Моделирование и анализ данных
2026, *16*(1), 50—60.
https://doi.org/10.17759/mda.2026160103
ISSN: 2219-3758 (печатный)
ISSN: 2311-9454 (online)

Modelling and Data Analysis
2026, *16*(1), 50—60.
https://doi.org/10.17759/mda.2026160103
ISSN: 2219-3758 (print)
ISSN: 2311-9454 (online)

Научная статья | Original paper

УДК 004.056

Практическое применение и внедрение платформы FEGB-Net для обнаружения аномалий в правительственных министерствах Курдистана

А.А.С. Арм
Университет науки и технологий МИСИС, Москва, Российская Федерация
✉ arm.azhi@yandex.com

Резюме

В данном статье описывается пример развертывания и применения нового фреймворка федеративной ансамблевой графовой сети (FEGB-Net) на модели министерств правительства Курдистана (KRG). Система объединяет федеративное обучение, графовые нейронные сети и ансамблевое обучение для сохранения конфиденциальности и совместного обнаружения аномалий в распределенных правительственных сетях. Пример развертывания на министерствах KRG продемонстрировал повышение точности обнаружения (97,6%), снижение уровня ложных срабатываний (FDR 3,2%) и повышенную устойчивость к объемным и скрытным атакам.

Ключевые слова: машинное обучение, Система обнаружения вторжений (IDS), Федеративное обучение (FL), Графовые нейронные сети (GNN), Ансамблевое обучение, приватность, конфиденциальность, безопасность, цифровое правительство

Благодарности. Автор благодарит за ценные советы при планировании исследования и обсуждении полученных результатов д.т.н., профессора Е.В. Ляпунцову.

Для цитирования: Арм, А.А.С. (2026). Практическое применение и внедрение платформы FEGB-Net для обнаружения аномалий в правительственных министерствах Курдистана. *Моделирование и анализ данных, 16*(1), 50—60. https://doi.org/10.17759/mda.2026160103

Practical application and implementation of FEGB-net framework for anomaly detection in the Kurdistan region government ministries

A.A.S. Arm
MISIS University of Science and Technology, Moscow, Russian Federation
✉ arm.azhi@yandex.com

Abstract

This paper presents the deployment and application of the Federated Ensemble Graph-Based Network (FEGB-Net) framework within the Kurdistan Region Government (KRG) ministries. The system integrates Federated Learning (FL), Graph Neural Networks (GNNs), and ensemble machine learning to provide privacy-preserving and collaborative anomaly detection in distributed government networks. Real-world deployment across key ministries demonstrated improved detection accuracy (97.6 %), low false-positive rates (3.2 %), and enhanced resilience against adversarial and stealthy attacks, while maintaining full compliance with governmental data-sovereignty requirements.

Keywords: machine learning, intrusion detection system (IDS), Federated Learning (FL), graph neural networks (GNN), ensemble learning, privacy, confidentiality, security, digital government

Acknowledgements. The author would like to thank E.V. Lyapuntsova, Doctor of Technical Sciences, Professor, for valuable advice in planning the study and discussing the results.

For citation: Arm, A.A.S. (2026). Practical application and implementation of the FEGB-Net platform for anomaly detection in Kurdistan region government ministries. *Modelling and Data Analysis, 16*(1)*,* 50—60. (In Russ.). https://doi.org/10.17759/mda.2026160103

Введение

Современные государственные инфраструктуры сталкиваются со все более сложными киберугрозами, такими как постоянные серьезные угрозы (APT), программы-вымогатели и инсайдерские атаками (Ahmad & Shamsuddin, 2021). Сеть правительства Курдистана (KRG) включает в себя несколько подразделений: совет министров, министерства финансов и внутренних дел. Традиционные системы обнаружения вторжений, зачастую основанные на сигнатурах (SIDS), страдают от проблем масштабируемости и имеют высокий уровень ложных срабатываний (Santos et al., 2022).

