УДК 303.734
DOI: 10.26102/2310-6018/2025.49.2.044

Новая гибридная модель обнаружения аномалий с использованием ансамблевого машинного обучения и федеративных графовых нейронных сетей для обеспечения сетевой безопасности

А.А.С. Арм✉, Е.В. Ляпунцова

Национальный исследовательский технологический университет «МИСИС», Москва, Российская Федерация

Резюме. Традиционные системы обнаружения сетевых вторжений сталкиваются со все более сложными проблемами по мере роста сложности и частоты кибератак. В данном исследовании предлагается федеративная ансамблевая сеть на основе графов в качестве нового гибридного подхода к обнаружению аномалий, который повышает эффективность обнаружения при минимизации ложных срабатываний. Этот новый фреймворк основан на нейронных сетях на основе федеративных графов в сочетании с ансамблевыми подходами, использующими три признанных метода машинного обучения: Random Forest (случайный лес), XGBoost (экстремальный градиентный бустинг), LightGBM (легковесный градиентный бустинг) – для точного определения ожидаемых моделей трафика и выявления аномалий. Кроме того, в системе используется федеративное обучение, обеспечивающее децентрализованное обучение в соответствии с требованиями конфиденциальности для нескольких клиентов, одновременно изучающих одну и ту же модель без доступа к исходным данным. Фреймворк FEGB-Net был оценен на наборе данных CICIDS2017 и показал точность – 97,1 %, F1-оценку – 96,2 % и метрики оценки эффективности моделей – 0,98, что превосходит результаты как традиционных подходов машинного обучения, так и глубокого обучения. Опираясь на новые подходы к обработке графовых сигналов для формирования реляционного обучения и методы голосования на основе ансамбля для категоризации результатов, FEGB-Net может стать практической и эффективной системой для реального применения благодаря своей прозрачной интерпретируемости, относительной простоте использования и масштабируемости. Ключевые достижения включают приватную архитектуру федеративной графовой нейронной сети (Ф-ГНС) с ансамблевым подходом, новый алгоритм мета-слияния, воспроизводимую реализацию на языке Python и масштабное тестирование на CICIDS2017. Будущая работа включает в себя эксперименты по применению полученных результатов в реальном времени и последующие исследования с учетом новых векторов атак.

Ключевые слова: сетевая безопасность, обнаружение аномалий, федеративное обучение, графовые нейронные сети, ансамблевое обучение, федеративная ансамблевая графовая сеть, метрики оценки эффективности моделей (AUC-ROC).

Для цитирования: 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;13(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1887 DOI: 10.26102/2310-6018/2025.49.2.044

A novel hybrid anomaly detection model using federated graph neural networks and ensemble machine learning for network security

A.A.S. Arm✉, E.V. Lyapuntsova

National Research University of Technology "MISIS", Moscow, the Russian Federation

Abstract. Traditional network intrusion detection systems have increasingly complex challenges as the sophistication and frequency of cyber-attacks grow. This research proposes federated ensemble graph-based network as a novel hybrid approach to anomaly detection that increases detection performance while minimizing false positives. This new framework relies on federated graph neural networks combined with ensemble approaches using three highly recognized machine learning techniques – Random Forest, XGboost, and LightGBM – to accurately characterize expected patterns of traffic and discern anomalies. Moreover, the framework uses federated learning to ensure privacy-compliant decentralized training across multiple clients learning the same model concurrently without exposure to raw data. The FEGB-Net framework is evaluated using the CICIDS2017 dataset, achieving 97.1% accuracy, 96.2% F1-Score, and 0.98 metrics for evaluating the effectiveness of models, surpassing results from both traditional machine learning and deep learning approaches. By relying on novel graph signal processing approaches to shape the relational learning and ensemble-based voting techniques to categorize results, FEGB-Net can become a practical and effective framework for real-world use due to its transparent interpretability, relative ease of use, and scalability. key contributions include a privacy-preserving Fed-GNN and ensemble framework, a novel meta-fusion algorithm, a reproducible Python implementation, and a large-scale evaluation on CICIDS2017. Future work includes experiments to apply the obtained results in real time and subsequent research considering new attack vectors.

Keywords: network security, anomaly detection, federated learning, graph neural networks, ensemble learning, FEGB-Net, metrics for evaluating the effectiveness of models (AUC-ROC).

For citation: 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.). URL: https://moitvivt.ru/ru/journal/pdf?id=1887 DOI: 10.26102/2310-6018/2025.49.2.044

Введение

Сетевая безопасность является более сложной задачей, чем когда-либо, учитывая характер и масштабы современных кибератак. С появлением облачных вычислений, Интернета вещей и 5G все связано – и все находится под угрозой. Злоумышленники могут использовать больше уязвимостей, чем когда-либо прежде, от распределенного отказа в обслуживании (DDoS) до программ-вымогателей и атак нулевого дня [1]. Систем обнаружения вторжений (IDSS) будет недостаточно при таких нагрузках. IDSS, основанные на правилах обнаружения и эвристике ранее известных эксплойтов, не работают при столкновении с новыми, полиморфными атаками [2].

