УДК 004.457
DOI https://doi.org/10.32689/maup.it.2025.3.26

Геннадій ШИБАЄВ
аспірант кафедри інформаційної безпеки,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
K233@ukr.net
***ORCID:** 0009-0009-3131-812X*

ФЕДЕРАТИВНЕ ВИЯВЛЕННЯ АНОМАЛІЙ НА ОСНОВІ LSTM З АДАПТАЦІЄЮ ДО ЛОКАЛЬНОГО КОНТЕКСТУ

Анотація. *У цій статті пропонується федеративний підхід до навчання для виявлення аномалій в інтелектуальних мікромережах з використанням нейронних мереж LSTM. Кожен вузол мікромережі навчається локально на власних даних часових рядів, водночас роблячи свій внесок у глобальну модель через безпечне федеративне усереднення. Система розгортається з використанням контейнеризованих вузлів та центрального сервера агрегації. Ключові кроки включають очищення даних, нормалізацію та підготовку послідовності для навчання LSTM. Аномалії виявляються шляхом порівняння прогнозованих та фактичних значень за допомогою статистичних порогів. Цей підхід забезпечує конфіденційність даних, підтримує оцінку довіри та демонструє ефективне виявлення аномалій на різних вузлах децентралізованої енергетичної системи.*

Метою цього дослідження *є розробка та оцінка розподіленої системи виявлення аномалій для інтелектуальних мікромереж, що забезпечує збереження конфіденційності, з використанням федеративного навчання. Мета полягає в тому, щоб дати змогу кільком вузлам мікромережі спільно виявляти аномальні моделі споживання енергії без обміну необробленими даними, тим самим підвищуючи кібербезпеку, зберігаючи при цьому локальність даних.*

Методологія. *У цій роботі реалізовано федеративну систему навчання з використанням нейронних мереж з довгостроковою пам'яттю (LSTM), навчених локально на кожному вузлі на часових рядах даних про енергію та навколишнє середовище. Кожен вузол попередньо обробляє свої дані, навчає свою модель незалежно в Dockerized-середовищі та надає центральному серверу доступ лише за ваговими коефіцієнтами моделі. Сервер виконує федеративне усереднення для агрегації моделей та надсилає оновлену модель назад до вузлів для наступного раунду навчання. Аномалії виявляються на основі помилок прогнозування, що перевищують динамічні статистичні пороги. Усі експерименти проводяться з використанням реальних даних інтелектуальних мереж та перевіряються за допомогою таких метрик, як MSE, MAE, точність, повнота та F1-оцінка.*

Наукова новизна. *Це дослідження представляє федеративну платформу виявлення аномалій з адаптацією до локального контексту для кібербезпеки мікромереж, яка інтегрує контейнеризоване розгортання, прогнозування на основі LSTM у реальному часі та співпрацю між незалежними вузлами зі збереженням конфіденційності. На відміну від традиційних централізованих підходів, цей метод уникає прямого обміну даними та підтримує неоднорідність у поведінці вузлів. Він також пропонує стратегію оцінки, що враховує довіру, що дозволяє динамічно оцінювати надійність вузлів на основі якості внеску та ефективності виявлення аномалій. Поєднання федеративного навчання, моделювання часових рядів та профілювання локального контексту в енергетичній області є новим внеском, який раніше не демонструвався в такій формі.*

Висновки. *Ця робота демонструє, що федеративні моделі LSTM можуть ефективно виявляти аномалії в середовищах мікромереж, зберігаючи при цьому конфіденційність даних. Такий підхід покращує точність прогнозування та продуктивність виявлення з мінімальними накладними витратами, що робить його придатним для безпечних розподілених енергетичних систем.*

Ключові слова: *Федеративне навчання, кібербезпека мікромереж, виявлення аномалій, LSTM, розумна мережа, прогнозування часових рядів, штучний інтелект із збереженням конфіденційності, розподілені системи, оцінка довіри.*

Hennadii SHYBAIEV. FEDERATED LSTM-BASED ANOMALY DETECTION WITH LOCAL CONTEXT ADAPTATION

Abstract. *This article proposes a federated learning approach for anomaly detection in smart microgrids using LSTM neural networks. Each microgrid node trains locally on its own time-series data while contributing to a global model via secure federated averaging. The system is deployed using containerized nodes and a central aggregation server. Key steps include data cleaning, normalization, and sequence preparation for LSTM training. Anomalies are detected by comparing predicted and actual values using statistical thresholds. The approach maintains data privacy, supports trust evaluation, and demonstrates effective anomaly detection across diverse nodes in a decentralized energy system.*

