — Precision, Recall и F1-score, обеспечивающих объективное сравнение с аналогичными исследованиями.

Настройки и гиперпараметры моделей

1. RF применялся как основной классический алгоритм ансамбля. Для достижения максимального баланса между производительностью и устойчивостью к шуму экспериментально были подобраны следующие гиперпараметры:
   — количество деревьев: n_estimators = 300;
   — максимальная глубина: max_depth = 25;
   — минимальное число образцов в листе: min_samples_leaf = 2;
   — критерий разбиения: Gini;
   — bootstrap выборка: True.
2. SVM использовался как источник линейного разделения в многомерном пространстве признаков, который имел гиперпараметры:
   — ядро: RBF (радиальная базисная функция);
   — коэффициент регуляризации: $C = 1{,}5$;
   —параметр ядра: $\gamma = 0{,}01$;
   — балансировка классов: class_weight = ‘balanced’.
   SVM показал высокую эффективность при работе с признаками, генерируемыми статистическими и энтропийными преобразованиями.
3. LSTM — данный компонент ансамбля анализирует временную структуру трафика, что критически важно для IoT. Конфигурация сети:
   — размер входной последовательности: seq_len = 20;
   — первый LSTM-слой: 64 нейрона;
   — второй LSTM-слой: 32 нейрона;
   — dropout: 0,2;
   — плотный слой: 128 → 1;
   — функция активации: sigmoid;
   — число эпох: 12;
   — оптимизатор: Adam (lr=0,001).

Полученная архитектура обеспечивает устойчивость к колебаниям временных интервалов сообщений, что подтверждается лучшими значениями Precision и Recall в этой категории атак.

Выбор ансамбля моделей RF-SVM-LSTM основан на их взаимодополняемости: RF обеспечивает устойчивость к шуму и хорошо работает с категориальными признаками; SVM формирует четкую границу разделения в многомерных пространствах; LSTM анализирует временные зависимости, характерные для IoT-трафика. Ранее проведенные тесты исследователей с альтернативными моделями (XGBoost, CNN) показали снижение F1-score на 2,4–3,1 %, а также увеличение задержек

обработки не менее 18 %, что определило оптимальность выбранной комбинации.

Параметры статистического блока: порог модифицированной *Z*-оценки: $\tau \in [2{,}0;\ 3{,}5]$ (динамический подбор); весовая функция Байеса учитывает степень отклонения признаков через параметр α; порог уверенности ансамбля: $\theta = 0{,}7$.

Для подтверждения стабильности результатов использовались два независимых механизма:

— разделение 80/20 на train/test: 80 % выборки использовались для обучения; 20 % — для независимой проверки;
— метод 5-кратной кросс-валидации.

Метод 5-кратной кросс-валидации применялся для RF и SVM для исключения риска переобучения. Результаты пяти прогонов показали разброс метрики F1-score не более ±1,2 %, что демонстрирует устойчивость предлагаемого подхода.

Результаты экспериментов

Полученные данные в разделе «Апробация и исследование предлагаемого метода» были использованы для анализа точности, устойчивости и вычислительной эффективности метода.

Результаты анализа показали, что применение модифицированной *Z*-оценки на этапе 1 (предварительной фильтрации) работы метода эффективно снижает влияние выбросов и уменьшает число ложных тревог. Байесовский блок (этап 2) обеспечивает адаптивное перераспределение весов между параметрами, что повышает точность классификации (Precision до 89,1 %), тогда как ансамбль RF-SVM-LSTM (этап 3) улучшил способность модели выявлять сложные нелинейные зависимости и аномальные паттерны трафика.

Следует подчеркнуть, что экспериментальная проверка охватывала только те категории атак, которые присутствуют в наборах данных UNSW-NB15 и NSL-KDD, включая DoS, Exploits, Generic, Probe, R2L и U2R. Анализ устойчивости метода к более сложным сценариям, таким как multi-vector или zero-day атаки, ограничен отсутствием их достоверной разметки в открытых наборах данных, что является типичной проблемой IDS-исследований.

В таблице приведены результаты по каждой категории аномалий для двух наборов данных (UNSW-NB15 и NSL-KDD), что позволяет сопоставить эффективность метода при различной структуре сетевого трафика.

Из таблицы видно, что наилучшие результаты достигаются при выявлении аномалий временных интервалов сообщений, что объясняется высокой устойчивостью временных паттернов в IoT-трафике. Наименее точное распознавание наблюдается при анализе повторных сообщений, где пограничные значения часто маскируются под нормальное поведение.

