НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2026 Том 26 № 1 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2026 Vol. 26 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2026-26-1-94-103
УДК 004.8:004.485:004.421

Ресурсно-эффективное обнаружение сетевых атак с использованием селективной State Space Models

Егор Олегович Здорников[1]✉, Илья Юрьевич Попов[2]

[1,2] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] e.zdornickow2012@yandex.ru✉, https://orcid.org/0009-0009-0154-5153
[2] ilyapopov27@gmail.com, https://orcid.org/0000-0002-6407-7934

Аннотация

Введение. Распространение уязвимых устройств интернет вещей приводит к увеличению количество атак на такие устройства и требует разработки точных и ресурсно-эффективных средств их выявления. Существующие модели системы обнаружения вторжений плохо адаптируются к разным наборам данных. Представлено решение этой проблемы на основе архитектуры Edge-Mamba — «легковесной модели» на базе линейно-временной селективной State Space-архитектуры. Приведена оценка возможности переносить модели между гетерогенными наборами данных и обеспечивать их работу на конечных устройствах в реальном времени. **Метод.** Предложенная модель основана на селективной State Space-архитектуре и обеспечивает линейную сложность обработки последовательностей. Адаптация модели для анализа сетевого трафика происходит путем кодирования 74 признаков и за счет применения двух блоков модели пространства состояний. Такое построение позволяет снизить вычислительные затраты и одновременно сохранить высокую точность классификации атак. **Основные результаты.** Эксперименты выполнены на современных наборах данных CICIDS-2017, TII-SSRC-23. Показано, что архитектура Edge-Mamba достигает на наборе данных TII-SSRC-23 точность 99 % при задержке 0,15 мс, а на наборе данных CICIDS-2017 — 98 % при задержке 2,4 мс. При переносе модели с одного набора данных на другой без дообучения точность классификации составляет 65 %, а дообучение (fine-tuning) на 10 % целевого набора повышает точность до 99 % без увеличения времени классификации. **Обсуждение.** Таким образом, предложенная модель демонстрирует сопоставимую или более высокую точность по сравнению с существующими подходами. При многоклассовой классификации архитектура Edge-Mamba превзошла CNN-BiLSTM и Transformer на 1–3 % по величине macro-F1, сохраняя меньшую задержку. Модель сохраняет эффективность работы на ресурсно-ограниченных устройствах. Представленная модель сочетает точность и возможность переноса модели на другие наборы данных, что делает ее применимой для систем обнаружения вторжений на сетевых шлюзах, хабах интернет вещей и в контейнеризированной инфраструктуре.

Ключевые слова

intrusion-detection, Mamba, DDoS, CICIDS-2017, TII-SSRC-23, IDS, кросс-обучение, fine-tuning, конечные устройства

Благодарности

Персональная благодарность Дарье Лоза за ее вклад в исследование.

Ссылка для цитирования: Здорников Е.О., Попов И.Ю. Ресурсно-эффективное обнаружение сетевых атак с использованием селективной State Space Models // Научно-технический вестник информационных технологий, механики и оптики. 2026. Т. 26, № 1. С. 94–103. doi: 10.17586/2226-1494-2026-26-1-94-103

Resource-efficient network attack detection using selective State Space Models

Egor O. Zdornikov[1]✉, Ilya Yu. Popov[2]

[1,2] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] e.zdornickow2012@yandex.ru✉, https://orcid.org/0009-0009-0154-5153

[2] ilyapopov27@gmail.com, https://orcid.org/0000-0002-6407-7934

Abstract

The spread of vulnerable Internet of Things devices leads to an increase in the number of attacks on them, which requires the development of accurate and resource-efficient detection methods. Existing Intrusion Detection System models adapt poorly to different datasets. This paper proposes a solution to this problem based on the Edge-Mamba architecture — a "lightweight model" (distilled models) built on a linear-time selective State Space architecture. An evaluation is provided of the ability to transfer models across heterogeneous datasets and ensure their operation on end devices in real time. The proposed model is based on a selective State Space architecture and provides linear complexity for sequence processing. Adaptation of the model for network traffic analysis is achieved through the encoding of 74 features and the application of two State Space Model blocks. This design reduces computational costs while maintaining high accuracy in attack classification. Experiments were conducted on modern datasets CICIDS-2017 and TII-SSRC-23. The results demonstrate that Edge-Mamba achieves an accuracy of 99 % with a latency of 0.15 ms on the TII-SSRC-23 dataset, and an accuracy of 98 % with a latency of 2.4 ms on the CICIDS-2017 dataset. When transferring the model from one dataset to another without additional training, the classification accuracy drops to 65 %; however, fine-tuning on 10 % of the target dataset increases the accuracy to 99 % without any increase in classification latency. Thus, the proposed model demonstrates comparable or superior accuracy relative to existing approaches. In multiclass classification, the Edge-Mamba model outperforms CNN-BiLSTM and Transformer by 1–3 % in terms of macro-F1 score while maintaining lower latency. The model preserves its efficiency on resource-constrained devices. Therefore, the proposed approach combines high accuracy with transferability across datasets, making it applicable for Intrusion Detection System deployment on network gateways, Internet of Things hubs, and containerized infrastructures.

Keywords

intrusion-detection, Mamba, DDoS, CICIDS-2017, TII-SSRC-23, IDS, cross-dataset transfer learning, fine-tuning, edge-computing

Acknowledgements

Personal gratitude to Darya Loza for her contribution to this research.

For citation: Zdornikov E.O., Popov I.Yu. Resource-efficient network attack detection using selective State Space Models. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2026, vol. 26, no. 1, pp. 94–103 (in Russian). doi: 10.17586/2226-1494-2026-26-1-94-103

Введение

Количество кибератак каждый год увеличивается, и они становятся более вариативными. Увеличение числа устройств, подключенных к сети Интернет, упрощает проведение крупных атак типа отказа в обслуживании (Denial of Service, DoS), что приносит прямо или косвенно огромные убытки физическим лицам и организациям. Одним из факторов роста числа атак стало увеличение рынка IoT-устройств (Internet of Things) и их уязвимостей [1]. В 2025 году компания Cloudflare (США) сообщила о самой крупной атаке за последнее время с помощью ботнета Mirai. Злоумышленники использовали более 13 тыс. IoT-устройств и на пике атаки был сгенерирован трафик объемом 5,6 Тбит/с UDP (User Datagram Protocol). Кроме того, частота ежедневных атак типа распределенного отказа в обслуживании (Distributed Denial of Service, DDoS) растет из года в год. Для выполнения атаки DoS могут применяться рассылки пакетов TCP (Transmission Control Protocol), UDP, ICMP (Internet Control Message Protocol), но чаще всего используются HTTP (Hypertext Transfer Protocol) или HTTPS (Hypertext Transfer Protocol Secure) протоколы [2].