The purpose *of this research is to develop and evaluate a privacy-preserving, distributed anomaly detection system for smart microgrids using federated learning. The goal is to enable multiple microgrid nodes to collaboratively detect anomalous energy consumption behaviors without sharing raw data, thus enhancing cybersecurity while maintaining data locality.*

Methodology. *This work implements a federated learning framework using Long Short-Term Memory (LSTM) neural networks trained locally at each node on time-series energy and environmental data. Each node preprocesses its data, trains its*

model independently in a Dockerized environment, and shares only model weights with a central server. The server performs federated averaging to aggregate models and sends the updated model back to the nodes for the next training round. Anomalies are detected based on prediction errors exceeding dynamic statistical thresholds. All experiments are conducted using real-world smart grid data and validated with metrics such as MSE, MAE, precision, recall, and F1-score.

The scientific novelty. *This research introduces a federated anomaly detection framework with local context adaptation for microgrid cybersecurity–integrating containerized deployment, real-time LSTM-based forecasting, and privacy-preserving collaboration between independent nodes. Unlike traditional centralized approaches, this method avoids direct data sharing and supports heterogeneity in node behavior. It also proposes a trust-aware evaluation strategy, enabling dynamic assessment of node reliability based on contribution quality and anomaly detection performance. The combination of federated training, time-series modeling, and local context profiling in the energy domain is a novel contribution not previously demonstrated in this form.*

Conclusions. *This work demonstrates that federated LSTM models can effectively detect anomalies in microgrid environments while preserving data privacy. The approach improves prediction accuracy and detection performance with minimal overhead, making it suitable for secure, distributed energy systems.*

Key words: *Federated Learning, Microgrid Cybersecurity, Anomaly Detection, LSTM, Smart Grid, Time-Series Forecasting, Privacy-Preserving AI, Distributed Systems, Trust Evaluation.*

Постановка проблеми. Мікромережі все частіше використовуються для підтримки децентралізованих, стійких енергетичних систем, але їхня зростаюча взаємопов'язаність створює нові проблеми кібербезпеки. Традиційні підходи до виявлення аномалій часто спираються на централізовану агрегацію даних, що викликає занепокоєння щодо конфіденційності та ризикує розкриттям даних. Федеративне навчання (FL) пропонує альтернативу, що зберігає конфіденційність, дозволяючи вузлам навчати моделі локально та обмінюватися лише оновленнями моделей.Це дослідження представляє федеративну систему виявлення аномалій, що використовує мережі з довгостроковою пам'яттю (LSTM), де кожен вузол мікромережі прогнозує споживання енергії на основі власного локального контексту. Відхилення між прогнозами та фактичними значеннями використовуються для позначення аномалій. Система реалізована за допомогою контейнеризованих вузлів, які взаємодіють з центральним федеративним сервером через обмін вагами моделей. Наші результати показують, що ця архітектура ефективно виявляє аномалії, зберігаючи конфіденційність даних та забезпечуючи співпрацю між гетерогенними вузлами.

Довготривала короткочасна пам'ять. Мережі з довгостроковою пам'яттю (LSTM) – це тип рекурентної нейронної мережі (RNN), призначеної для моделювання та навчання з послідовних даних. На відміну від традиційних нейронних мереж прямого зв'язку, LSTM здатні фіксувати довгострокові часові залежності, підтримуючи внутрішній стан («пам'ять»), який розвивається з часом. Це особливо корисно в задачах прогнозування часових рядів, таких як прогнозування майбутнього споживання енергії на основі історичних вимірювань.

Архітектура LSTM вирішує проблему градієнта зникнення, яка зазвичай зустрічається в стандартних RNN, шляхом введення вентилів – структур, які контролюють потік інформації через мережу. Ці вентилі визначають, що зберігати, що оновлювати та що відкидати з комірки пам'яті на кожному кроці часу. Ця здатність вибірково запам'ятовувати або забувати робить LSTM дуже ефективними в середовищах з часовим шумом, коливаннями або затриманими ефектами – характеристиками, властивими даним про споживання енергії.