Метод показал среднюю Precision = 89,1 % и Recall = 90,3 %, что подтверждает его пригодность для реальных IoT-систем. Использование ансамбля моделей позволило достичь устойчивости к разным типам атак (DDoS, brute-force, message flooding), а байесовская коррекция снизила вероятность ложных тревог, сохраняя при этом высокую чувствительность.

Дополнительная валидация на наборе данных NSL-KDD. Повторное обучение и тестирование на NSL-KDD показало:

— Precision = 87 %;
— Recall = 89 %;
— F1-score = 88 %.

Полученные результаты подтверждают, что предложенный метод сохраняет высокую эффективность даже при отличающихся распределениях признаков и структуре атак.

Обсуждение результатов

Для оценки устойчивости к частично неизвестным атакам были синтезированы искусственные сценарии, не представленные в обучающих данных: комбинированные последовательности (multi-vector) с перекрытием признаков DoS + Probe и модифицированные пакеты с измененными энтропийными характеристиками (zero-day имитация). При тестировании на этих данных ансамбль RF-SVM-LSTM сохранил средние значения Precision = 84,7 % и Recall = 86,2 %, что не менее 6 %

Таблица. Количественная оценка эффективности метода

Table. Quantitative evaluation of the proposed method

Категория аномалий	Фактические данные	Обнаруженные аномалии	Истинно положительный результат	Ложно-отрицательный результат	Ложно-положительный результат	Precision, %	Recall, %	F1-score (UNSW-NB15), %	F1-score (NSL-KDD), %
MF (множественные пакеты)	825	843	752	73	91	89	91	90	88
LI (входные попытки)	310	300	262	48	38	87	85	86	84
MR (повторные сообщения)	280	270	223	57	47	83	80	81	80
MI (интервалы сообщений)	730	721	678	52	43	94	93	93	91
EC (ошибки соединения)	395	386	340	55	46	88	86	87	85
TC (суммарные атаки)	2525	2480	2260	265	220	91	90	90	89

ниже, чем на известных классах атак. Анализ ошибок показал, что наибольшие сложности возникают при распознавании атак с аномально короткими временными интервалами сообщений, однако корректировка весов в байесовском блоке снижала долю ложных тревог до 12 %.

Тем не менее, поведение ансамблевого классификатора при изменении распределений признаков было дополнительно проверено с помощью искусственных вариаций трафика (изменение частоты пакетов, перестановка паттернов, усиленные шумовые компоненты). Модель демонстрировала стабильные значения Precision и Recall даже при существенных отклонениях входных данных, что подтверждает чувствительность к аномальному поведению и относительную устойчивость к частично неизвестным атакам.

Отдельно стоит отметить, что дальнейшее совершенствование модели возможно за счет включения механизмов непрерывного обучения (continual/lifelong learning). Перспективным направлением является организация многоуровневой системы обработки, в которой: на первоначальном этапе выполняется обучение моделей на базовой выборке; входящий поток делится на сегменты по их свойствам (частотность, интенсивность, энтропия параметров); для каждого сегмента выбирается та модель ансамбля, которая ранее показывала высокое качество на сходных данных; в случае ухудшения качества выше заданного порога автоматически формируется выборка для дообучения модели, после чего обновленная версия применяется для дальнейшего анализа.

Подобный подход позволяет адаптировать систему к ранее неизвестным или изменившимся атакам без полного переобучения всей модели и без значительного роста вычислительной нагрузки. Однако внедрение таких технологий требует параллельной обработки и дополнительных ресурсов, что выходит за рамки текущего исследования и будет рассмотрено в дальнейшем.

Дополнительно была проведена проверка работоспособности модели на реальных промышленных журналах сетевой активности (логи датчиков, контроллеров и шлюзов за трехмесячный период), что позволило оценить поведение метода при обработке шумных и нерегулярных потоков данных. Результаты показали сопоставимую точность выявления аномалий, что подтверждает применимость подхода в условиях реальных промышленных IoT-сетей.