Алгоритмы машинного обучения дают возможность обнаруживать ранее не наблюдаемые атаки в отличие от стандартных систем обнаружения или предотвращения вторжений, большинство из которых в значительной степени зависят от заранее определенных правил (сигнатур) и практически не способны распознавать ранее не встречающиеся атаки [3]. Процесс поддержки актуальной базы данных сигнатур ресурсоемкий и должен успевать за тенденциями атак. Машинное обучение уже давно применяется в системах обнаружения вторжений (Intrusion Detection Systems, IDS) и наиболее популярными имплементациями являются: наивный байесовский классификатор, алгоритм «деревья решений», метод ближайших соседей (*k*-NN), метод опорных векторов и др. [4]. Подходы на основе деревьев решений и их ансамблей показывают хорошие результаты на популярных наборах данных, таких как KDD Cup 99 и NSL-KDD, обеспечивая точность 99 % [5], но при этом показывают большое количество ложных срабатываний.

Вместе с тем на более современных наборах данных, таких как UNSW-NB15, точность может падать до 90 %. Современные системы обнаружения и реагирования на сетевые инциденты (Network Detection and Response) активно используют глубокое обучение и позволяют обнаруживать гораздо сложные атаки и совместно с инструментами автоматизированного реагирования, оперативно обрабатывать инциденты [6].

Обзор литературы

Опубликовано большое количество работ, посвященных распознаванию вредоносной активности пу-

тем анализа сетевого трафика с помощью алгоритмов машинного обучения. Для обучения и тестирования моделей машинного обучения могут использоваться как собственные данные, так и публичные наборы данных. Новые наборы данных для обучения становятся более приближенными к реальным атакам, а обученные на них модели теряют в точности по сравнению с моделями, обученными на старых наборах данных. Например, на KDD-99 многие модели достигали почти 99–100 % точность, но на NSL-KDD показатель точности был меньше. UNSW-NB15 и CIC-IDS2017/2019 в связи с их схожестью с настоящими атаками и разнообразием позволяют получить точность порядка 90–99 %.

В работах [5, 7, 8] рассмотрены методы машинного обучения, применяемые для классификации вредоносного трафика на основе наборов данных KDD-99 и его улучшенной версии NSL-KDD. Лучший результат показывает модель на основе алгоритма «деревья решений» или случайного леса. В [9, 10] выполнен анализ эффективности различных алгоритмов машинного обучения, но дополнительно использован современный набор данных UNSW-NB15 для более достоверных результатов.

В работе [11] приведено сравнение алгоритмов: наивный Байес, решающие деревья, случайный лес, XGBoost, DNN, Transformer и большие языковые модели (Large Language Models, LLM). Наилучшие результаты показали Transformer и GPT-4o. Обученная модель на базе архитектуры LLM в режиме few-shot смогла значительно повысить точность без дообучения на большом наборе данных [11]. Ключевыми метриками оценки модели являются точность обнаружения, скорость работы модели и устойчивость к атакам «нулевого дня» [12]. В табл. 1 представлен обзор работ сравнения алгоритмов.

На сегодняшний день существует большое количество наборов данных, что дает преимущество исследователям и компаниям для обучения собственных моделей обнаружения атак. Всего насчитывается более 20 наборов данных сетевого трафика разного времени создания и объема. Для объективной оценки моделей исследователи улучшают наборы данных, используя реальный трафик или синтетически воспроизводят атаки на инфраструктуру с помощью новых методов. В последние два года опубликованы [25, 26] специализированные наборы данных под IoV/IoMT (CICIoV2024, CICIoMT2024) и временные ряды сетевых потоков (time-series NetFlow, CESNET-TimeSeries24), что актуализирует перенос моделей на отраслевые сегменты.

Несмотря на рост точности моделей для обнаружения атак, остаются нерешенными проблемы обобщения между наборами данных, adversarial-атак, развертывания на конечных устройствах и обнаружения атак «нулевого дня». В известных научных работах в основном рассмотрены модели, обученные на наборах данных, которым уже более 10 лет, таких как NSL-KDD, что может приводить к ошибочным выводам из-за появления новых способов атак.

Целью настоящей работы является оценка переносимости модели линейно-временной архитектуры Mamba между гетерогенными наборами данных и проверка ее применимости для обнаружения атак в реальном времени на ресурсно-ограниченных периферийных устройствах. Предлагаемая модель ориентирована на работу на уровне периферийных сетевых шлюзов и IoT-хабов, что позволяет локально обрабатывать трафик и снизить задержки при обнаружении угроз. Также данную модель можно использовать на обычных серверах в контейнеризированной среде (Docker, LXC, Podman), чтобы анализировать отдельные сегменты корпоративной сети или сервисов.

Описание предлагаемого решения

Описание модели Mamba. Mamba — линейно-временная селективная модель состояний. Каждый вычислительный блок реализует селективную модель и использует представление чисел с плавающей точкой одинарной точности (32-битное представление, IEEE

Таблица 1. Сравнительный обзор моделей и алгоритмов для классификации сетевого трафика
Table 1. Comparative overview of models and algorithms for network traffic classification

Ссылка на источник	Алгоритмы/Модель	Наборы данных
[13]	NetMamba (State Space Model)	ISCXVPN2016, CICIoT2022, USTC-TFC2016
[14]	ET-Mamba	USTC-TFC2016, ISCX-VPN2016, ISCX-Tor2016
[15]	Взвешенный *k*-NN с адаптивным выбором признаков	Набор данных зашифрованного трафика, разработанный в [15]
[16]	Adversarial Autoencoder + Deep Clustering (DC-CAAE)	USTC-TFC2016
[17]	Graph Neural Network (CGNN)	Набор данных, разработанный в работе [17]
[18]	CNN + Autoencoder	ISCX VPN-nonVPN
[19]	Transformer (BERT-подобная модель)	ISCX-Tor, ISCX-VPN-Service, CSTNET-TLS 1.3
[20]	Глубокое обучение + обучение с подкреплением	CTU-Mix-Captures
[21]	XGBoost + SHAP (Explainable AI)	CTU-13, набор данных, разработанный в [21]
[22]	CTC model + IIFS-MC	NSL-KDD, ISCXIDS2012, CICIDS2017
[23]	Flow-based Node Graph Neural Network (FN-GNN)	CICIDS-2017, UNSW-NB15
[24]	Robust Adaptive Graph Neural Network (RAGN)	CICIDS-2017, UNSW-NB15

754[1]). Переход на более компактные форматы (8- или 16-битное квантование) для рекуррентного скалярного ядра вызывает заметную деградацию качества классификации, поэтому сохранен формат float32.