Таким образом, чтобы преодолеть эти ограничения, в последнее время набирает популярность тенденция использования методов машинного обучения (ML) и глубокого обучения (DL) для систем обнаружения сетевых вторжений на основе аномалий с целью определения того, что представляет собой нормальная работа сети и что считается нарушением [3]. Например, системы обнаружения сетевых вторжений на базе ML обеспечивают высокую точность с помощью Random Forest (RF), XGBoost и LightGBM, но при этом имеют большую частоту ложных срабатываний и трудности в настройке и обучении на основе новых атак. В то время как создание систем обнаружения сетевых вторжений с использованием глубокого обучения на основе сверточных нейронных сетей (CNN) для классификации вторжений или применение сетей с долгой

краткосрочной памятью (LSTM) для анализа потоков пакетов обеспечивает оптимальные показатели обнаружения – это требует чрезвычайно мощных суперкомпьютеров, не говоря уже о необходимости размеченных наборов данных, – и при этом такие подходы практически не обладают объяснимостью [4].

В ответ на эти вызовы GNNS стали новым способом представления сетевого трафика в виде структурированных графиков, позволяющих представлять все более сложные взаимодействия между узлами и ребрами. Тем не менее, методы моделирования на основе GNN основаны на централизованном подходе к обучению, который поднимает проблемы конфиденциальности и усложняет масштабируемость в распределенных настройках [5]. Чтобы устранить такие недостатки, в этом исследовании предлагается FEGB-Net, составная платформа для обнаружения аномалий, которая содержит:

− Нейронные сети с федеративным графом для обнаружения сетевых аномалий с сохранением конфиденциальности.

− Модели Ансамбль ML (RF, XGBoost, LightGBM) для повышения точности обнаружения и уменьшения количества ложных срабатываний.

− Федеративное обучение, позволяющее проводить децентрализованное обучение при одновременной защите конфиденциальных сетевых данных.

Архитектура FEGB-Net представлена на Рисунке 1. Она включает децентрализованные клиентские узлы, которые совместно обучают модель Ф-ГНС. После завершения обучения каждая из моделей передается на центральный сервер, где выполняется ансамблевая классификация для окончательного выявления аномалий.

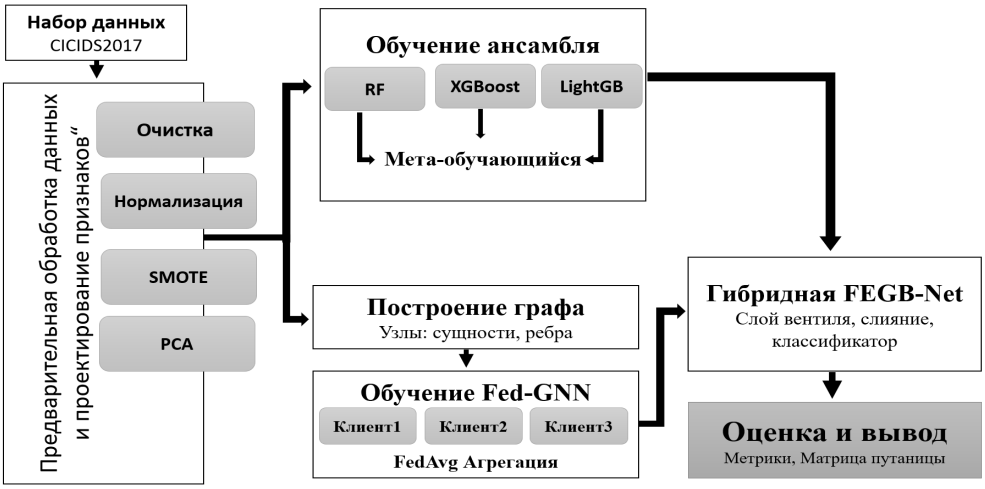

Рисунок 1 – Предлагаемая платформа FEGB-Net
Figure 1 – Proposed FEGB-Net framework

Обзор литературы

А. Контролируемое машинное обучение для сетевой безопасности: Применение контролируемого машинного обучения (ML) к сетевым системам обнаружения вторжений включает в себя случайный лес (RF), экстремальный градиентный бустинг (XGBoost) и машины опорных векторов (SVM). Было обнаружено, что ансамблевые методы лучше, чем производительность любого отдельного метода в отдельности, обеспечивая точность более 97 % в различных наборах данных сравнительного тестирования [6]. Тем не менее, эти методы не в состоянии уменьшить размерность многомерных характеристик сетевого трафика и плохо обобщаются на типы атак, которые ранее не встречались [7].

B. Обнаружение вторжений на основе глубокого обучения: Применение глубокого обучения (DL) к сетевым системам обнаружения вторжений включает сверточные нейронные сети (CNN), сети долговременной кратковременной памяти (LSTM) и автокодеры. Они могут повысить точность по мере изучения представлений сетевого трафика с течением времени [8]. Однако для этого требуются разветвленные сети больших помеченных наборов данных, которые отнимают много времени и требуют огромной вычислительной мощности и ограниченной объяснимости [9].