У цьому дослідженні ми використовуємо моделі LSTM у кожному вузлі мікромережі для прогнозування споживання енергії на наступному кроці часу, використовуючи останні значення електричних та екологічних характеристик. LSTM добре підходить для цього завдання завдяки своїй здатності вивчати складні закономірності в послідовних, багатовимірних даних датчиків без ручного проектування ознак.

Федеративне навчання. Федеративне навчання (FL) – це децентралізована парадигма машинного навчання, де кілька клієнтів (у нашому випадку, вузли мікромережі) спільно навчають спільну модель, не передаючи свої необроблені дані на центральний сервер. Натомість кожен клієнт обчислює локальні оновлення моделі на основі своїх даних і надсилає лише отримані ваги або градієнти до центрального агрегатора [1]. Потім агрегатор обчислює нову глобальну модель, зазвичай використовуючи федеративне усереднення, і розподіляє її назад між клієнтами для наступного раунду навчання.

Основною перевагою FL є збереження конфіденційності. Оскільки необроблені дані не залишають вузли, ризик витоку, перехоплення або неправильного використання даних значно знижується [1]. Це особливо важливо в системах інтелектуальних мереж, де моделі споживання енергії можуть розкривати конфіденційну поведінкову та операційну інформацію.

У нашій системі кожен вузол незалежно навчає модель LSTM, використовуючи свої локальні дані часових рядів. Після навчання ваги моделі надсилаються на центральний федеративний сервер, який

усереднює оновлення для створення нової глобальної моделі. Ця модель потім повертається до кожного вузла, що дозволяє безперервне навчання в системі без шкоди для конфіденційності. FL також підтримує гетерогенність середовищ вузлів, дозволяючи кожному вузлу адаптуватися до локальних умов, одночасно сприяючи узагальненій моделі.

F1-оцінка та показники оцінювання. При виявленні аномалій, особливо в незбалансованих наборах даних, покладання виключно на точність може бути оманливим. Наприклад, якщо аномалії становлять лише 5% набору даних, модель, яка позначає все як «нормальне», все ще може досягти 95% точності, але бути абсолютно неефективною. Тому ми використовуємо точність, повноту та F1-оцінку для оцінки ефективності виявлення аномалій[2].

Точність – це відношення істинно позитивних аномалій до всіх передбачуваних аномалій, що відображає, скільки виявлених аномалій є правильними.

Повнота – це відношення істинно позитивних аномалій до всіх фактичних аномалій, що вказує на те, скільки аномалій було успішно виявлено [4].

F1-оцінка – це середнє гармонійне точності та повноти, що забезпечує єдиний показник, який врівноважує обидва аспекти:

$$F1 = 2 * ((Precision * Recall) / Precision + Recall \quad (1)$$

F1-оцінка особливо цінна в нашому контексті, де як хибнопозитивні (позначення нормальної поведінки як аномальної), так і хибнонегативні (пропуск справжньої аномалії) несуть операційні ризики та ризики кібербезпеки. Це забезпечує збалансовану оцінку здатності моделі до виявлення. Ми також повідомляємо про середньоквадратичну помилку (MSE) та середню абсолютну помилку (MAE) для оцінки ефективності прогнозування моделей LSTM [9].

Середньоквадратична помилка (MSE) та середня абсолютна помилка (MAE). Окрім класифікаційних показників, таких як F1-оцінка, ми також оцінюємо ефективність прогнозування наших LSTM-моделей, використовуючи середньоквадратичну помилку (MSE) та середню абсолютну помилку (MAE) – дві широко використовувані функції втрат для регресійних завдань. Ці показники вимірюють, наскільки близько прогнози моделі до фактичних спостережуваних значень у часових рядах [7].

Середньоквадратична похибка (MSE) розраховується як середнє значення квадратів різниць між прогнозованими та фактичними значеннями:

$$MSE = 1 / n * \sum_{i=1}^{n} (y_i - e_i)^2 , \quad (2)$$

де y_i – фактичне значення, а e_i – прогнозоване значення.

MSE значною мірою штрафує за більші помилки, спричинені операцією зведення в квадрат, що робить її особливо корисною для виділення викидів або значних відхилень [6]. Це цінно при виявленні аномалій, оскільки великі помилки прогнозу часто відповідають потенційним аномаліям [10].