Для дискретной последовательности признаков u_t динамика описывается уравнениями:

$$x_{t+1} = \mathbf{A}x_t + \mathbf{B}u_t,$$
$$y_t = \mathbf{C}x_t + \mathbf{D}u_t,$$

где $x_{t+1} = R^d$ — скрытое состояние внутреннего пространства модели размерностью d (d — число скрытых состояний; u_t — входная переменная признаков сетевого пакета или потока на шаге t; y_t — выход модели (предсказанный класс); **A**, **B**, **C**, **D** — обучаемые матрицы (в Mamba они диагональны и параметризуются через экспоненты, что упрощает вычисления).

В модели Mamba матрица **A** диагональна:

$$\mathbf{A} = diag(\exp(\mathbf{a})),$$

где $\mathbf{a} \in R^d$ — вектор обучаемых параметров, определяющий диагональные элементы матрицы состояния **A**. Это гарантирует экспоненциальную устойчивость:

$$||e^{(\mathbf{A}t)}|| \le e^{(-\alpha t)}, \alpha = \min_i e^{(\alpha_i)} > 0,$$

где $\alpha > 0$ — коэффициент экспоненциальной устойчивости модели.

Для равномерного шага дискретизации Δ получаем:

$$x_{k+1} = e^{\mathbf{A}\Delta}x_k + (\mathbf{A}^{-1}(e^{\mathbf{A}\Delta} - \mathbf{I}))\mathbf{B}u_k = \tilde{\mathbf{A}}x_k + \tilde{\mathbf{B}}u_k,$$
$$y_k = \mathbf{C}x_k + \mathbf{D}u_k,$$

где k — номер дискретного шага после разбиения временной шкалы на равномерные интервалы Δ; **A** и **B** вычисляются аналитически, что исключает численные ошибки интеграции. $\tilde{\mathbf{A}}$ и $\tilde{\mathbf{B}}$ — дискретизированные матрицы состояний, полученные из $e^{\mathbf{A}\Delta}$ и $e^{\mathbf{B}\Delta}$. Таким образом, переменные x_k, u_k, y_k описывают дискретизированные значения состояний и входов модели на каждом шаге, **I** — единичная матрица соответствующей размерности.

Ключевой элемент — селективное сканирование: при обучении вычисляется свертка по всему времени, но на выводе выполняется потоковое сканирование с требуемой памятью $O(1)$. Благодаря этому сложность по длине последовательности линейная, а задержка постоянная. Пусть $K = \{K_0, \ldots, K_{L-1}\}$ — импульсная характеристика, получаемая из $\tilde{\mathbf{A}}$, $\tilde{\mathbf{B}}$; z_t — промежуточный результат после свертки с импульсной характеристикой, тогда свертка «полная»:

$$z_t = \sum_{i=0}^{t} K_{t-i}u_i.$$

Алгоритм селективного сканирования поддерживает рекурренту:

$$s_{t+1} = \tilde{\mathbf{A}}u_t + \tilde{\mathbf{B}}u_t,\ z_t = \mathbf{C}s_t,$$

где s_t — рекуррентное состояние для селективного сканирования, что дает сложность $O(T)$ и память $O(d)$. Функция потерь (кросс-энтропия с весами классов) по параметрам модели вычисляется как:

$$\mathcal{L} = \frac{1}{N}\sum_{k=1}^{N}(f_\theta(X_k), y_k),$$

производные по параметрам State Space-архитектуры вычисляются методом обратного распространения ошибки во времени (Backpropagation Through Time), широко используемого для обучения рекуррентных нейронных сетей [27]

$$\frac{\partial \mathcal{L}}{\partial \mathbf{A}} = \sum_t \left(\Lambda_t \frac{\partial \tilde{\mathbf{A}}}{\partial \mathbf{A}} S_{t-1}\right), \Lambda_t = \frac{\partial \mathcal{L}}{S_t},$$

где Λ_t — градиент функции потерь по состоянию на шаге t. Диагональная структура **A** упрощает $\partial\tilde{\mathbf{A}}/\partial\mathbf{A}$ до поэлементных операций. Для функции потерь и взвешивания классов используется кросс-энтропия с инверсно-частотными весами, что компенсирует дисбаланс выборки:

$$L = -\frac{1}{N}\sum_{i=1}^{N} w_{y_i}\log(softmax(y)_{y_i}),$$

где w_y — вес класса, рассчитанный по инверсно-частотной схеме:

$$w_y = \frac{N}{c_n^k}.$$

Предлагаемый метод: архитектура Edge-Mamba. Для достижения поставленной цели была разработана и протестирована легковесная архитектура Edge-Mamba, включающая два блока Mamba, которые позволяют увеличить точность модели. Количество Mamba блоков выбрано на основе абляционного анализа. При использовании одного блока происходит снижение точности примерно на 2 %, а при трех блоках качество улучшается незначительно (менее 0,2 %) при заметном росте времени инференса (на 25 %) и потребления памяти (на 28 %). Таким образом, два блока обеспечивают оптимальный баланс между точностью и вычислительными затратами, что критично для применения на периферийных устройствах. Схема предлагаемой архитектуры показана на рис. 1.

Edge-Mamba разработана на основе оригинальной модели Mamba [28], но адаптирована для решения задачи анализа сетевого трафика. В частности, добавлены входной блок (Embedding), специальные слои нормализации (LayerNorm) между стадиями и оптимизирована глубина. Многократное использование линейной нормализации (LayerNorm) предназначено стабилизировать распределение признаков на разных уровнях глубины сети. Без нормализации при обучении наблюдается быстрое накопление градиентов и падение точности на 2–3 %. Использование Sigmoid Linear Unit (SiLU) в качестве функции активации выбрано для по-

[1] IEEE Standard for Floating-Point Arithmetic, IEEE Std 754-2019, Institute of Electrical and Electronics Engineers.