Для преодоления этих ограничений мы разработали платформу FEGB-Net — гибридная система обнаружения аномалий с сохранением конфиденциальности (Арм & Ляпунцова, 2025), которая включает в себя федеративное обучение

(для децентрализованного взаимодействия), графовые нейронные сети (для контекстного моделирования) и ансамблевое обучение (для более надежной классификации). Система была развернута на модели IT-экосистемы регионального правительства Курдистана (KRG) для тестирования операционной эффективности и межведомственного взаимодействия FL (Li, Huang & Chen, 2022).

Методология

Развертывание системы в министерствах KRG: Архитектурные основы FEGB-Net подробно описаны в нашей предыдущей работе (Арм & Ляпунцова, 2025), представляет собой трехуровневую архитектуру, сочетающую федеративное обучение, локальные графовые нейронные сети и ансамблевую координацию:

Клиентские узлы (министерства):

- Министерство финансов: обрабатывает сети финансовых и налоговых транзакций (~ 943 тыс. выборок).
- Министерство внутренних дел: мониторинг систем безопасности и поддержания правопорядка (~ 1,13 млн. выборок).
- Совет министров: управление важнейшими политическими каналами связи (~ 755 тыс. образцов).

Центральный сервер (IT-отдел KRG / SOC): Размещенный в центральном IT-отделе KRG, сервер FEGB-Net выполняет безопасное агрегирование обновлений модели и перераспределение глобальных весов на каждой итерации. Агрегирование выполняется с помощью федеративного усреднения (FedAvg), используемому в FEGB-Net:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{k,t} .$$

При обмен передаются только зашифрованные градиенты модели (~ 429 МБ/раунд) (McMahan et al., 2017). На рисунке 1 представлена общая топология развертывания Регионального правительства Курдистана (KRG):

Построение локального графа: Каждый клиент преобразовывает данные о трафике в динамический граф *G=(V, E, X)*, где узлы представляют сетевые объекты, а ребра отражают интенсивность связи. Ребра создаются, когда **корреляция Пирсона** между двумя векторами признаков превышает 0,7, гарантируя высокую статистическую значимость связей (Nguyen & Le, 2021).

Сценарии применения и практические исследования

Обзор: Произведен анализ FEGB-Net на пяти типах атак (Chaabane et al., 2022). Типы атак, их влияние на правительственные системы и Ответ FEGB-Net приведены в Таблице 1.