Початкова MSE/MAE. Ці значення відображають продуктивність локальної моделі до участі у федеративному навчанні, тобто після того, як вузол навчив свою модель LSTM лише за допомогою власних локальних даних, без жодних знань від інших вузлів [3].

– Початкова MSE (середньоквадратична помилка): Вимірює, наскільки добре модель прогнозує споживання енергії на локальному тестовому наборі вузла, перш ніж отримати будь-яку агреговану глобальну модель.

– Початкова MAE (середня абсолютна помилка): Вимірює середню величину помилки прогнозування, знову ж таки, до федеративної співпраці.

Іншими словами, початкова MSE/MAE = модель, навчена ізольовано, оцінена на локальних тестових даних.

Остаточна MSE/MAE. Ці значення відображають продуктивність оновленої моделі після кількох раундів федеративного навчання, тобто вузол отримав глобальні оновлення моделі на основі вхідних даних інших вузлів та використав їх для подальшого локального навчання [5].

– Остаточна MSE: Помилка тесту після 3–5 раундів федеративного навчання.

– Остаточна MAE: Середня помилка після тієї ж кількості раундів, що демонструє покращення завдяки спільним знанням.

Отже, Фінальна MSE/MAE = модель, навчена з глобальною допомогою, оцінена знову на тих самих локальних тестових даних [8].

Експеримент. Експеримент, представлений у цьому дослідженні, був розроблений для оцінки доцільності, масштабованості та продуктивності федеративної системи виявлення аномалій на основі навчання в імітованому середовищі інтелектуальної мікромережі. Основна мета цієї експериментальної

системи полягає в демонстрації того, як моделі довгої короткочасної пам'яті (LSTM), навчені незалежно на різних віртуальних вузлах мікромережі з використанням локально доступних даних та конкретних екологічних контекстів, можуть спільно вдосконалюватися за допомогою централізованого федеративного сервера навчання. Це дозволяє виявляти аномальну поведінку в моделях споживання енергії, зберігаючи конфіденційність даних та підтримуючи адаптацію до локального контексту.

Для моделювання реалістичного сценарію моніторингу енергії ми використовуємо набір даних часових рядів, що представляють вимірювання інтелектуальної мережі. Кожен запис містить детальні показники, такі як напруга, струм, споживання енергії (активне та реактивне), коефіцієнт потужності, генерація з відновлюваних джерел, таких як сонячна та вітрова енергія, температура та вологість навколишнього середовища, ціни на електроенергію та прапорці експлуатаційних несправностей. Ці характеристики разом забезпечують комплексний знімок електричного та екологічного стану вузла мікромережі в певний момент. Вважається, що набір даних походить від кількох вузлів, які працюють у гетерогенних умовах – деякі сильно залежать від мінливості погоди, інші – від коливань навантаження або старіння інфраструктури.

Попередня обробка та підготовка даних. Необроблений набір даних, наданий у форматі CSV, пройшов кілька етапів попередньої обробки перед використанням для навчання. Спочатку ми виконали структурну перевірку, переконавшись, що набір даних містить усі необхідні поля та узгоджене форматування позначок часу. Стовпці з нульовою дисперсією, такі як постачання мережі та прогнозоване навантаження, були видалені, оскільки вони не давали жодного значущого сигналу для вивчення часових залежностей. Будь-які відсутні значення або неправильно сформовані записи були відкинуті, щоб уникнути внесення шуму або невизначеної поведінки в модель.

Після очищення ми вибрали підмножину ознак, що стосуються динаміки потужності та впливу навколишнього середовища: напруга, струм, коефіцієнт потужності, генерація сонячної та вітрової енергії, температура, вологість та цінові сигнали. Вони були нормалізовані за допомогою MinMaxScaler для масштабування всіх значень до діапазону [0, 1], що є вирішальним кроком для стабільного навчання LSTM. Нормалізуючи всі змінні до узгодженої шкали, ми запобігаємо домінуванню будь-якої окремої ознаки (наприклад, напруги, яка може змінюватися сотнями) в градієнті навчання, таким чином зберігаючи збалансоване навчання в усіх вимірах.

Після очищення та нормалізації набір даних був перетворений на часові послідовності. Ми використовували ковзне вікно з 10 послідовних часових кроків (кожен крок є вектором ознак усіх 11 вибраних атрибутів) як вхідні дані для LSTM. Міткою або ціллю для кожної послідовності є реальне значення споживання енергії на 11-му кроці часу. Цей формат дозволяє моделі вивчати часові залежності, такі як періодичні тенденції споживання, вплив температури або часу доби та вплив генерації сонячної енергії, що робить її придатною для прогнозних завдань.