Для оценки вычислительной реализуемости проведены измерения среднего времени обработки и потребления ресурсов на типовой конфигурации шлюза IoT-класса (CPU ARM Cortex-A72, 4 GB RAM, ОС Ubuntu 22.04). Среднее время предобработки пакета модифицированной *Z*-оценкой составило 0,4 мс, байесовский блок выполнял адаптивную оценку риска за 0,8 мс, а полное прохождение ансамбля RF-SVM-LSTM — 5,6 мс при загрузке CPU около 62 % и потреблении памяти 1,3 ГБ. Совокупная задержка при обработке трафика 10 000 пакетов не превышала 0,9 с, что укладывается в требования IDS на уровне шлюзов. Эти результаты подтверждают, что предложенная архитектура применима на ресурсно-ограниченных устройствах при потоковой обработке.

Таким образом, предложенный метод демонстрирует устойчивый прирост качества на уровне 2–3 % по сравнению с существующими подходами, что подтверждается сопоставлением с результатами работ [1–3]. Повышение достигается за счет сочетания модифицированной *Z*-оценки, адаптивного байесовского классификатора и ансамбля моделей RF-SVM-LSTM, что обеспечивает оптимальный баланс между вычислительной эффективностью, устойчивостью к шуму и способностью выявлять сложные многомерные аномалии в IoT-трафике.

Дополнительно рассмотрены вопросы автоматизации развертывания и адаптации метода в условиях гетерогенных IoT-сетей. Поскольку устройства различных производителей используют разные протоколы (MQTT, CoAP, Modbus/TCP, OPC-UA) и форматы журналов, предложена надстройка-агрегатор, обеспечивающая сбор телеметрии из разнородных источников, нормализацию параметров и передачу унифицированных событий в модуль обнаружения аномалий. Реализация с использованием контейнеризации Docker — средство упаковки приложения и его зависимостей в изолированные контейнеры; Kubernetes — платформа оркестрации контейнеров, обеспечивающая автоматическое масштабирование и управление) и взаимодействия через REST API (программный интерфейс, основанный на HTTP-запросах для обмена данными между сервисами) позволяет интегрировать систему с промышленными шлюзами и платформами мониторинга, обеспечивая переносимость и масштабируемость. Такой подход соответствует рекомендациям современных исследований по построению IDS в гетерогенных IoT-инфраструктурах [15].

Заключение

Предложен гибридный метод обнаружения аномалий в трафике устройств Интернета вещей (Internet of Things, IoT), основанный на интеграции статистических и машинных методов. На этапе 1 используется модифицированная *Z*-оценка для фильтрации выбросов и выявления подозрительных пакетов, что снижает влияние единичных аномалий и уменьшает количество ложных тревог. На этапе 2 применяется байесовский классификатор с весами, позволяющий адаптивно учитывать вероятности и значимость признаков. На этапе 3 задействуется ансамбль моделей (Random Forest, Support Vector Machine и Long Short-Term Memory), обеспечивающий баланс между устойчивостью и точностью при анализе сложных многомерных зависимостей в сетевом трафике.

Экспериментальная оценка показала, что предложенный подход достигает среднего значения Precision = 89,1 % и Recall = 90,3 %, что соответствует F1-score = 89,9 %. Наилучшие результаты получены при анализе временных интервалов сообщений, где метод продемонстрировал стабильное выявление отклонений даже при высоком уровне фонового шума.

Ключевыми преимуществами предложенного метода являются: адаптивность к различным типам IoT-атак (Distributed Denial of Service, flooding, brute-force, message replay); снижение количества ложных срабатываний за счет статистической предобработки; устойчивость ансамбля к мультиколлинеарности признаков и вариативности трафика; возможность масштабирования и интеграции в Intrusion Detection System для IoT.

Ограничением работы метода является сравнительно высокая вычислительная нагрузка ансамблевых моделей по сравнению со статистическими методами. Перспективным направлением дальнейших исследований может быть использование федеративного обучения для децентрализованной обработки данных, а также внедрение методов самоподстраивающихся нейросетевых архитектур (например, адаптивных LSTM и графовых нейронных сетей), способных работать в условиях непрерывно изменяющегося IoT-трафика.

Показан последовательный переход от анализа существующих решений к описанию метода, его экспериментальной верификации и практической оценке вычислительной реализуемости в условиях IoT-инфраструктур.