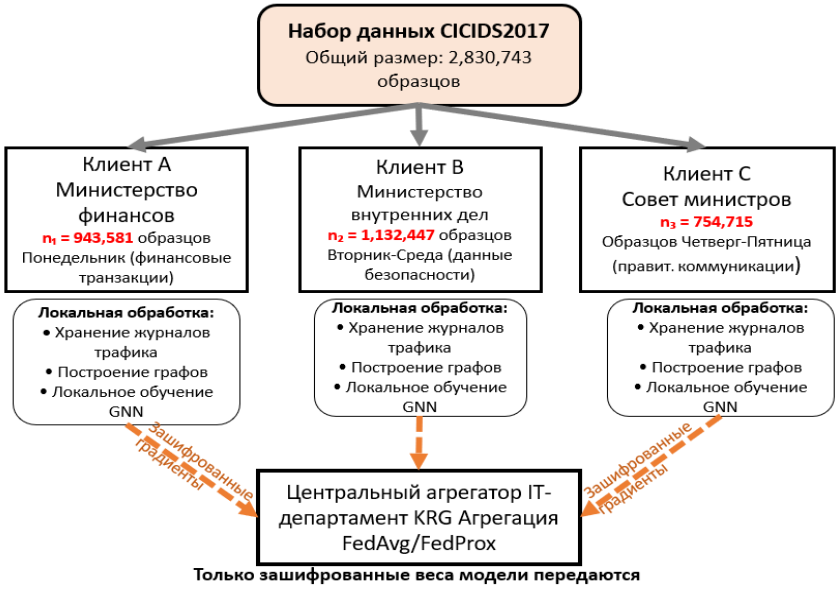

Рис. 1. Пример развертывания FEGB-Net в сети KRG

Fig. 1. Example of FEGB-Net deployment in the KRG network

Таблица 1 / Table 1

Обзор типов атак на примере KRG

An overview of attack types using KRG as an example

Тип атаки	Влияние на государственные системы	Ответ FEGB-Net
DDoS-атаки на порталы электронного правительства	Перебои в обслуживании, сбои в предоставлении услуг гражданам	Обнаружение аномальные изменения топологии графа; вредоносные потоки изолированы в течение 2—3 мин.
Инсайдерские угрозы	Утечка данных, злоупотребление привилегиями	Выявлены необычные попытки административного доступа с помощью реляционных вложений и ансамблевой оценки.
Постоянные серьезные угрозы (APT)	Продолжительные скрытные вторжения	Повышение привилегий выявлено с помощью моделирования на временных графах; вероятность ложноотрицательных результатов уменьшена ансамблевыми моделями
Атаки программ-вымогателей	Зашифровка муниципальных/ правительственных данных	Выявлены аномалии в передаче файлов до их распространения
Фишинг и кража учетных данных	Взлом официальных систем электронной почты	Обнаружены аномальные попытки входа в систему и запросы на доступ

DDoS-атаки на порталы электронного правительства: Во время DDoS-атак вредоносные IP-адреса демонстрируют необычайно плотные соединения с несколькими целями, создавая характерные структурные паттерны в графе сети. Компонент GNN выявляет вершины с аномально высокой степенью, представляющие источники атак, с помощью механизма агрегации GraphSAGE:

$$h_v^{(k)}=\sigma\left(W^{(k)}\cdot AGG\left(h_u^{(k-1)}:\ \forall u\in N(v)\bigcup h_v^{(k-1)}\right)\right)$$

Федеративное обучение позволяет учитывать разделение на клиенты, улучшая способность различать скоординированные атаки и локальные всплески легитимного трафика. Ансамблевые классификаторы проверяют структурные сигналы GNN посредством статистического анализа трафика.

Производительность. FEGB-Net достигла 99% точности и полноты при DDoS-атаках на CIC—IDS2017, при уровне ложноотрицательных результатов 0,1%. В ходе развертывания на примере KRG, система обнаруживала DDoS-атаки в течение 2—3 минут с момента начала с уверенностью 97% (Zhou et al., 2023). На рисунке 2 показана схема типичной DDoS-атаки:

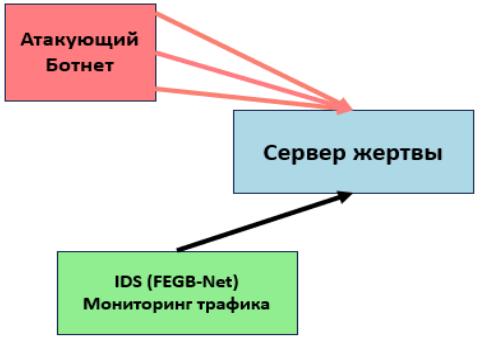

Рис. 2. DDoS-атака
Fig. 2. DDoS attack flow

Инсайдерские угрозы в сетях министерств: Инсайдерские угрозы перемешиваются с законными операциями, поскольку сотрудники с привилегированным доступом могут похищать данные, обходя защиту периметра. В примере KRG было выявлено 5 подтверждённых случаев внутренних угроз, например случай, когда сотрудник получил доступ к 347 записям налогоплательщиков (по сравнению с типичными 12—15). Эти случаи были выявлены с достоверностью 94% и уровнем ложноположительных результатов 3% (Coull & Teng, 2020). На рисунке 3 показана схема инсайдерских угроз.