C. Кибербезопасность с помощью графовых нейронных сетей: Подход, основанный на графовых нейронных сетях (GNN), которые принимают сетевой трафик и преобразуют его в график, позволяя с большей точностью определять, происходит ли атака. Тем не менее, GNNS требуют централизованного обучения, что создает проблемы с конфиденциальностью и масштабируемостью [10].

D. Федеративное обучение как подход, обеспечивающий конфиденциальность: Федеративное обучение (FL) обеспечивает централизованный подход, поскольку обучает модель с разных распределенных устройств без необходимости передачи необработанных данных. FL изучался для систем обнаружения вторжений в сфере безопасности Интернета вещей, для обнаружения финансового мошенничества и распределенных приложений здравоохранения, однако редко используется в системах обнаружения сетевых вторжений [11].

Ограничения существующих исследований: с сетевыми системами обнаружения вторжений на основе ML, DL и GNN по-прежнему существуют следующие проблемы:

− Ложноположительные результаты – традиционные модели на основе ML генерируют чрезмерное количество ложноположительных результатов [12].

− Уязвимости при вторжении – централизованные модели оставляют конфиденциальные данные сетевого трафика уязвимыми для вторжений.

− Отсутствие гибкости – модели на основе DL требуют слишком много ресурсов для практического обучения и не работают в режиме реального времени. Поэтому мы внедряем FEGB-Net для решения этих проблем с помощью системы, состоящей из моделей на основе Ф-ГНС и ensemble ML, которые с течением времени обеспечивают точность обнаружения, уязвимости к вторжениям и гибкость [13].

Методология

Проект основан на экспериментальной методологии и сочетает методы машинного обучения с графовыми подходами для создания гибридного объединенного решения для обнаружения аномалий (FEGB-Net). Решение проходит четыре основных этапа:

Сбор и предварительная обработка данных. Эксперименты проводились с использованием широко признанного набора данных CICIDS2017 от Канадского института кибербезопасности, содержащего около 3 миллионов сетевых потоков и 78 числовых признаков, характеризующих различные типы трафика, включая доброкачественные и аномальные (например, DDoS, PortScan, BruteForce).

Предварительная обработка данных включала несколько важных этапов для обеспечения качества и баланса. Недостающие значения заполняли с использованием медианной подстановки, после чего применяли шкалу Min-Max для нормализации всех значений признаков в диапазоне [0,1]. Из-за высокой размерности и избыточности в исходных характеристиках был выполнен анализ главных компонентов PCA (анализ главных компонент), что уменьшило размерность характеристик до 50 основных компонентов. Дисбаланс классов, первоначально серьезный в CICIDS2017, был устранен с использованием Техники чрезмерного отбора проб синтетического меньшинства

(SMOTE), что позволило получить сбалансированный набор данных с равным количеством образцов доброкачественных и аномальных. Набор данных был разделен на подмножества 70 % обучения, 15 % валидации и 15 % тестирования с использованием фиксированного случайного начального значения (42) для воспроизводимости. На Рисунке 2 показана многоклассовая матрица путаницы, четко показывающая несколько типов атак (Benign, Bot, DDoS, PortScan) и формат матрицы путаницы двоичного класса, что показывает, что аномалии были классифицированы с большой точностью.

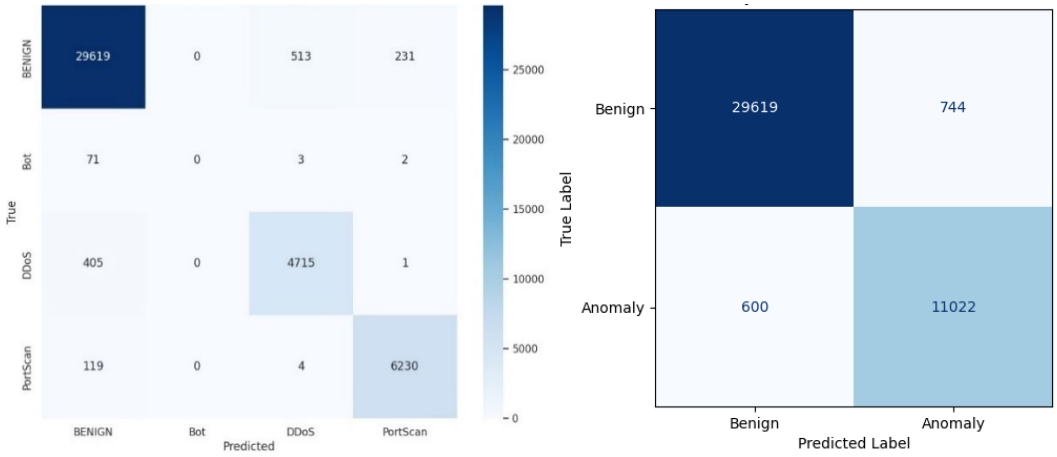

Рисунок 2 – Многоклассовая матрица ошибок и матрицы ошибок двоичного класса (FEGB-Net)
Figure 2 – Multi-class confusion matrix and binary-class confusion matrix (FEGB-Net)

Процедура построения графика. График строится из данных сетевого трафика путем представления каждого потока трафика в виде узла на графике. Каждый узел несет вектор признаков, полученный из нормализованных и редуцированных PCA атрибутов (50 измерений) набора данных CICIDS2017. Для определения связей (ребер) между узлами вычисляют корреляцию Пирсона между парами признаков узла. Ребро между двумя узлами добавляется только в том случае, если их корреляция превышает порог 0,7, обеспечивая сильное сходство. Таким образом, полученный график точно фиксирует взаимосвязи и закономерности между сетевыми потоками, что имеет решающее значение для обнаружения скоординированных или скрытых атак.