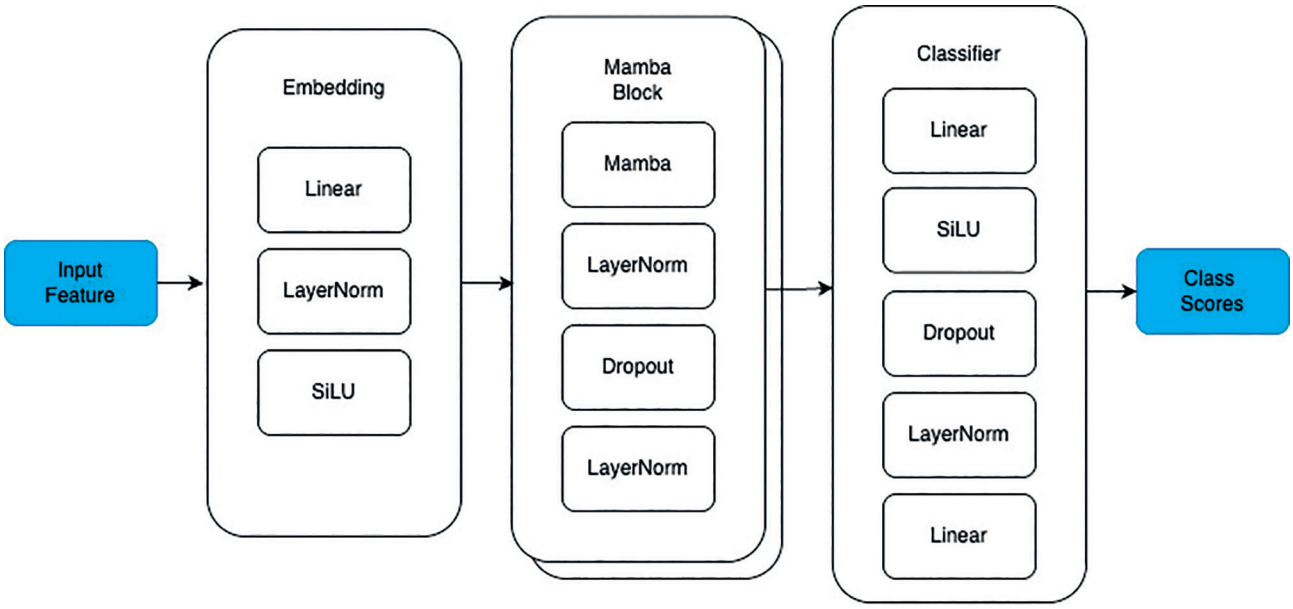

Рис. 1. Архитектура Edge-Mamba
Fig. 1. Edge-Mamba architecture

вышения гладкости градиентов и лучшей адаптивности по сравнению с Rectified Linear Unit.

Архитектура модели Edge-Mamba представляет собой последовательность трех основных блоков: входного преобразования (Embedding), селективного блока (Mamba Block) и классификатора (Classifier). Входной слой (Input Layer), принимающий входной вектор признаков сетевого пакета (Input Feature) сетевого трафика обрабатывается линейным слоем (Linear) и функцией активации (SiLU), после чего нормализуется и подается в рекуррентный слой (Dropout). Mamba Block — модуль селективной State Space-архитектуры обрабатывает последовательности признаков во времени с линейной сложностью. Classifier реализован в виде полносвязного линейного слоя (Linear), проецирующего выходное состояние в пространство классов. На выходе (Class Scores) используется классификационный блок с Dropout-регуляризацией и линейным слоем, преобразующим представление в распределение вероятностей классов.

Экспериментальное исследование предлагаемой модели данных

Наборы данных. Эксперименты проведены на рабочей станции AMD Ryzen 7 5800U, NVIDIA GeForce GTX 1050 Ti, 16 ГБ оперативной памяти. Для обучения и тестирования выбраны два публичных современных набора данных: CICIDS-2017[1] и TII-SSRC-23[2]. CICIDS-2017 собран в 2017 году на стенде с реальным клиентами и серверами. Всего было собрано около 2,8 млн пакетов за 5 рабочих дней. Этот набор данных охватывает 7 групп сценариев атак: атаки перебором (Brute Force), Heartbleed (уязвимость в OpenSSL), ботнет-атаки (Botnet), атаки, DoS, DDoS, Web-атаки и атаки внедрения (Infiltration), а также обычный легальный трафик. Набор данных TII-SSRC-23 представлен в 2023 году, который был собран исследовательской группой Technology Innovation Institute (Абу-Даби, Объединенные Арабские Эмираты). Собранный набор состоит из 6,4 млн записей трафика из 10 типов атак, производных от ботнетов BASHLITE и Mirai. Данные были предварительно обработаны, удалены сильно коррелирующие признаки и приведены к единому количеству признаков равному 74.

Бинарная классификация внутри одного и между разными наборами данных. Проведена серия экспериментов бинарной классификации сетевого трафика с использованием наборов данных: CICIDS-2017 и TII-SSRC-23. В обоих случаях модель обучалась и тестировалась на соответствующем наборе данных по оценке внутри наборов данных. В табл. 2 приведены результаты модели при обучении и тестировании двух наборов данных.

Квантование для библиотеки Mamba на данный момент не поддерживается, но при попытке квантования Linear-слоев это не приводит к значимому уменьшению времени инференса на тестовой выборке.

Модель, обученная на TII-SSRC-23, при тестировании на CICIDS-2017 показывает плохие результаты из-за сильного распределительного сдвига (домашняя IoT-сеть ↔ корпоративный офис). Небольшое дообучение модели — на 10 % CICIDS-2017 данных восстанавливает точность до 99 %, практически совпадая с тестом первоначальной модели. Аналогичная ситуация наблюдается при обучении на CICIDS-2017 и тестировании на TII-SSRC-23. В табл. 3 представлены результаты кросс-обучения.

[1] [Электронный ресурс]. Режим доступа: https://unb.ca/cic/datasets/ids-2017.html (дата обращения: 02.12.2025).

[2] [Электронный ресурс]. Режим доступа: https://kaggle.com/datasets/daniaherzalla/tii-ssrc-23 (дата обращения: 02.12.2025).

Таблица 2. Результаты классификации и время предсказания модели
Table 2. Classification results and model inference time

Набор данных	Точность, %	FAR (False Acceptance Rate), %	FRR (False Rejection Rate), %	Среднее время на образец, с
CICIDS-2017	98,60	1,99	1,40	0,002387
TII-SSRC-23	99,52	1,84	1,07	0,000153

Таблица 3. Переносимость модели между наборами данных
Table 3. Model transferability between datasets

Сценарий	Обучение	Время, с	Тест	Точность, %
T → C	TII-SSRC-23	0,00018	CICIDS-2017	71,48
T → C (+10 % FT)	TII-SSRC-23 + fine-tuning 200 тыс. CICIDS-строк	0,00019	CICIDS-2017	98,99

Примечание: T — TII-SSRC-23; C — CICIDS-2017; FT — fine-tuning.

Использованное в эксперименте дообучение не является новым подходом, а представляет собой адаптацию предварительно обученной модели на ограниченной выборке целевого набора данных. Это позволяет быстро увеличить точность при переносе между гетерогенными наборами данных без полного обучения. Выбор долей дообучения обусловлен результатами предварительных экспериментов (рис. 2), где можно увидеть, что прирост по точности невелик после определенного процента подмешивания данных. Дополнительно проведен эксперимент с объединением наборов данных, который показал небольшой прирост точности на 1 %, но при этом увеличил время обучения примерно в 2,5 раза.