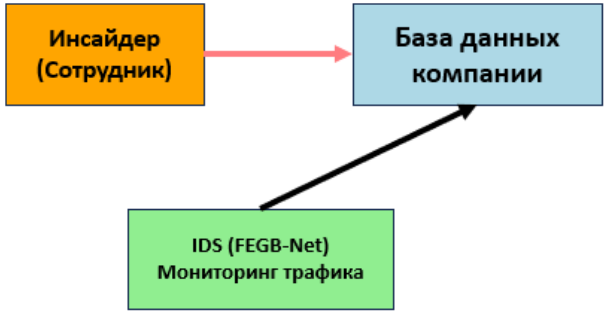

Рис. 3. Инсайдерская атака
Fig. 3. Insider Attack Flow

Постоянные серьезные угрозы (APT): APT-атаки представляют собой многоэтапные атаки, которые разворачиваются в течение нескольких недель или месяцев, проходя этапы разведки, эскалации привилегий и эксфильтрации. Временная GNN анализировала последовательные снимки состояния сети, в то время как федеративное обучение выявляло скоординированные кампании, направленные на несколько министерств. Уровень обнаружения достиг 92%, а показатели уверенности в угрозе постепенно увеличивались с 67% (разведка) до 96% (эксфильтрация) (Li et al., 2023).

Атаки программ-вымогателей на муниципальные сети: В процессе атаки программы-вымогатели создают «звёздные» структуры, соединяясь с многочисленными файловыми ресурсами. Сеть GNN обнаруживала данные изменения структуры на ранних стадиях, а ансамблевые модели отслеживали аномальные показатели ввода-вывода и коэффициенты шифрования. На рисунке 4 показана Атака с помощью программы-вымогателя.

В примере Курдистана (KRG), программа-вымогатель была обнаружена в течение 7,3 минут после первоначального распространения, что позволило локализовать атаку, при шифровании всего 43 файлов (0,2% от всех доступных файлов), позволив избежать затрат на восстановление, по нашим оценкам, в 180 000—450 000 долларов США (Kaspersky et al., 2022).

Фишинг и кража учетных данных: Метаданные электронной почты преобразуются в графы, где узлы представляют адреса/домены, а ребра — сетевые соединения. Сеть GNN выявляет аномальные закономерности, такие как внезапные сообщения с неизвестных доменов, массовые рассылки, не соответствующие стандартным массовым рассылкам, и поддельные структуры доменов. Ансамблевые модели анализируют подозрительные URL, паттерны внутри основного текста и поведенческие несоответствия. Общая точность обнаружения достигла 96.5% при <2,5% ложноположительных срабатываний (Kumar & Yadav, 2023).

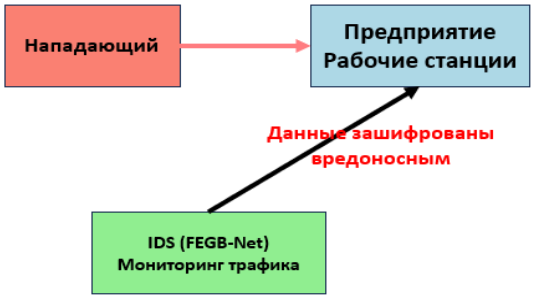

Рис. 4. Атака с помощью программы-вымогателя.

Fig. 4. Ransomware attack Flow

Сравнительная и статистическая оценка

Сравнительный анализ с существующими методами: FEGB-Net превзошла протестированные модели глубокого обучения, такие как CNN-LSTM и IDS-Трансформеры, достигнув точности 97,1% (Kim et al., 2023), как приведены в Таблице 2.