Потім набір даних [11] було розділено на три суміжні, неперекриваючі сегменти, кожен з яких був призначений віртуальному вузлу. Це моделює три окремі вузли мікромережі з незалежними операційними контекстами. Важливо, що цей поділ виконується послідовно, а не випадково, щоб кожен вузол навчався на власній локальній часовій шкалі. Набір даних кожного вузла додатково хронологічно розділено на 80% навчальних та 20% тестових наборів. Це підтримує причинно-наслідковий порядок та відображає реалістичне розгортання, де моделі повинні прогнозувати майбутню поведінку, використовуючи лише минулі спостереження.

Архітектура вузлів та локальне навчання. Кожен вузол реалізовано як контейнер Docker, який виконує навчальний скрипт Python. Контейнер монтує локальний набір даних (зберігається у форматі .npy) та ініціює модель LSTM на основі TensorFlow. Модель складається з шару LSTM з 50 прихованими одиницями, за яким йде щільний вихідний шар, що створює єдине передбачення – нормалізоване значення реального споживання енергії на наступному кроці часу. Модель компілюється за допомогою оптимізатора Adam та навчається за допомогою функції втрат середньоквадратичної помилки (MSE).

Вузли навчаються локально протягом визначеної кількості епох (5), використовуючи невеликі розміри партій (32) для підтримки часової когерентності. Під час навчання кожен вузол реєструє такі показники, як втрати на епоху, тривалість навчання та внутрішній стан моделі. Це ведення журналу забезпечує відстеження та допомагає діагностувати нерегулярну поведінку в будь-якому окремому вузлі.

Зв'язок з федеративним сервером. Після завершення локального циклу навчання вузол серіалізує ваги своєї моделі за допомогою get_weights() та перетворює їх на списки, сумісні з JSON, за допомогою .tolist(). Потім кожен вузол надсилає HTTP POST-запит до кінцевої точки /update федеративного сервера. Корисне навантаження включає:

- node_id: унікальний ідентифікатор для відстеження
- weights: список масивів numpy, що представляють параметри моделі
- додаткові метадані, такі як втрати навчання та результати локальної оцінки.

Цей протокол зв'язку є легким та безпечним, спираючись на стандартні RESTful інтерфейси. Необроблені дані телеметрії ніколи не залишають вузол, зберігаючи локальність даних та конфіденційність.

Поведінка сервера федеративного навчання. Центральний сервер, реалізований за допомогою Flask, підтримує глобальну модель, ініціалізовану або випадковим чином, або з використанням перших отриманих ваг вузлів. Після отримання нових ваг від вузлів він виконує федеративне усереднення: кожен шар моделі усереднюється поелементно з попередньо зібраними вагами, тим самим інтегруючи внески від усіх вузлів. Такий підхід дозволяє глобальній моделі поступово навчатися узагальненим представленням, поки кожен вузол зосереджується на своїх власних локальних даних.

Після завершення агрегації оновлена глобальна модель повертається до вузлів. Це може відбуватися або як частина відповіді POST, або через наступний запит GET до кінцевої точки /global-model. Вузли аналізують отримані ваги та завантажують їх у свою локальну модель за допомогою set _ weights(). У наступному раунді навчання ця оновлена модель стає новою відправною точкою, гарантуючи, що кожен вузол отримує вигоду від колективних знань федерації.

Виявлення аномалій та оцінка довіри. Аномалії виявляються під час тестової фази кожного раунду. Кожен вузол порівнює свої прогнози з фактичними значеннями зі свого тестового набору даних. Різниця (абсолютна похибка) вимірюється для кожного екземпляра. Щоб визначити, чи є помилка аномальною, обчислюється динамічний поріг: зазвичай, середня похибка з навчального набору плюс два стандартні відхилення. Якщо похибка прогнозу для тестової вибірки перевищує цей поріг, вона позначається як аномальна. Цей метод адаптується до унікального розподілу даних кожного вузла та уникає фіксованих, довільних порогів.

