МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

ШУБИН БОГДАН ПЕТРОВИЧ

Кваліфікаційна наукова
праця на правах рукопису
УДК 004.652

Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою

122 – комп’ютерні науки

Дисертація на здобуття наукового ступеня
доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____/Б.П. Шубин/

Науковий керівник

Максимюк Тарас Андрійович, д.т.н., доцент

Львів – 2025

АНОТАЦІЯ

Шубин Б.П. Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 "Комп'ютерні науки". – Національний університет "Львівська політехніка", Львів, 2025.

У дисертаційній роботі розв’язано наукову задачу розроблення нових та вдосконалення існуючих методів та моделей федеративного машинного навчання для інформаційно-комунікаційних систем автоматизованого управління, з метою підвищення точності в умовах неповноти, нестаціонарності даних та обмеженості обчислювальних ресурсів кінцевих пристроїв

Розроблено метод багатораундного федеративного навчання, який на відміну від відомих, використовує хронологічну стратифікацію навчальної вибірки, з поетапним усередненням агрегованих моделей кожного раунду. Розроблено структурно-функціональну модель інтелектуальної інформаційно-комунікаційної системи, яка базується на відокремленні площини пристроїв, площини передавання даних, площини автоматизованої інфраструктури та площини інтелектуальної обробки даних, які взаємодіють на основі спільного онтологічного ядра. Удосконалено метод обчислення параметрів агрегованої моделі федеративного навчання, введенням додаткового середньозваженого критерію оцінювання ефективності локальних моделей кінцевих пристроїв.

Розділ 1 «Аналіз сучасних методів та моделей побудови інтелектуальних інформаційно-комунікаційних систем» присвячено аналізу сучасних методів та моделей побудови інформаційно-комунікаційних систем автоматизованого управління індустріальною інфраструктурою з використанням елементів штучного інтелекту. Визначено, що перехід від Індустрії 4.0 до Індустрії 5.0 формує нові вимоги до кіберфізичних виробничих та невиробничих комплексів, що, у свою чергу, стимулює перехід до децентралізованих граничних обчислень та методів федеративного навчання. Окреслено основні виклики та обмеження стосовно інтеграції федеративного навчання в індустріальних системах.

Розділ 2 «Розроблення методів та моделей інтеграції федеративного навчання в інформаційно-комунікаційних системах» присвячено формуванню цілісної методологічної основи інтеграції федеративного навчання в інформаційно-комунікаційні системи автоматизованого управління, що охоплює всі ключові рівні від периферійних пристроїв до хмарного інтелектуального ядра. Представлено ієрархічну структурно-функціональну модель, яка завдяки децентралізації ресурсів та стандартизованим інтерфейсам забезпечує масштабованість, відмовостійкість та горизонтальне перенесення знань між галузями. Представлено розроблений метод обчислення параметрів агрегованої моделі, шляхом введення додаткового середньозваженого критерію оцінювання ефективності локальних моделей кінцевих пристроїв. Описано розроблений метод багатораундного федеративного навчання для кінцевих пристроїв з обмеженими обчислювальними ресурсами, який використовує хронологічну стратифікацію навчальної вибірки.

Розділ 3 «Імітаційне моделювання та дослідження показників ефективності функціонування інтелектуальної інформаційно-комунікаційної системи» висвітлює комплексне експериментальне випробування розроблених алгоритмів федеративного навчання на телеметричних даних автономних пристроїв з різною кількістю раундів тренування. Запропонований метод агрегації, у межах якого вагомість локальних моделей визначаються їхньою актуальною прогностичною точністю, продемонстрував середнє зниження середньоквадратичної та середньої абсолютної помилки на 19% порівняно з існуючими методами федеративного навчання, що підтверджує доцільність і практичну ефективність розробленого методу для індустріальних систем автоматизованого управління.

Розділ 4 «Практична реалізація інтелектуальної інформаційно-комунікаційної системи управління індустріальною інфраструктурою» присвячено впровадженню та експериментальній оцінці розробленого алгоритму на реальних периферійних пристроях AGV Formica-1. Зокрема, реалізовано програмно-апаратну модель інтелектуальної інформаційно-

комунікаційної системи, яка забезпечує наскрізний контур «дані-аналітика-управління» для автономних транспортних роботів та стаціонарних технологічних ліній. На базі цієї моделі впроваджено граничне федеративне навчання з використанням розроблених алгоритмів, яке дало змогу здійснювати локальне тренування нейронних мереж. Результати експериментів свідчать про те, що розроблений алгоритм багатораундного федеративного навчання підвищує енергетичну ефективність процесу федеративного навчання на кінцевих пристроях на 37% при використанні 4 раундів навчання та на 50% - при використанні 8 раундів навчання при забезпеченні аналогічної похибки прогнозування часових характеристик індустріальної системи.

Висновок підсумовує основні результати дисертаційної роботи та розв’язок наукової задачі розроблення нових та вдосконалення існуючих методів та моделей федеративного машинного навчання для інформаційно-комунікаційних систем автоматизованого управління, з метою підвищення точності прийняття рішень в умовах неповноти й нестаціонарності даних та обмежених обчислювальних ресурсів кінцевих пристроїв.

Основні наукові результати дисертації опубліковано в 25 працях, зокрема: 2 статті у наукових фахових періодичних виданнях України; 12 статей у наукових періодичних виданнях інших держав, які включені до наукометричних баз; 1 стаття у періодичному виданні України, 10 публікацій у матеріалах міжнародних та всеукраїнських наукових, науково-технічних конференцій.