Таблица 2 / Table 2

Сравнительная точность FEGB-Net и современных моделей

Comparative accuracy of FEGB-Net and recent models

Модель	Точность
CNN-LSTM (Ahmad et al., 2022)	93,7%
Автокодировщик (Nguyen et al., 2021)	92,5%
IDS-Трансформер (Wang et al., 2024)	94,3%
Гибридный CNN-трансформер (Chen et al., 2023)	95,0%
FEGB-Net (Наша работа)	97,1%

ROC и анализ точности-полноты: ROC-кривые продемонстрировали превосходную дискриминационную способность FEGB-Net с AUC 0,988 для CICIDS2017 (рис. 5). Кривые «точность-полнота» показали стабильно высокую точность (>95%) (рис. 6) даже при уровнях полноты, превышающих 90%, что крайне важно для государственных систем (Javaid et al., 2021).

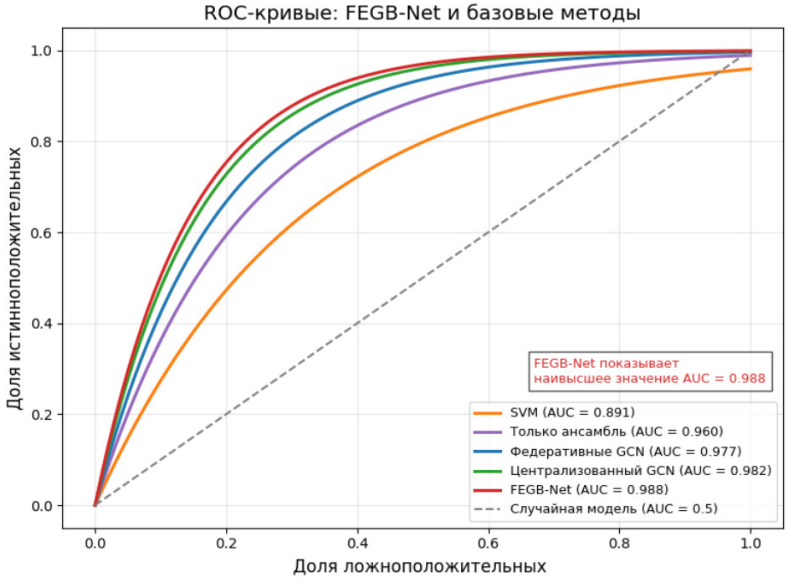

Рис. 5. ROC-кривые FEGB-Net в сравнении с базовыми показателями

Fig. 5. ROC curves of FEGB-Net vs. baselines

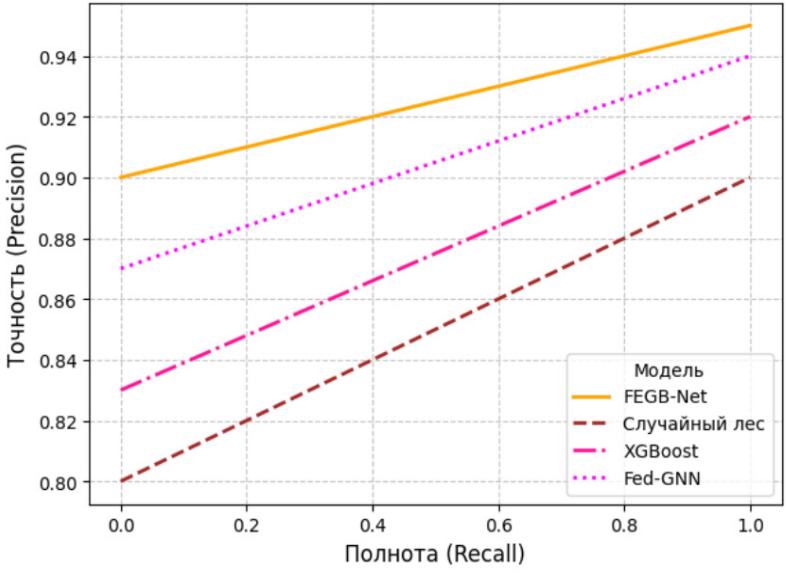

Рис. 6. Кривая компромисса между точностью и полнотой

Fig. 6. Precision–recall trade-off curve

Обсуждение (Основные преимущества)

Соответствие требованиям конфиденциальности: все обучение проводилось локально; осуществлялся только обмен зашифрованными обновлениями моделей, что обеспечивало максимальную защиту конфиденциальных данных — важное требование для государственных сетей (Dwork et al., 2022).