Для сравнения была рассмотрена модель Mamba-ECANet [29], реализующая гибридную архитектуру на основе State Space-архитектуры и модуля внимания к каналу (Efficient Channel Attention, ECA). На наборе данных CICIDS-2017 она продемонстрировала точность 97,64 %, уступая Edge-Mamba в настоящей работе (98,60 %) при значительно большей вычислительной нагрузке.

Многоклассовая классификация. При мультиклассовой классификации, проведенной на одном и том же наборе данных, модель на основе Mamba демонстрирует отличную точность, превосходя результаты на архитектуре Transformer [19] на 0,5–1 % при меньшем времени распознавания 0,146 мс на один образец. Edge-Mamba также опережает модель, рассматриваемую в работе [30] на 1,8 %. Результаты тестирования модели на наборе данных TII-SSRC-23 приведены в табл. 4.

Аналогично для набора данных CICIDS-2017 модель демонстрирует высокую точность. Несмотря на большую вариативность атак и наличие редких сценариев (например, Heartbleed и атаки внедрения), модель успешно классифицирует большинство категорий, достигая точности выше 0,99 на основных сценариях (DoS, DDoS, сканирование портов), которые присутствуют в TII-SSRC-23. Итоговые метрики для многоклассовой классификации на этом наборе данных приведены в табл. 5.

Для лучшей интерпретируемости моделей стоит обратиться к SHAP-анализу (SHapley Additive

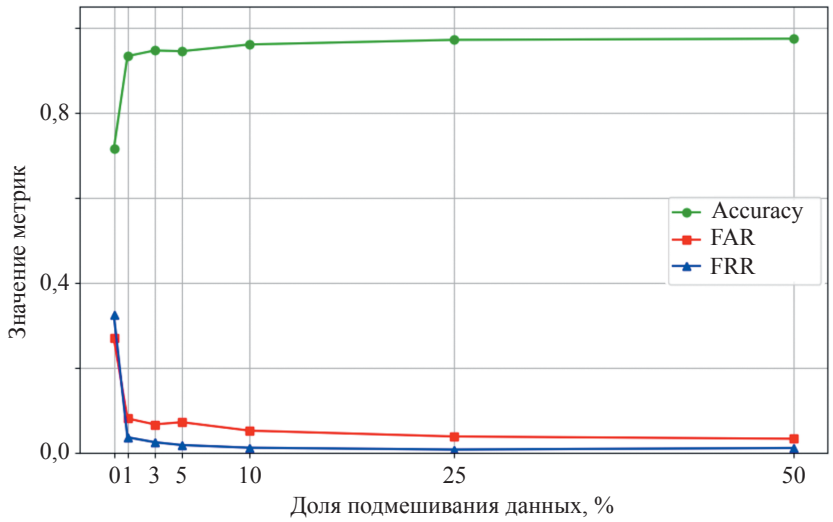

Рис. 2. Влияние дообучения на точность, FAR, FRR в сценарии T → C
Fig. 2. Impact of fine-tuning on accuracy, FAR, FRR in the T → C scenario

Таблица 4. Итоговые метрики на наборе данных TII-SSRC-23
Table 4. Final metrics on the TII-SSRC-23 dataset

Сценарий атаки	Всего в тесте	Верно распознано	FAR, %	FRR, %	Точность, %
Атаки DoS	10 000	9940	0,08	0,50	99,4
Сбор информации	4000	3992	0,17	0,28	99,8
Ботнет-атаки (Mirai)	4000	3962	0,34	1,27	99,0
Атаки перебором	3900	3877	0,23	0,55	99,4
Легальный трафик	800	792	0,03	0,50	99,0

Таблица 5. Итоговые метрики на наборе данных CICIDS-2017
Table 5. Final metrics on the CICIDS-2017 dataset

Сценарий атаки	Всего в тесте	Верно распознано	FAR, %	FRR, %	Точность, %
Легальный трафик	15 000	14 850	0,58	2,05	99,0
Атаки DoS	10 000	9880	0,55	1,55	98,8
DDoS	9000	8982	0,08	1	99,8
Сканирование портов	6000	5988	0,37	0,20	99,8
Атаки перебором	4000	3988	0,57	0,29	99,7
Веб-атаки	980	912	0,80	0,30	93,1
Ботнет-атаки	200	200	0	0	100
Атаки внедрения	15	10	0,01	50	66,6
Атаки Heartbleed	5	5	0	0	100

exPlanations), чтобы выявить наиболее важные признаки, влияющие на определение классов сценариев. Приведем краткий анализ пяти важнейших признаков в порядке убывания: средний размер сегмента в прямом направлении (от источника к получателю); средний размер сегмента в обратном направлении; начальный размер окна TCP в прямом направлении; общее количество данных, переданных от источника к получателю в рамках одного TCP-соединения; количество установленных флагов подтверждения.

На практике дообучение (fine-tuning) модели выполняется на данных, собираемых непосредственно на сетевом шлюзе или IoT-хабе. В таком сценарии используется небольшой процент реального трафика (1–5 % за период), который размечается полуавтоматическими средствами (IDS-алгоритмы+экспертная валидация) и используется для обновления весов модели. Возможно применение федеративного обучения, когда локальные обновления выполняются только на периферийных устройствах без передачи исходных данных.

Для оценки производительности в реальном времени обученная модель была развернута на Raspberry Pi 4. Среднее время классификации на один пакет доходило до 3,2 мс.

Обсуждение

Полученные результаты демонстрируют, что архитектура Edge-Mamba обладает рядом важных свойств, отвечающих актуальным требованиям к системам обнаружения атак на уровне конечных устройств. Разработанная архитектуры показала высокую точность на современных наборах данных TII-SSRC-23 и CICIDS-2017, что подтверждает ее применимость к актуальным сценариям киберугроз. В многоклассовой классификации Edge-Mamba превзошла архитектуры CNN-BiLSTM и Transformer на 1–3 %, при этом сохранив низкое время классификации (менее 0,2 мс). Это свидетельствует об эффективности как в точности, так и в ресурсоемкости, что критично для IoT-среды и ограниченных вычислительных ресурсов. Особый интерес представляет способность архитектуры к переносу между гетерогенными наборами данных. Проведенные эксперименты по перекрестной проверке выявили резкое падение точности в сценарии без дообучения (около 65 %), что подтверждает наличие существенных различий между корпоративным и IoT-трафиком.