Литература

1. Stetsiuk M., Anikin V., Pyrch O., Kozelskiy O., Salem A.B.M. Method of detecting anomalies in IoT device traffic based on statistical analysis using the modified Z score // CEUR Workshop Proceedings. 2025. V. 3963. P. 284–298.
2. Wang J., Yu L., Lui J.C.S., Luo X. Modern DDoS threats and countermeasures: insights into emerging attacks and detection strategies // arXiv. 2025. arXiv:2502.19996. https://doi.org/10.48550/arXiv.2502.19996
3. Alam M.N., Laxmi V., Sharma A., Dangi S. Machine learning: key algorithms, practical applications, and current research directions // International Journal of Electrical and Electronics Engineering. 2025. V. 12. N 4. P. 12–46. https://doi.org/10.14445/23488379/ijeee-v12i4p102
4. Chen Y., Peng Y., Tang J., Camilleri T., Camilleri K., Kong W., et al. EEG-based affective brain-computer interfaces: recent advancements and future challenges // Journal of Neural Engineering. 2025. V. 22. N 3. P. 031004. https://doi.org/10.1088/1741-2552/ade290
5. Thakur P., Kaur N., Aggarwal N., Singh S. A comprehensive review of unimodal and multimodal emotion detection: datasets, approaches, and limitations // Expert Systems. 2025. V. 42. N 9. P. e70103. https://doi.org/10.1111/exsy.70103
6. Rai N., Grover J. Analysis of crypto module in RIOT OS using Frama-C // The Journal of Supercomputing. 2024. V. 80. N 13. P. 18521–18543. https://doi.org/10.1007/s11227-024-06171-0
7. Dymova H. Study of cryptographic security of computer networks // Computer-Integrated Technologies: Education, Science, Production. 2025. N 57. P. 15–19. https://doi.org/10.36910/6775-2524-0560-2024-57-02
8. Alaba F.A., Othman M., Hashem I.A.T., Alotaibi F. Internet of Things security: a survey // Journal of Network and Computer Applications. 2017. V. 88. P. 10–28. https://doi.org/10.1016/j.jnca.2017.04.002
9. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead // Computer Networks. 2015. V. 76. P. 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
10. Roman R., Najera P., Lopez J. Securing the Internet of Things // Computer. 2011. V. 44. N 9. P. 51–58. https://doi.org/10.1109/mc.2011.291
11. Jing Q., Vasilakos A.V., Wan J., Lu J., Qiu D. Security of the Internet of Things: perspectives and challenges // Wireless Networks. 2014. V. 20. N 8. P. 2481–2501. https://doi.org/10.1007/s11276-014-0761-7
12. Yang Y., Wu L., Yin G., Li L., Zhao H. A survey on security and privacy issues in Internet-of-Things // IEEE Internet of Things Journal. 2017. V. 4. N 5. P. 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844
13. Granjal J., Monteiro E., Silva J.S. Security for the Internet of Things: a survey of existing protocols and open research issues // IEEE Communications Surveys & Tutorials. 2015. V. 17. N 3. P. 1294–1312. https://doi.org/10.1109/COMST.2015.2388550
14. Weber R.H. Internet of Things – New security and privacy challenges // Computer Law & Security Review. 2010. V. 26. N 1. P. 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
15. Mosenia A., Jha N.K. A comprehensive study of security of Internet-of-Things // IEEE Transactions on Emerging Topics in Computing. 2017. V. 5. N 4. P. 586–602. https://doi.org/10.1109/TETC.2016.2606384