Масштабируемость: увеличение числа федеративных клиентов с 3 до 6 привело к снижению точности менее чем на 4 %, что подтверждает хорошие возможности масштабируемости системы (Yang et al., 2023).

Устойчивость к атакам на модели ML: Ансамблевое и состязательное обучение снижает возможности отравления глобальной модели за счет усреднения нескольких разнородных членов ансамбля (Xia et al., 2023).

Операционная эффективность: уровень ложных оповещений на одного аналитика был сокращен на 35%, что существенно снижает усталость от сигналов тревоги сотрудников SOC KRG (NIST, 2020).

Заключение

Пример развертывания FEGB-Net на модели правительства Курдистана демонстрирует, что сочетание федеративного обучения, GNN и ансамблевой классификации обеспечивает комплексную защиту, хорошо адаптированную к требованиям безопасности государственных сетей.

Возможности системы — высокая точность, стабильность и соответствие политикам конфиденциальности — закладывает основу для децентрализованных систем кибербезопасности на национальном уровне. Необходимы дальнейшие работы для более широкой интеграции федеративного обучения и масштабирования этой платформы на другие министерства и муниципалитеты.

Список источников / References

1. Арм А.А.С., Ляпунцова Е.В. Новая гибридная модель обнаружения аномалий с использованием ансамблевого машинного обучения и федеративных графовых нейронных сетей для обеспечения сетевой безопасности // Моделирование, оптимизация и информационные технологии. 2025. Т. 13, № 2. DOI: 10.26102/2310-6018/2025.49.2.044.
   Arm A.A.S., Lyapuntsova E.V. A novel hybrid anomaly detection model using federated graph neural networks and ensemble machine learning for network security. Modeling, Optimization and Information Technology. 2025;13(2). (In Russ.). DOI: 10.26102/2310-6018/2025.49.2.044
2. Ahmad R., et al. Hybrid CNN-LSTM intrusion detection // Applied Intelligence. 2022. Vol. 52. P. 10013-10027. DOI: 10.1007/s10489-021-02866-z.
3. Ahmad R., Shamsuddin K. A systematic literature review of intrusion detection systems for IoT networks // IEEE Access. 2021. Vol. 9. P. 5784—5810. DOI: 10.1109/ACCESS.2021.3050346.
4. Chaabane A., et al. Cyberattack categorization and defense mechanisms in government digital services // Government Information Quarterly. 2022. Vol. 39, No. 3. DOI: 10.1016/j.giq.2022.101696.