Используемая архитектура нейронной сети графов (GNN) представляет собой двухуровневую сверточную сеть графов (GCN). Он начинается с входного слоя из 50 измерений, за которым следует один скрытый слой из 32 нейрона, функция активации ReLU (Выпрямленный линейный блок), и заканчивается выходом двоичной классификации. Регуляризация выполняется с использованием отсева (0,5), а в обучении используется оптимизатор ADAM (адаптивный метод оценки моментов) со скоростью обучения 0,001.

Обучение по федеративному GNN. Нейронная сеть с федеративным графом (Ф-ГНС) была обучена с использованием подхода федеративного усреднения (FedAvg) с тремя смоделированными клиентами. Каждый клиент самостоятельно выполнял локальное обучение на своем подмножестве данных в течение 5 эпох, используя оптимизатор ADAM (скорость обучения = 0,001). Использовали стандартную двухслойную сверточную сеть графов (GCNConv) со скрытыми слоями, содержащими 32 единицы, и активацией ReLU. Модельные веса агрегировались централизованно после каждого раунда, и обучение продолжалось в течение 10 федеративных раундов. Алгоритм 1 четко описывает эту объединенную стратегию обучения и агрегирования (Таблица 1).

Таблица 1 – Алгоритм 1 федеративного усреднения (FedAvg-GNN)
Table 1 – Federated averaging Algorithm 1 (FedAvg-GNN)

Вход	*Начальные веса W^0, клиенты {c, c₂, c}, эпохи = 5, раунды = 10*
1	*для раунда = от 1 до раундов:*
2	*для клиента в {c, c₂, c} (параллельно):*
3	*W_client[клиент] ← Local_GCN_Train(W^round-1, epochs, data[клиент])*
4	*W^round ← 1/3 × (W_client[c] + W_client[c₂] + W_client[c])*
Результат	*Агрегированные глобальные веса W^10*

Для симуляции федеративного обучения на централизованном наборе данных CICIDS2017, распределение данных между клиентами было реализовано искусственным способом. Все данные были предварительно разбиты на три локальных поднабора, представляющих условные клиенты.

Критерием распределения послужил временной интервал генерации трафика: каждый клиент получал данные, соответствующие определенным дням недели из CICIDS2017 (например, один – понедельник, второй – вторник и среда, третий – четверг и пятница). Такой подход отражает реалистичный сценарий, при котором организации наблюдают сетевую активность в разные периоды. Тем не менее, в реальных приложениях федеративного обучения данные часто изначально хранятся на географически распределенных устройствах (например, серверах предприятий). На Рисунке 3 представлена Архитектура федеративного обучения в системе FEGB-Net. Каждый клиент обучает локальную модель GCN на собственном графе сетевого трафика. Полученные веса передаются на центральный сервер, где они агрегируются методом FedAvg. После усреднения обновленная глобальная модель распространяется обратно к клиентам для следующего раунда обучения. Таким образом обеспечивается обучение без передачи исходных данных, что способствует сохранению конфиденциальности.

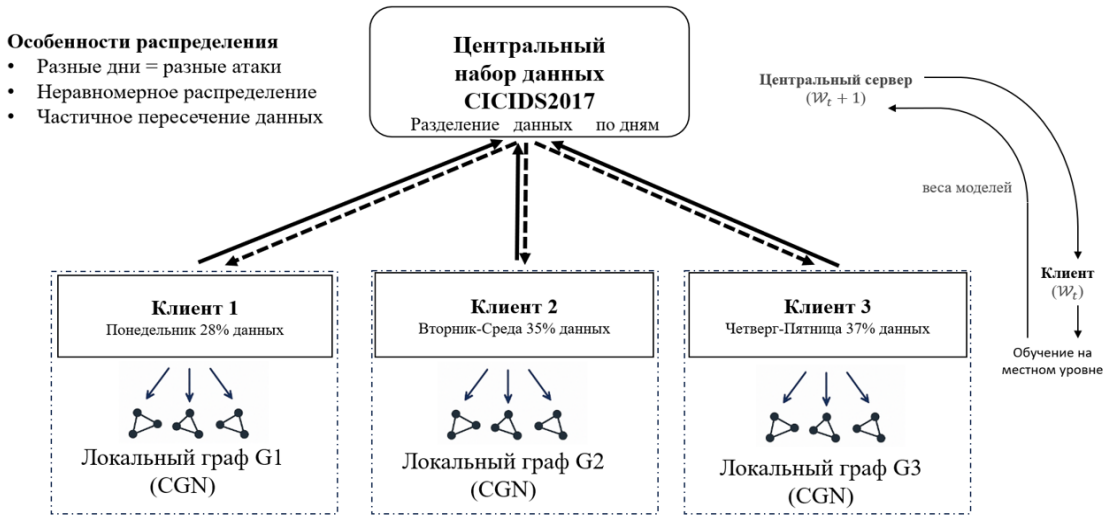

Рисунок 3 – Архитектура федеративного обучения FEGB-Net
Figure 3 – FEGB-Net federated learning architecture