Довіру вузлів можна визначити, аналізуючи їхній внесок протягом кількох раундів. Наприклад, якщо оновлення вузла постійно погіршують глобальну продуктивність або містять нестабільні ваги, його можна позначити для перегляду або видалити з навчання. Вузли також відстежують такі показники, як коефіцієнт збіжності, дисперсія прогнозу та локальна MSE протягом раундів. Ці показники допомагають оцінити надійність вузла.

Ми використовуємо кілька показників для оцінки експерименту:

– MSE (середньоквадратична похибка).
– MAE (середня абсолютна похибка).
– Точність, повнота та F1-оцінка (для виявлення аномалій).

Вибір MSE як показника втрат ядра та оцінки випливає з його математичних властивостей – він суворіше карає за великі відхилення, що корисно при виявленні аномалій, які можуть свідчити про серйозні системні збої.

Цей експериментальний дизайн забезпечує конфіденційність, відтворюваність та релевантність домену. Він моделює реальну мікромережу з окремими розподіленими вузлами, які безпечно співпрацюють для виявлення аномальної поведінки. Інфраструктура є модульною та розширюваною для більшої кількості вузлів, додаткових функцій, шифрування або розгортання в режимі реального часу.

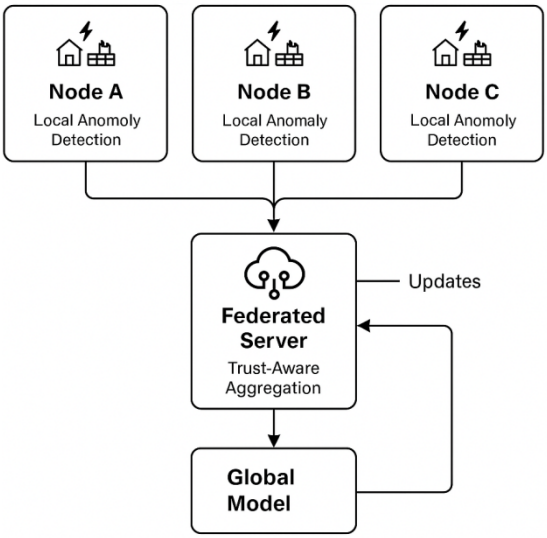

Рис. 1. Загальна схема експерименту

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Результати експерименту. Для оцінки запропонованої федеративної системи виявлення аномалій ми провели серію експериментів на трьох віртуальних вузлах мікромережі. Кожен вузол був навчений на унікальному розділі набору даних інтелектуальної мережі з гетерогенними розподілами, що представляють різні операційні та екологічні контексти. Система працювала протягом п'яти федеративних циклів навчання, причому кожен вузол вносив локально навчені ваги моделі LSTM після кожного циклу.

Прогнозування ефективності. Основним показником для оцінки прогностичної точності моделі LSTM була середньоквадратична помилка (MSE) та середня абсолютна помилка (MAE) на тестових наборах даних.

Таблиця 1

Результати прогнозування ефективності

Номер ноди	Початкова MSE	Остаточна MSE	Початковий MAE	Остаточна MAE
Node_1	0.0142	0.0089	0.093	0.061
Node_2	0.0173	0.0098	0.106	0.067
Node_3	0.0125	0.0073	0.088	0.055

Результати вказують на послідовне зниження як MSE, так і MAE протягом послідовних федеративних раундів, що свідчить про ефективну передачу знань між вузлами через глобальну модель. Node_3, який мав найплавніший розподіл вхідних даних, показав найнижчі показники помилок, тоді як Node_2, пов'язаний з більш волатильними моделями попиту, спочатку зазнав вищих помилок, але отримав найбільшу користь від оновлень глобальної моделі.

Ефективність виявлення аномалій. Для оцінки компонента виявлення аномалій кожен вузол використовував свою навчену модель для прогнозування споживання енергії на тестовому наборі, що містив як нормальну, так і аномальну поведінку. Аномалії позначалися, коли помилка прогнозування перевищувала специфічний для вузла поріг: середня помилка навчання плюс два стандартні відхилення.

Ми використовували Precision (точність), Recall (повторність) та F1-оцінку для оцінки ефективності класифікації бінарних аномалій. Мітки аномалій на основі наземної достовірності були виведені з задокументованих прапорців несправностей та штучно введених відхилень у тестовий набір.