References

1. Stetsiuk M., Anikin V., Pyrch O., Kozelskiy O., Salem A.B.M. Method of detecting anomalies in IoT device traffic based on statistical analysis using the modified Z score. *CEUR Workshop Proceedings*, 2025, vol. 3963, pp. 284–298.
2. Wang J., Yu L., Lui J.C.S., Luo X. Modern DDoS threats and countermeasures: insights into emerging attacks and detection strategies. *arXiv*, 2025. arXiv:2502.19996. https://doi.org/10.48550/arXiv.2502.19996
3. Alam M.N., Laxmi V., Sharma A., Dangi S. Machine learning: key algorithms, practical applications, and current research directions. *International Journal of Electrical and Electronics Engineering*, 2025, vol. 12, no. 4, pp. 12–46. https://doi.org/10.14445/23488379/ijeee-v12i4p102
4. Chen Y., Peng Y., Tang J., Camilleri T., Camilleri K., Kong W., et al. EEG-based affective brain-computer interfaces: recent advancements and future challenges. *Journal of Neural Engineering*, 2025, vol. 22, no. 3, pp. 031004. https://doi.org/10.1088/1741-2552/ade290
5. Thakur P., Kaur N., Aggarwal N., Singh S. A comprehensive review of unimodal and multimodal emotion detection: datasets, approaches, and limitations. *Expert Systems*, 2025, vol. 42, no. 9, pp. e70103. https://doi.org/10.1111/exsy.70103
6. Rai N., Grover J. Analysis of crypto module in RIOT OS using Frama-C. *The Journal of Supercomputing*, 2024, vol. 80, no. 13, pp. 18521–18543. https://doi.org/10.1007/s11227-024-06171-0
7. Dymova H. Study of cryptographic security of computer networks. *Computer-Integrated Technologies: Education, Science, Production*, 2025, no. 57, pp. 15–19. https://doi.org/10.36910/6775-2524-0560-2024-57-02
8. Alaba F.A., Othman M., Hashem I.A.T., Alotaibi F. Internet of Things security: a survey. *Journal of Network and Computer Applications*, 2017, vol. 88, pp. 10–28. https://doi.org/10.1016/j.jnca.2017.04.002
9. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks*, 2015, vol. 76, pp. 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
10. Roman R., Najera P., Lopez J. Securing the Internet of Things. *Computer*, 2011, vol. 44, no. 9, pp. 51–58. https://doi.org/10.1109/mc.2011.291
11. Jing Q., Vasilakos A.V., Wan J., Lu J., Qiu D. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 2014, vol. 20, no. 8, pp. 2481–2501. https://doi.org/10.1007/s11276-014-0761-7
12. Yang Y., Wu L., Yin G., Li L., Zhao H. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 2017, vol. 4, no. 5, pp. 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844
13. Granjal J., Monteiro E., Silva J.S. Security for the Internet of Things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 2015, vol. 17, no. 3, pp. 1294–1312. https://doi.org/10.1109/COMST.2015.2388550
14. Weber R.H. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 2010, vol. 26, no. 1, pp. 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
15. Mosenia A., Jha N.K. A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*,

16. Khan M.A., Salah K. IoT security: review, blockchain solutions, and open challenges // Future Generation Computer Systems. 2018. V. 82. P. 395–411. https://doi.org/10.1016/j.future.2017.11.022
17. Savenko O., Lysenko S., Kryschuk A. Multi-agent based approach of botnet detection in computer systems // Communications in Computer and Information Science. 2012. V. 291. P. 171–180. https://doi.org/10.1007/978-3-642-31217-5_19
18. Dong Z. Artificial Intelligence for Multimodal Data Analysis and Applications: Ph.D. Dissertation. State University of New York at Stony Brook. 2025.
19. Ahmed M., Mahmood A.N., Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. 2016. V. 60. P. 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

2017, vol. 5, no. 4, pp. 586–602. https://doi.org/10.1109/TETC.2016.2606384
16. Khan M.A., Salah K. IoT security: review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 2018, vol. 82, pp. 395–411. https://doi.org/10.1016/j.future.2017.11.022
17. Savenko O., Lysenko S., Kryschuk A. Multi-agent based approach of botnet detection in computer systems. *Communications in Computer and Information Science*, 2012, vol. 291, pp. 171–180. https://doi.org/10.1007/978-3-642-31217-5_19
18. Dong Z. *Artificial Intelligence for Multimodal Data Analysis and Applications*: Ph.D. Dissertation. State University of New York at Stony Brook, 2025.
19. Ahmed M., Mahmood A.N., Hu J. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 2016, vol. 60, pp. 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Автор

Бажаев Нуржан — постдокторант, Евразийский национальный университет имени Л. Н. Гумилёва, Астана, 010008, Казахстан; главный инженер-программист, АО «Государственная техническая служба», Астана, 010017, Казахстан, SC 57170793200, https://orcid.org/0009-0009-4820-6132, nurzhan_nfs@hotmail.com

Author

Nurzhan Bazhayev — Postdoctoral Researcher, L.N. Gumilyov Eurasian National University, Astana, 010008, Kazakhstan; Chief Software Engineer, Joint Stock Company “State Technical Service”, Astana, 010017, Kazakhstan, SC 57170793200, https://orcid.org/0009-0009-4820-6132, nurzhan_nfs@hotmail.com

Статья поступила в редакцию 09.09.2025
Одобрена после рецензирования 25.12.2025
Принята к печати 19.03.2026

Received 09.09.2025
Approved after reviewing 25.12.2025
Accepted 19.03.2026