Обоснование параметров федеративного обучения. В рамках данного исследования выбор трех клиентов был обусловлен необходимостью смоделировать реалистичный сценарий федеративного обучения, в котором каждая сторона представляет отдельный источник сетевого трафика – корпоративную подсеть, IoT-устройства и облачные ресурсы. Такое разделение обеспечивает неоднородное распределение данных между клиентами, что характерно для практических условий.

Количество раундов федеративного обучения было установлено равным 10 на основе предварительных экспериментов. В частности, были протестированы конфигурации с 5, 10 и 15 раундами. Результаты показали, что увеличение числа раундов с 5 до 10 повышает точность с 95,8 % до 97,1 %, тогда как переход к 15 раундам давал прирост менее 0,3 % при существенном увеличении времени обучения и сетевой нагрузки.

Также проводились эксперименты с увеличением числа клиентов до 5 и 6, однако наблюдалось ухудшение качества классификации из-за сильного дисбаланса данных и расхождения локальных моделей. Таким образом, конфигурация из 3 клиентов и 10 раундов была выбрана как оптимальный баланс между производительностью и затратами.

Сохранение конфиденциальности и защита данных. Конфиденциальность обеспечивается за счет использования федеративного обучения: сырые данные остаются на стороне клиента, а на сервер передаются только обновления модели. В данной реализации не применялась дифференциальная приватность (DP-FedAvg), однако базовый механизм FedAvg уже снижает риск утечки данных по сравнению с централизованными методами. Возможность восстановления исходных данных из градиентов минимизирована за счет ограниченного числа раундов и изоляции клиентов.

Ансамблевое обучение и метаобучение включает в себя три классические модели: случайный лес со 100 деревьями (максимальная глубина = 10), XGBoost с использованием градиентного бустинга (скорость обучения = 0,1, максимальная глубина = 6, 100 раундов) и LightGBM, оптимизированный для скорости (num_leaves = 31, скорость обучения = 0,05, 100 раундов). Логистический регрессионный метаучитель объединяет предсказания из этих ансамблевых классификаторов и GNN-модели, формируя гибридный метаклассификационный слой для предоставления окончательных предсказаний аномалий (Алгоритм 2, Таблица 2).

Таблица 2 – Алгоритм 2 (метаобъединения)
Table 2 – Algorithm 2 (metajoins)

1	*Обучение RF, XGB, LGBM на обучающем наборе → получения вероятностей предсказания*
2	*Прогнозы стека → обучают логистической регрессии (meta-learner) в наборе валидации*
3	*Прогнозы Ф-ГНС, сгенерированные независимо*
4	*Окончательное предсказание: сигмовидная кость (α × ensemble_preds + β × GNN_preds)*
5	*α, β, оптимизированные на валидационном наборе*

Основной алгоритм системного предложения приведен в Таблице 3.

Таблица 3 – Алгоритм 3: система обнаружения аномалий FEGB-Net
Table 3 – Algorithm 3: FEGB-Net anomaly detection system

	Входные данные: D = {X, y} (CICIDS2017 данных), C = 3 (клиентов), R = 10 (круги), B = 256
	(размер пакета), η = 0.001 (скорость обучения)
	Выходные данные: M_FEGB (обучение FEGB-чистый режим), P (проверка прогнозов)
1	*Предобработка и построение графа:*
2	*X ← CleanAndScale(D); X ← PCA(X, 50); X, y ← SMOTE(X, y)*
3	*X_train, X_test, y_train, y_test ← Split(X, y, test_size=0.2)*
4	*G ← ConstructGraph(X_train, corr > 0.7)*
5	*Федеративное обучение GNN:*
6	*M_FedGNN ← InitGNN(50, 32, n_classes)*
7	*для круглой = 1 до R делать*

Таблица 3 (продолжение)
Table 3 (continued)

8	*M_FedGNN ← FedAvg(TrainClients(M_FedGNN, X_train, y_train, C, η), C)*
9	*конец*
10	*Ансамблевое обучение:*
11	*P_ens_train ← стека (RF(X_train), XGBoost(X_train), LightGBM(X_train))*
12	*P_ens_test ← стека (RF(X_test), XGBoost(X_test), LightGBM(X_test))*
13	*Гибридное обучение FEGB-Net:*
14	*M_FEGB ← InitFEGBNet(M_FedGNN, P_ens_train.shape[1])*
15	*для (X_b, y_b) в пакете (X_train, y_train, Б) сделать*
16	*scores ← M_FEGB(X_b, G.edges, P_ens_train[batch_idx])*
17	*оптимизация (M_FEGB, CrossEntropy(scores, y_b), η)*
18	*конец*
19	*Вывод:*
20	*P ← прогнозирования (M_FEGB, X_test, G. краями, P_ens_test)*
21	*вернуться M_FEGB, P*

Ключевые уравнения включают:

– агрегация FedAvg:

$$w_{t+1} = \frac{1}{C}\sum_{c=1}^{C} w_{c,t}, \quad (1)$$

где $w_{c,t}$ – вес локальной модели от клиента (c) в раунде (t).