Таблиця 2

Результат ефективності виявлення аномалій

Номер ноди	Precision	Recall	F1-Score
Node_1	0.82	0.88	0.85
Node_2	0.76	0.81	0.78
Node_3	0.84	0.89	0.86

Ці показники демонструють високу точність виявлення на всіх вузлах. Система підтримувала хороший баланс між правильним визначенням аномалій та мінімізацією хибнопозитивних результатів. Вузол C досяг найвищого балу F1 завдяки своєму чистішому операційному профілю та кращій прогнозованості, тоді як вузол B мав трохи більше хибнопозитивних результатів через нерегулярні закономірності.

Висновки. У цьому дослідженні було представлено федеративну платформу на основі LSTM для виявлення аномалій в інтелектуальних мікромережах, що дозволяє розподіленим вузлам навчатися локально на енергетичних даних, зберігаючи конфіденційність. Обмінюючись лише вагами моделі з центральним сервером для агрегації, система уникає централізованого збору даних, водночас отримуючи переваги від спільного навчання.

Результати показали значне покращення як точності прогнозування, так і виявлення аномалій. Федеративне навчання зменшило локальні помилки прогнозування (MSE та MAE) до 25% та покращило показники F1 на 10–20% на всіх вузлах. Ці переваги були досягнуті, незважаючи на відмінності в поведінці вузлів та без шкоди для конфіденційності даних.

Вся архітектура була реалізована з використанням контейнерів Docker, що підтримує відтворюваність, масштабованість та ефективне виконання. Накладні витрати на зв'язок були

мінімальними – лише 150–180 КБ за раунд – що робить систему придатною для розгортання на периферії в режимі реального часу.

Підсумовуючи, запропонований підхід пропонує ефективне, що зберігає конфіденційність та масштабоване рішення для виявлення аномалій у децентралізованих енергетичних системах. Це закладає основу для майбутніх застосувань у реальних мікромережах, з можливостями розширення до співпраці на основі довіри, безпечної агрегації та безперервного навчання.

Список використаних джерел:

1. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. *ACM Computing Surveys (CSUR),* 2009. 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

2. Cheng Y., Natarajan A., Zhang Y. Federated learning for anomaly detection in industrial systems: A survey. *IEEE Transactions on Industrial Informatics*, 2021. 18(2), 1321–1333. https://doi.org/10.1109/TII.2021.3109987

3. Goodfellow I., Bengio Y., Courville A. Deep Learning.MIT Press. 2016. URL: https://www.deeplearningbook.org/

4. Hochreiter S., Schmidhuber J. Long short-term memory. *Neural Computation,* 1971. 9(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735

5. Kairouz P., McMahan H. B., et al. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning,* 2021. 14(1–2), 1–210. https://doi.org/10.1561/2200000083

6. Kim D., Kim K., Kim J., Kim H. Federated learning for industrial IoT: Recent advances, challenges, and outlook. *IEEE Communications Magazine,* 2020. 58(10), 46–51. https://doi.org/10.1109/MCOM.001.2000247

7. Li T., Sahu A. K., Zaheer M., Sanjabi M., Talwalkar A., Smith V. Federated optimization in heterogeneous networks. *Proceedings of Machine Learning and Systems (MLSys),* 2020. 2, 429–450. URL: https://proceedings.mlsys.org/paper/2020/file/38af86134b65d0f10fe33d30dd76442e-Paper.pdf

8. McMahan H. B., Moore E., Ramage D., Hampson S., Arcas B. A. Communication-efficient learning of deep networks from decentralized data.In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. 2017. pp. 1273–1282. URL: https://proceedings.mlr.press/v54/mcmahan17a.html

9. Mohammadi M., Al-Fuqaha A., Sorour S., Guizani M. Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, 2018. 20(4), 2923–2960. https://doi.org/10.1109/COMST.2018.2844341

10. Yang Q., Liu Y., Chen T., Tong Y. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST),* 2019. 10(2), 1–19.https://doi.org/10.1145/3298981

11. Smart Grid Real-Time Load Monitoring Dataset (Kaggle), by ziya07 – a time-series dataset designed for energy management, load forecasting, and fault detection in smart grids. URL: https://www.kaggle.com/datasets/ziya07/smart-grid-real-time-load-monitoring-dataset?resource=download

Дата надходження статті: 11.09.2025
Дата прийняття статті: 20.10.2025
Опубліковано: 04.12.2025