По сравнению с другими State Space-архитектурами, такими как Mamba-ECANet, предложенный вариант оказался компактнее и быстрее в инференсе, что делает его более подходящим для внедрения на IoT-устройствах и сетевых шлюзах. Из рис. 2 видно, что даже небольшое дообучение (5 %) существенно повышает точность и снижает FAR/FRR, однако оптимальным компромиссом оказался объем в 10 % целевого набора данных. При обучении на 5 % остается выше целевых значений (точность более 98 %), а дальнейшее увеличение объема более 10 % не давало заметного прироста качества. Таким образом, архитектура Edge-Mamba устойчива к выбору доли дообучения и может быть адаптирована даже при очень ограниченном объеме данных. Дополнительной ценностью архитектуры

является ее интерпретируемость. SHAP-анализ позволил выявить ключевые признаки, такие как размер сегментов и TCP-параметры, что облегчает встраивание результатов архитектуры в существующие сценарии реагирования и корреляционные правила систем мониторинга.

Полученная архитектура содержит около 5 млн параметров и занимает 2–25 МБ, с учетом буфера для инференса потребление оперативного запоминающего устройства составляет 40–45 МБ. Для удобства развертывания архитектура может быть упакована в контейнер (например, Docker или Podman). Контейнеризация обеспечивает изоляцию и позволяет в некоторых случаях анализировать трафик только определенных сервисов. В экспериментах использовались наборы данных с TCP-трафиком, однако архитектура Mamba не зависит от протокола и может применяться к другим протоколам (UDP, HTTP, HTTPS) при наличии размеченных данных, так как оперирует общим набором признаков (как для TCP, так и для UDP). Похожие State Space-архитектуры уже применялись для UDP-трафика, например в работах [12, 13].

Остаются открытыми вопросы устойчивости архитектуры к атакам «нулевого дня», а также с приватностью в условиях распределенного обучения. Для их решения перспективным направлением исследования является внедрение федеративного дообучения (fine-tuning) модели архитектуры с дифференциальной приватностью и расширение архитектуры за счет интеграции модулей больших языковых моделей для генерации сигнатур атак.

Заключение

Впервые предложена архитектура Edge-Mamba, объединяющая линейную State Space-архитектуру (модель состояний) и дообучение (fine-tuning) на сетевых данных. Архитектура демонстрирует точность 99,5 % на наборах данных TII-SSRC-23 и 98,6 % на CICIDS-2017 при задержке менее 0,2 мс. В сценарии без дообучения точность упала до 65 %, однако дообучение на 10 % целевых данных восстановило точность до 99 %, что можно охарактеризовать как высокую переносимость. В многоклассовой задаче получена точность 99 %, что превосходит CNN-BiLSTM и Transformer на 1–3 %. SHAP-анализ показал, что решающие признаки связаны с параметрами TCP-окон и размером сегментов, что облегчает интеграцию результатов в правила Security Operations Center. Edge-Mamba содержит около 5 млн параметров (примерно 25 МБ) и протестирована на устройствах уровня Raspberry Pi 4.

По результатам экспериментов можно сделать вывод, что Edge-Mamba применима для задач обнаружения атак в реальном времени на конечных сетевых шлюзах и может быть развернута как на сетевых шлюзах и хабах интернета вещей, так и в контейнеризированной инфраструктуре. Дана оценка переносимости между гетерогенными наборами данных. Показано, что без дообучения переносимость ограничена (точность 65 %), но при минимальном дообучении (10 % целевого набора данных) точность восстанавливается до 99 %. Это подтверждает применимость архитектуры в сценариях кросс-доменных атак при ограниченном объеме данных. Перспективные направления будущих исследований включают защиту от adversarial-трафика, федеративное дообучение с дифференциальной приватностью и гибридизацию с большими лингвистическими моделями для автогенерации сигнатур.

Литература

1. Gelgi M., Guan Y., Arunachala S., Rao M.S.S., Dragoni N. Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques // Sensors. 2024. V. 24. N 11. P. 3571. https://doi.org/10.3390/s24113571
2. Singh A., Gupta B.B. Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms // International Journal on Semantic Web and Information Systems. 2022. V. 18. N 1. P. 43. https://doi.org/10.4018/ijswis.297143
3. Diana L., Dini P., Paolini D. Overview on intrusion detection systems for computers // Computers. 2025. V. 14. N 3. P. 87. https://doi.org/10.3390/computers14030087
4. Arnob A.K.B., Roy Chowdhury R., Chaiti N.A., Saha S., Roy A. A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions // Journal of Edge Computing. 2025. V. 4. N 1. P. 73–104. https://doi.org/10.55056/jec.885
5. Ravipati R.D., Abualkibash M. Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets: a review paper // International Journal of Computer Science and Information Technology. 2019. V. 11. N 3. P. 65–80. https://doi.org/10.5121/ijcsit.2019.11306
6. Talukder M.A., Islam M.M., Uddin M.A., Hasan K.F., Sharmin S., Alyami S.A., Moni M.A. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction // Journal of Big Data. 2024. V. 11. N 1. P. 33. https://doi.org/10.1186/s40537-024-00886-w
7. Sapre S., Ahmadi P., Islam K. A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets Through

References

1. Gelgi M., Guan Y., Arunachala S., Rao M.S.S., Dragoni N. Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques. *Sensors*, 2024, vol. 24, no. 11, pp. 3571. https://doi.org/10.3390/s24113571
2. Singh A., Gupta B.B. Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms. *International Journal on Semantic Web and Information Systems*, 2022, vol. 18, no. 1, pp. 43. https://doi.org/10.4018/ijswis.297143
3. Diana L., Dini P., Paolini D. Overview on intrusion detection systems for computers. *Computers*, 2025, vol. 14, no. 3, pp. 87. https://doi.org/10.3390/computers14030087
4. Arnob A.K.B., Roy Chowdhury R., Chaiti N.A., Saha S., Roy A. A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions. *Journal of Edge Computing*, 2025, vol. 4, no. 1, pp. 73–104. https://doi.org/10.55056/jec.885
5. Ravipati R.D., Abualkibash M. Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets: a review paper. *International Journal of Computer Science and Information Technology*, 2019, vol. 11, no. 3, pp. 65–80. https://doi.org/10.5121/ijcsit.2019.11306
6. Talukder M.A., Islam M.M., Uddin M.A., Hasan K.F., Sharmin S., Alyami S.A., Moni M.A. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *Journal of Big Data*, 2024, vol. 11, no. 1, pp. 33. https://doi.org/10.1186/s40537-024-00886-w
7. Sapre S., Ahmadi P., Islam K. A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets Through