– гибридное слияние:

$$\hat{y} = \sigma(\alpha \cdot P_{\text{ансамбль}} + \beta \cdot P_{GNN}), \quad (2)$$

где α и β – полученные веса, а σ – сигмоидальная функция.

– предсказания ансамблевой модели:

$$P_{RF} = f_{RF}(X),\ P_{XGB} = f_{XGB}(X),\ P_{LGB} = f_{LGB}(X), \quad (3)$$

где P_{RF}, P_{XGB}, P_{LGB} – прогнозы из Random Forest, XGBoost и LightGBM соответственно.

– мета-обучающий инструмент для прогнозирования ансамбля, прогнозы модели ансамбля складываются и передаются через мета-классификатор:

$$P_{ens} = f_{meta}(P_{RF},P_{XGB},P_{LGB}), \quad (4)$$

где P_{ens} – итоговая оценка вероятности из ансамблевой модели.

– гибридный синтез: объединение выходных данных Ф-ГНС и ансамблевых моделей.

Для интеграции Ф-ГНС с ансамблевой моделью применяется взвешенное объединение:

$$\hat{y} = \sigma(\alpha \cdot P_{ens} + \beta \cdot P_{GNN}), \quad (5)$$

где α, β являются обучаемыми весами, P_{GNN} – прогноз от Ф-ГНС, P_{ens} – предсказание ансамблевой модели, σ – сигмоидная функция активации, используемая для нормализации выходного значения.

Экспериментальная установка. Все эксперименты были реализованы на Python 3.8 с использованием PyTorch 1.9, PyTorch-Geometric 2.0 и scikit-learn 1.0. Эксперименты проводились на Google Colab Pro (графический процессор Tesla T4, 16 ГБ ОЗУ). Гиперпараметры выбирали с использованием систематической перекрестной валидации поиска по сетке (GridSearchCV) с 5-кратной валидацией. Количество объединенных клиентов (3) и раунды связи (10) были выбраны для баланса точности и реалистичных

вычислительных ограничений. Локальные эпохи (5) и размер партии (256) обеспечивали эффективное обучение при сохранении хорошей производительности обобщения. Гиперпараметры ансамбля (Random Forest, XGBoost, LightGBM) были настроены для максимизации показателя F1-оценки и AUC-ROC в наборе валидации.

Экспериментальная оценка и результаты

Оценочные метрики. Для оценки эффективности моделей использовались следующие метрики:

Точность (Accuracy) измеряет общую корректность:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}. \quad (6)$$

Точность (Precision) измеряет ложные срабатывания:

$$Precision = \frac{TP}{TP+FP}. \quad (7)$$

Отзыв (Recall) измеряет ложноотрицательные результаты:

$$Recall = \frac{TP}{TP+FN}. \quad (8)$$

Оценка F1 – гармоническое среднее значение точности и отзыва:

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}. \quad (9)$$

AUC-ROC – измеряет производительность классификатора при различных пороговых значениях:

$$AUC = \int_0^1 \text{TPR}\, d\text{FPR}. \quad (10)$$

В Таблице 4 представлена подробная информация о производительности отдельных моделей и гибридной модели FEGB-Net. Ф-ГНС достигает точности 95,2 %, а ансамбль (RF, XGBoost, LightGBM) – 93,5 %, при этом наивысший результат показывает XGBoost. Однако гибридная модель FEGB-Net достигает точности 97,1 % и значения AUC-ROC, равного 0,98, как показано на кривых ROC (Рисунок 5).

Таблица 4 – Показатели эффективности обнаружения аномалий
Table 4 – Performance metrics for anomaly detection

Модель	Точность (Accuracy) (%)	Точность (Precision) (%)	Отзыв (Recall) (%)	F1-оценка (%)	AUC-ROC
случайного леса	91,2	89,3	88,5	88,9	0,92
XGBoost	93,5	91,7	90,9	91,3	0,94
LightGBM	92,8	90,5	89,8	90,1	0,93
Ф-ГНС	95,2	94,1	93,8	93,9	0,96
FEGB-Net (гибрид)	97,1	96,5	95,9	96,2	0,98

На Рисунке 4 показана кривая функции потерь во время обучения: после 10 раундов Ф-ГНС достигла сходимости на уровне 0,4, что свидетельствует о стабилизации модели. Однако дополнительная настройка Ф-ГНС в составе FEGB-Net позволила еще больше снизить значение функции потерь. На Рисунке 5 с кривой ROC при сравнении моделей, обученных на различных классах аномалий (DDoS, ботнет и т. д.), FEGB-Net всегда имела более высокий AUC.