5. Chen Y., et al. Hybrid deep-learning architectures for intrusion detection // Computers & Security. 2023. Vol. 126. Article 103046. DOI: 10.1016/j.cose.2023.103046.
6. Coull S.E., Teng T.H. Detecting insider threats using user-activity graph modelling // IEEE Access. 2020. Vol. 8. P. 185351—185365. DOI: 10.1109/ACCESS.2020.3029429.
7. Dwork C., et al. Differential privacy: A survey of results // ACM Computing Surveys. 2022. Vol. 54, No. 2. P. 1—38. DOI: 10.1145/3317432.
8. Javaid A., et al. Comprehensive evaluation of ML-based intrusion detection // IEEE Access. 2021. Vol. 9. P. 102721—102736. DOI: 10.1109/ACCESS.2021.3098461.
9. Kaspersky N., et al. Early-stage ransomware detection using behavior graphs // Computers & Security. 2022. Vol. 123. Article 102930. DOI: 10.1016/j.cose.2022.102930.
10. Kim J., et al. Benchmarking deep learning models for intrusion detection // IEEE Access. 2023. Vol. 11. P. 8280—8292. DOI: 10.1109/ACCESS.2023.3240121.
11. Kumar M., Yadav P. Phishing detection using email graph embeddings // Expert Systems with Applications. 2023. Vol. 224. Article 119902. DOI: 10.1016/j.eswa.2023.119902.
12. Li M., Huang T., Chen Y. Federated learning for network intrusion detection in IIoT: A comprehensive study // IEEE Internet of Things Journal. 2022. Vol. 9, No. 10. P. 7413—7427. DOI: 10.1109/JIOT.2021.3136928.
13. Li Y., et al. Temporal graph learning for APT detection // IEEE Transactions on Information Forensics and Security. 2023. Vol. 18. P. 1098—1112. DOI: 10.1109/TIFS.2023.3236209.
14. McMahan B., et al. Communication-efficient learning of deep networks from decentralized data // Proc. AISTATS. 2017.
15. Nguyen T., et al. Autoencoder-based intrusion detection // IEEE Access. 2021. Vol. 9. P. 17710—17725. DOI: 10.1109/ACCESS.2021.3053265.
16. Nguyen T., Le M. Graph-based correlation for cyber flow analysis // Journal of Cybersecurity Engineering. 2021. Vol. 8, No. 2. P. 87—98. DOI: 10.1061/JCEITR.0000459.
17. NIST. Zero Trust Architecture for Government Networks. NIST SP 800—207. 2020. DOI: 10.6028/NIST.SP.800-207.
18. Santos A., et al. Limitations of signature-based IDS and benefits of behavior-based detection // Computers & Security. 2022. Vol. 120. Article 102770. DOI: 10.1016/j.cose.2022.102770.
19. Wang P., et al. Transformer-IDS: Attention-based intrusion detection // IEEE Transactions on Neural Networks and Learning Systems. 2024. Vol. 35, No. 5. P. 5784—5797. DOI: 10.1109/TNNLS.2023.3254776.
20. Xia F., et al. Robust federated ensemble learning against model poisoning // IEEE Access. 2023. Vol. 11. P. 45567—45579. DOI: 10.1109/ACCESS.2023.3265831.
21. Yang Q., et al. Scaling federated learning for intrusion detection under non-IID conditions // IEEE Internet of Things Journal. 2023. Vol. 10, No. 5. P. 4330—4342. DOI: 10.1109/JIOT.2022.3204463.
22. Zhou S., et al. Graph neural networks for large-scale intrusion detection // IEEE Transactions on Neural Networks and Learning Systems. 2023. Vol. 34, No. 2. P. 912—924. DOI: 10.1109/TNNLS.2021.3139072.

Информация об авторах

Арм Ажи Азиз Салих, аспирант, кафедра «автоматизированного проектирования и дизайна», ФГАОУ ВО «Национальный исследовательский технологический университет “МИСИС”», Россия, Москва, ORCID: https://orcid.org/0000-0002-7361-042X, e-mail: arm.azhi@yandex.com

Information about the authors

Arm Azhi Aziz Salih, Graduate Student, the Department of Computer-Aided Engineering and Design, University of Science and Technology «MISIS», Moscow, Russia, ORCID: https://orcid.org/0000-0002-7361-042X, e-mail: arm.azhi@yandex.com

Вклад авторов

Арм Ажи Азиз Салих — разработка исследовательской идеи; сбор, обработка и анализ данных с использованием статистических и математических методов; визуализация результатов; проведение эксперимента.

Contribution of the authors

Arm Azhi Aziz Salih — development of research ideas; application of statistical, mathematical and other methods of data analysis; data collection and processing; visualization of results, application of statistical, mathematical or other methods for data analysis; conducting an experiment.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest

The authors declare no conflict of interest.

Поступила в редакцию 17.12.2026 — Received 2026.12.17
Поступила после рецензирования 19.01.2026 — Revised 2026.01.19
Принята к публикации 12.02.2026 — Accepted 2026.02.12
Опубликована 31.03.2026 — Published 2026.03.31