Various Machine Learning Algorithms // arXiv. 2019. arXiv:1912.13204. https://doi.org/10.48550/arXiv.1912.13204
8. Лапина М.А., Мовзалевская В.В., Токмакова М.Е., Бабенко М.Г., Саджид М. Применение технологий машинного обучения для обнаружения веб-атак // Вопросы кибербезопасности. 2024. № 4 (62). С. 92–103. https://doi.org/10.21681/2311-3456-2024-4-92-103
9. Divekar A., Parekh M., Savla V., Mishra R., Shirole M. Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives // Proc. of the IEEE 3rd International Conference on Computing, Communication and Security (ICCCS). 2018. P. 1–8. https://doi.org/10.1109/CCCS.2018.8586840
10. Choudhary S., Kesswani N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT // Procedia Computer Science. 2020. V. 167. P. 1561–1573. https://doi.org/10.1016/j.procs.2020.03.367
11. Antari A., Abo-Aisheh Y., Shamasneh J., Ashqar H.I. Network traffic classification using machine learning, transformer, and large language models // Proc. of the IEEE 4th International Conference on Computing and Machine Intelligence (ICMI). 2025. P. 1–5. https://doi.org/10.1109/icmi65310.2025.11141207
12. Bilge L., Dumitras T. Before we knew it: an empirical study of zero-day attacks in the real world // Proc. of the ACM conference on Computer and communications security. 2012. P. 833–844. https://doi.org/10.1145/2382196.2382284
13. Wang T., Xie X., Wang W., Wang C., Zhao Y., Cui Y. NetMamba: efficient network traffic classification via pre-training unidirectional Mamba // Proc. of the IEEE 32nd International Conference on Network Protocols (ICNP). 2024. P. 1–11. https://doi.org/10.1109/icnp61940.2024.10858569
14. Xu J., Chen L., Xu W., Dai L., Wang C., Hu L. ET-Mamba: a Mamba model for encrypted traffic classification // Information. 2025. V. 16. N 4. P. 314. https://doi.org/10.3390/info16040314
15. Ma C., Du X., Cao L. Improved KNN algorithm for fine-grained classification of encrypted network flow // Electronics. 2020. V. 9. N 2. P. 324. https://doi.org/10.3390/electronics9020324
16. Zhang W., Zhang L., Zhang X., Wang Y., Liu P., Gui G. Intelligent unsupervised network traffic classification method using adversarial training and deep clustering for secure Internet of things // Future Internet. 2023. V. 15. N 9. P. 298. https://doi.org/10.3390/fi15090298
17. Pang B., Fu Y., Ren S., Wang Y., Liao Q., Jia Y. C. GNN: Traffic Classification with graph neural network // arXiv. 2021. arXiv:2110.09726. https://doi.org/10.48550/arXiv.2110.09726
18. Lotfollahi M., Jafari Siavoshani M., Shirali Hossein Zade R., Saberian M. Deep packet: a novel approach for encrypted traffic classification using deep learning // Soft Computing. 2020. V. 24. N 3. P. 1999–2012. https://doi.org/10.1007/s00500-019-04030-2
19. Lin X., Xiong G., Gou G., Li Z., Shi J., Yu J. ET-BERT: a contextualized datagram representation with pre-training transformers for encrypted traffic classification // Proc. of the ACM Web Conference. 2022. P. 633–642. https://doi.org/10.1145/3485447.3512217
20. Yang J., Liang G., Li B., Wen G., Gao T. A deep-learning- and reinforcement-learning-based system for encrypted network malicious traffic detection // Electronics Letters. 2021. V. 57. N 9. P. 363–365. https://doi.org/10.1049/ell2.12125
21. Zeleke S.N., Jember A.F., Bochicchio M. Integrating explainable AI for effective malware detection in encrypted network traffic // arXiv. 2024. arXiv:2501.05387. https://doi.org/10.48550/arXiv.2501.05387
22. Panigrahi R., Borah S., Bhoi A.K., Ijaz M.F., Pramanik M., Kumar Y., Jhaveri R.H. A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets // Mathematics. 2021. V. 9. N 7. P. 751. https://doi.org/10.3390/math9070751
23. Tran D.-H., Park M. FN-GNN: a novel graph embedding approach for enhancing graph neural networks in network intrusion detection systems // Applied Sciences. 2024. V. 14. N 16. P. 6932. https://doi.org/10.3390/app14166932
24. Akpaku E., Chen J., Ahmed M., Agbenyegah F.K., Brown-Acquaye W.L. RAGN: Detecting unknown malicious network traffic using a robust adaptive graph neural network // Computer Networks. 2025. V. 262. P. 111184. https://doi.org/10.1016/j.comnet.2025.111184
25. Areia J., Bispo I.A., Santos L., De Carvalho Costa R.L. IoMT-TrafficData: dataset and tools for benchmarking intrusion detection in Internet of medical things // IEEE Access. 2024. V. 12. P. 115370–115385. https://doi.org/10.1109/ACCESS.2024.3437214