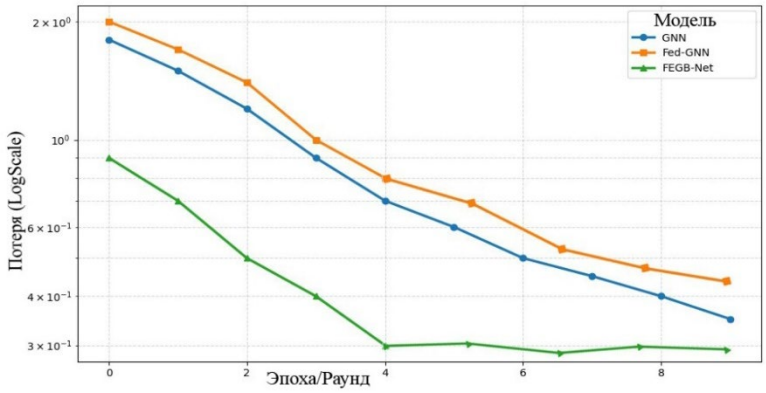

Рисунок 4 – Кривая потерь при обучении
Figure 4 – Training loss curve

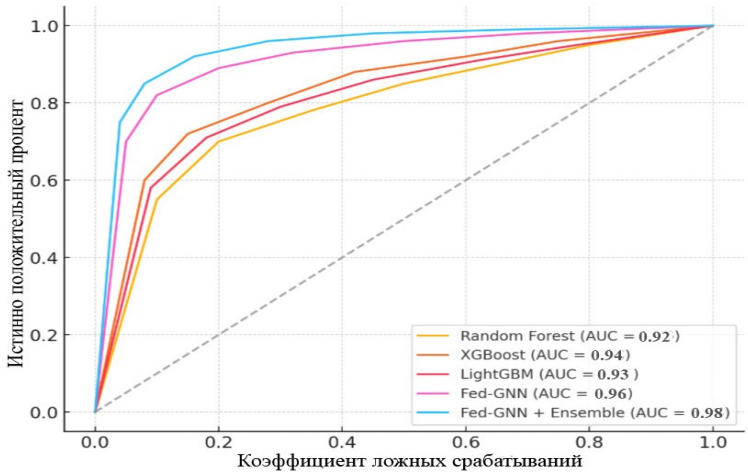

Рисунок 5 – Кривые AUC-ROC для разных моделей
Figure 5 – ROC curves for different models

Сравнительный анализ. Как показано в Таблице 5, точность слияния FEGB-Net (97,1 %) превосходит недавние подходы к глубокому обучению, такие как CNN-LSTM (93,7 %) [14] и автокодировщики (92,5 %) [15]. Более того, он достигает более высокой точности по сравнению с современными методами на основе трансформаторов, такими как Transformer-IDS (94,3%) [16] и гибридная архитектура CNN-Transformer (95,0 %) [17], которые недавно продемонстрировали высокую производительность. Важно отметить, что в отличие от этих моделей на основе трансформаторов и гибридных моделей, которые требуют централизованного хранения данных, FEGB-Net обеспечивает надежные гарантии конфиденциальности благодаря своему объединенному механизму обучения.

Таблица 5 – Сравнительный анализ точности FEGB-Net и существующих моделей обнаружения аномалий
Table 5 – Comparative accuracy analysis of FEGB-Net and existing anomaly detection models

Метод	Точность (%)	F1-оценка (%)	AUC-ROC
CNN-LSTM	93,7	91,2	0,94
Автокодировщик	92,5	89,8	0,93
Transformer-IDS	94,3	92,0	0,95
CNN-Transformer Hybrid	95,0	93,1	0,96
FEGB-Net (предлагается)	97,1	96,2	0,98

Заключение

В статье представлена архитектура FEGB-Net – гибридная система обнаружения аномалий, объединяющая федеративную графовую нейронную сеть с ансамблем методов машинного обучения (Random Forest, XGBoost, LightGBM) для повышения эффективности защиты. Достоинством FEGB-Net является сочетание федеративного обучения и ансамблевой классификации без обмена исходным трафиком, что обеспечивает сохранение конфиденциальности данных, при этом достигается точность до 97,1 %. Широкая оценка на полном наборе данных, включая метрики по каждому типу атаки, исследования абляции и анализ затрат на коммуникацию, продемонстрировала явное превосходство FEGB-Net над нефедеративными и традиционными подходами.

Новизна работы заключается в едином конвейере, сочетающем приватный Ф-ГНС и тройной ансамбль через обучаемый механизм мета-стэкинга, который интегрирует как графовые, так и табличные предсказания. Следует отметить ряд практических ограничений: операции обмена сообщениями в GNN и этап стэкинга в ансамбле привносят значительную вычислительную сложность, что может осложнить развертывание на устройствах с ограниченными ресурсами. В будущем планируется исследовать методы сжатия моделей, асинхронные схемы обновления и валидацию на других наборах данных для повышения эффективности и надежности решения в реальных условиях.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Singh N., Buyya R., Kim H. Securing Cloud-Based Internet of Things: Challenges and Mitigations. *Sensors*. 2025;25(1). https://doi.org/10.3390/s25010079
2. Neupane S., Ables J., Anderson W., et al. Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities. *IEEE Access*. 2022;10:112392–112415. https://doi.org/10.1109/ACCESS.2022.3216617
3. Chinnasamy R., Subramanian M., Easwaramoorthy S.V., Cho J. Deep Learning-Driven Methods for Network-Based Intrusion Detection Systems: A Systematic Review. *ICT Express*. 2025;11(1):181–215. https://doi.org/10.1016/j.icte.2025.01.005
4. Garg I., Sharma P., Singh G., Sharma P., Sharma V. Network Intrusion Detection System: Machine Learning Approach. In: *Proceedings of the 2nd International Conference on Advanced Computing & Communication Technologies (ICACCTech 2024), 16–17 November 2024, Sonipat, India.* IEEE; 2024. P. 222–229. https://doi.org/10.1109/ICACCTech65084.2024.00045
5. Wettewa S., Hou L., Zhang G. Graph Neural Networks for Building and Civil Infrastructure Operation and Maintenance Enhancement. *Advanced Engineering Informatics*. 2024;62. https://doi.org/10.1016/j.aei.2024.102868
6. Bhavani T.T., Rao M.K., Reddy A.M. Network Intrusion Detection System Using Random Forest and Decision Tree Machine Learning Techniques. In: *First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019, 29–30 March 2019, Jaipur, India*. Singapore: Springer; 2020. P. 637–643. https://doi.org/10.1007/978-981-15-0029-9_50
7. Zuo F., Zhang D., Li L., He Q., Deng J. GSOOA-1DDRSN: Network Traffic Anomaly Detection Based on Deep Residual Shrinkage Networks. *Heliyon*. 2024;10(11). https://doi.org/10.1016/j.heliyon.2024.e32087
8. Wang Ya. Deep Learning-Based Network Intrusion Detection Systems. *Applied and Computational Engineering*. 2024;109:179–188. https://doi.org/10.54254/2755-2721/2024.18104

9. Fink O., Wang Q., Svensén M., Dersin P., Lee W.-J., Ducoffe M. Potential, Challenges and Future Directions for Deep Learning in Prognostics and Health Management Applications. *Engineering Applications of Artificial Intelligence*. 2020;92. https://doi.org/10.1016/j.engappai.2020.103678
10. Sozol M.S., Saki G.M., Rahman M.M. Anomaly Detection in Cybersecurity with Graph-Based Approaches. *International Journal of Scientific Research in Engineering and Management*. 2024;8(8). https://doi.org/10.55041/IJSREM37061
11. Kalluri K. Federated Learning: A Privacy-Preserving Approach to Decentralized AI Systems. [Preprint]. ResearchGate. URL: https://www.researchgate.net/publication/388007124 [Accessed 13th March 2025].
12. Ennaji S., De Gaspari F., Hitaj D., Kbidi A., Mancini L.V. Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects. arXiv. URL: https://doi.org/10.48550/arXiv.2409.18736 [Accessed 13th March 2025].
13. Tarlow D., Moitra S., Rice A., et al. Learning to Fix Build Errors with Graph2Diff Neural Networks. In: *ICSEW'20: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, 27 June – 19 July 2020, Seoul, Republic of Korea.* New York: Association for Computing Machinery; 2020. P. 19–20. https://doi.org/10.1145/3387940.3392181
14. Vinayakumar R., Alazab M., Soman K.P., Poornachandran P., Al-Nemrat A., Venkatraman S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access.* 2019;7:41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
15. Zavrak S., İskefiyeli M. Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. *IEEE Access.* 2020;8:108346–108358. https://doi.org/10.1109/ACCESS.2020.3001350
16. Gan G., Kong W. Research on Network Intrusion Detection Based on Transformer. *Frontiers in Computing and Intelligent Systems*. 2023;3(3):22–26. https://doi.org/10.54097/fcis.v3i3.7987
17. Yao R., Wang N., Chen P., Ma D., Sheng X. A CNN-Transformer Hybrid Approach for an Intrusion Detection System in Advanced Metering Infrastructure. *Multimedia Tools and Applications.* 2023;82(13):19463–19486. https://doi.org/10.1007/s11042-022-14121-2

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Арм Ажи Азиз Салих, аспирант, Национальный исследовательский технологический университет «МИСИС», Москва, Российская Федерация.
e-mail: arm.azhi@yandex.com

Azhi A. S. Arm, Postgraduate, National Research University of Technology "MISIS", Moscow, the Russian Federation.

Ляпунцова Елена Вячеславовна, доктор технических наук, профессор, Национальный исследовательский технологический университет «МИСИС», Москва, Российская Федерация.
e-mail: liapuntsova.ev@misis.ru
ORCID: 0000-0002-3420-3805

Elena V. Lyapuntsova, Doctor of Engineering Sciences, Professor, National Research University of Technology "MISIS", Moscow, the Russian Federation.

Статья поступила в редакцию 11.04.2025; одобрена после рецензирования 02.06.2025; принята к публикации 10.06.2025.

The article was submitted 11.04.2025; approved after reviewing 02.06.2025; accepted for publication 10.06.2025.