Various Machine Learning Algorithms. *arXiv*, 2019. arXiv:1912.13204. https://doi.org/10.48550/arXiv.1912.13204
8. Lapina M.A., Movzalevskaya V.V., Tokmakova M.E., Babenko M.G., Sajid M. Detecting web attacks using machine learning algorithms. *Voprosy Kiberbezopasnosti*, 2024, no. 4 (62), pp. 92–103. (in Russian). https://doi.org/10.21681/2311-3456-2024-4-92-103
9. Divekar A., Parekh M., Savla V., Mishra R., Shirole M. Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives. *Proc. of the IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, 2018, pp. 1–8. https://doi.org/10.1109/CCCS.2018.8586840
10. Choudhary S., Kesswani N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. *Procedia Computer Science*, 2020, vol. 167, pp. 1561–1573. https://doi.org/10.1016/j.procs.2020.03.367
11. Antari A., Abo-Aisheh Y., Shamasneh J., Ashqar H.I. Network traffic classification using machine learning, transformer, and large language models. *Proc. of the IEEE 4th International Conference on Computing and Machine Intelligence (ICMI)*, 2025, pp. 1–5. https://doi.org/10.1109/icmi65310.2025.11141207
12. Bilge L., Dumitras T. Before we knew it: an empirical study of zero-day attacks in the real world. *Proc. of the ACM conference on Computer and communications security*, 2012, pp. 833–844. https://doi.org/10.1145/2382196.2382284
13. Wang T., Xie X., Wang W., Wang C., Zhao Y., Cui Y. NetMamba: efficient network traffic classification via pre-training unidirectional Mamba. *Proc. of the IEEE 32nd International Conference on Network Protocols (ICNP)*, 2024, pp. 1–11. https://doi.org/10.1109/icnp61940.2024.10858569
14. Xu J., Chen L., Xu W., Dai L., Wang C., Hu L. ET-Mamba: a Mamba model for encrypted traffic classification. *Information*, 2025, vol. 16, no. 4, pp. 314. https://doi.org/10.3390/info16040314
15. Ma C., Du X., Cao L. Improved KNN algorithm for fine-grained classification of encrypted network flow. *Electronics*, 2020, vol. 9, no. 2, pp. 324. https://doi.org/10.3390/electronics9020324
16. Zhang W., Zhang L., Zhang X., Wang Y., Liu P., Gui G. Intelligent unsupervised network traffic classification method using adversarial training and deep clustering for secure Internet of things. *Future Internet*, 2023, vol. 15, no. 9, pp. 298. https://doi.org/10.3390/fi15090298
17. Pang B., Fu Y., Ren S., Wang Y., Liao Q., Jia Y. C. GNN: Traffic Classification with graph neural network. *arXiv*, 2021. arXiv:2110.09726. https://doi.org/10.48550/arXiv.2110.09726
18. Lotfollahi M., Jafari Siavoshani M., Shirali Hossein Zade R., Saberian M. Deep packet: a novel approach for encrypted traffic classification using deep learning. *Soft Computing*, 2020, vol. 24, no. 3, pp. 1999–2012. https://doi.org/10.1007/s00500-019-04030-2
19. Lin X., Xiong G., Gou G., Li Z., Shi J., Yu J. ET-BERT: a contextualized datagram representation with pre-training transformers for encrypted traffic classification. *Proc. of the ACM Web Conference*, 2022, pp. 633–642. https://doi.org/10.1145/3485447.3512217
20. Yang J., Liang G., Li B., Wen G., Gao T. A deep-learning- and reinforcement-learning-based system for encrypted network malicious traffic detection. *Electronics Letters*, 2021, vol. 57, no. 9, pp. 363–365. https://doi.org/10.1049/ell2.12125
21. Zeleke S.N., Jember A.F., Bochicchio M. Integrating explainable AI for effective malware detection in encrypted network traffic. *arXiv*, 2024. arXiv:2501.05387. https://doi.org/10.48550/arXiv.2501.05387
22. Panigrahi R., Borah S., Bhoi A.K., Ijaz M.F., Pramanik M., Kumar Y., Jhaveri R.H. A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets. *Mathematics*, 2021, vol. 9, no. 7, pp. 751. https://doi.org/10.3390/math9070751
23. Tran D.-H., Park M. FN-GNN: a novel graph embedding approach for enhancing graph neural networks in network intrusion detection systems. *Applied Sciences*, 2024, vol. 14, no. 16, pp. 6932. https://doi.org/10.3390/app14166932
24. Akpaku E., Chen J., Ahmed M., Agbenyegah F.K., Brown-Acquaye W.L. RAGN: Detecting unknown malicious network traffic using a robust adaptive graph neural network. *Computer Networks*, 2025, vol. 262, pp. 111184. https://doi.org/10.1016/j.comnet.2025.111184
25. Areia J., Bispo I.A., Santos L., De Carvalho Costa R.L. IoMT-TrafficData: dataset and tools for benchmarking intrusion detection in Internet of medical things. *IEEE Access*, 2024, vol. 12, pp. 115370–115385. https://doi.org/10.1109/ACCESS.2024.3437214
26. Koumar J., Hynek K., Cejka T., Šiška P. CESNET-TimeSeries24: time series dataset for network traffic anomaly detection and forecasting.

26. Koumar J., Hynek K., Cejka T., Šiška P. CESNET-TimeSeries24: time series dataset for network traffic anomaly detection and forecasting // Scientific Data. 2025. V. 12. N 1. P. 338. https://doi.org/10.1038/s41597-025-04603-x
27. Werbos P.J. Backpropagation through time: what it does and how to do it // Proceedings of the IEEE. 1990. V. 78. N 10. P. 1550–1560. https://doi.org/10.1109/5.58337
28. Gu A., Dao T. Mamba: linear-time sequence modeling with selective state spaces // arXiv. 2023. arXiv:2312.00752. https://doi.org/10.48550/arXiv.2312.00752
29. Wang M., Zhang H., Zhou N. A study on the Mamba-ECANet model for intrusion detection in data security using end-to-end learning // Optimizations in Applied Machine Learning. 2024. V. 1. N 1. P. 01001. https://doi.org/10.71070/oaml.v1i1.8
30. Jouhari M., Guizani M. Lightweight CNN-BiLSTM based Intrusion detection systems for resource-constrained IoT devices // Proc. of the International Wireless Communications and Mobile Computing (IWCMC). 2024. P. 1558–1563. https://doi.org/10.1109/iwcmc61514.2024.10592352

Scientific Data, 2025, vol. 12, no. 1, pp. 338. https://doi.org/10.1038/s41597-025-04603-x
27. Werbos P.J. Backpropagation through time: what it does and how to do it. *Proceedings of the IEEE*, 1990, vol. 78, no. 10, pp. 1550–1560. https://doi.org/10.1109/5.58337
28. Gu A., Dao T. Mamba: linear-time sequence modeling with selective state spaces. *arXiv*, 2023. arXiv:2312.00752. https://doi.org/10.48550/arXiv.2312.00752
29. Wang M., Zhang H., Zhou N. A study on the Mamba-ECANet model for intrusion detection in data security using end-to-end learning. *Optimizations in Applied Machine Learning*, 2024, vol. 1, no. 1, pp. 01001. https://doi.org/10.71070/oaml.v1i1.8
30. Jouhari M., Guizani M. Lightweight CNN-BiLSTM based Intrusion detection systems for resource-constrained IoT devices. *Proc. of the International Wireless Communications and Mobile Computing (IWCMC)*, 2024, pp. 1558–1563. https://doi.org/10.1109/iwcmc61514.2024.10592352

Авторы

Здорников Егор Олегович — программист, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0009-0009-0154-5153, e.zdornickow2012@yandex.ru
Попов Илья Юрьевич — кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57278564300, https://orcid.org/0000-0002-6407-7934, ilyapopov27@gmail.com

Authors

Egor O. Zdornikov — Software Developer, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0009-0009-0154-5153, e.zdornickow2012@yandex.ru
Ilya Yu. Popov — PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57278564300, https://orcid.org/0000-0002-6407-7934, ilyapopov27@gmail.com

Статья поступила в редакцию 10.06.2025
Одобрена после рецензирования 24.08.2025
Принята к печати 24.01.2026

Received 10.06.2025
Approved after reviewing 24.08.2025
Accepted 24.01.2026