Ключові слова: інформаційно-комунікаційні системи, системи автоматизованого управління, федеративне навчання, індустріальний Інтернет речей.

ABSTRACT

Shubyn B.P. Methods and Models for Building Intelligent Information and Communication Systems of Automated Infrastructure Management. – Qualifying scientific work as a manuscript. Dissertation for the degree of Doctor of Philosophy in specialty 122 “Computer Science” – Lviv Polytechnic National University, Lviv, 2025.

The dissertation tackles the scientific problem of designing new and refining existing methods and models of federated machine learning for information and communication automated-control systems, with the aim of improving decision-making accuracy when data are incomplete, non-stationary, and processed under limited computational resources on edge devices.

A multi-round federated-learning method has been developed which, unlike known approaches, applies chronological stratification of the training data and stepwise averaging of the aggregated models produced at each round. A structural–functional model of an intelligent information and communication system is proposed: it distinguishes a device plane, data-transfer plane, automated-infrastructure plane, and intelligent data-processing plane, all interacting through a common ontological core. The procedure for computing the aggregated model’s parameters has been enhanced by introducing an additional weighted-average criterion that assesses the performance of local models on edge devices.

Chapter 1 “Analysis of current methods and models for building intelligent information and communication systems”, surveys contemporary approaches to the design of industrial automated information and communication systems that incorporate artificial-intelligence components. It demonstrates that the transition from Industry 4.0 to Industry 5.0 imposes new requirements on cyber-physical production and non-production complexes, thereby stimulating the adoption of decentralized edge computing and federated-learning techniques; the principal challenges and constraints of integrating federated learning in industrial systems are outlined.

Chapter 2 “Development of methods and models for integrating federated learning into information and communication systems”, establishes a coherent methodological framework that spans all key levels from edge devices to the cloud-based intelligent core. A hierarchical structural-functional model is introduced which, through clear resource decentralization and standardized interfaces, ensures scalability, fault tolerance, and horizontal knowledge transfer between sectors. The chapter details the refined aggregation procedure based on the additional weighted criterion and describes the multi-round federated-learning method for resource-constrained edge devices that employ chronological stratification of the training data.

Chapter 3 “Simulation modelling and investigation of performance indicators of the intelligent information and communication system”, presents comprehensive experimental trials of the proposed federated-learning algorithms on telemetry obtained from autonomous devices across different numbers of training rounds. The aggregation strategy whereby each local model is weighted by its current predictive accuracy reduced both mean squared error and mean absolute error by an average of 19 % compared with baseline federated-learning approaches, thereby confirming the practicality and effectiveness of the method for industrial automated-control systems.

Chapter 4 “Practical implementation of the intelligent information and communication system for industrial-infrastructure management”, covers deployment and experimental evaluation of the algorithm on Fromica-1 AGV edge devices. A hardware-and-software prototype implementing an end-to-end “data-analytics-control” loop for autonomous transport robots and stationary production lines was realised, enabling local neural-network training via edge-level federated learning. Experiments show that the proposed multi-round algorithm improves the energy efficiency of federated learning on edge devices by 37 % with four training rounds and by 50 % with eight rounds, while maintaining prediction errors for the system’s timing characteristics at a level comparable with the baseline.

The *conclusion* summarizes the principal results and the solution to the scientific problem of advancing methods and models of federated machine learning for information-and-communication automated-control systems, aimed at increasing decision-making accuracy under data incompleteness, non-stationarity, and restricted edge-device resources.

The main scientific results of the dissertation have been published in 25 works, including 2 articles in Ukrainian peer-reviewed journals, 12 articles in foreign peer-reviewed journals indexed by scientific databases, 1 article in other journal and 10 publications in international and Ukrainian conference proceedings.

Keywords: information-communication systems; automated-control systems; federated learning; industrial Internet of Things.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації:

1. B. Shubyn, D. Kostrzewa, P. Grzesik, P. Benecki, T. Maksymyuk, V. Sunderam, J.-H. Syu, J. C.-W. Lin, and D. Mrozek, “Federated learning for improved prediction of failures in autonomous guided vehicles,” Journal of Computational Science, p. 101956, 2023.

   Особистий внесок здобувача: розробка методу інтеграції федеративного навчання в середовище інтелектуального виробництва, розробка математичної моделі оцінки впливу локальних моделей на формування глобальної моделі, розробка алгоритму ітеративного оновлення моделей з метою постійного навчання системи, експериментальна оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

2. B. Shubyn, D. Mrozek, T. Maksymyuk, V. Sunderam, D. Kostrzewa, P. Grzesik, and P. Benecki, “Federated learning for anomaly detection in industrial IoT-enabled production environment supported by autonomous guided vehicles,” *Lecture Notes in Computer Science*, vol. 13353, 2022, pp. 409–421.

   Особистий внесок здобувача: розробка архітектурних підходів до впровадження федеративного навчання в середовище інтелектуального виробництва з метою покращення точності роботи прогностичних моделей з метою виявлення аномалій в інтелектуальних пристроях виробництва, проведення експериментів з метою оцінки доцільності застосування федеративного навчання в середовищі інтелектуального виробництва експериментальна запропонованих підходів, обговорення результатів, підготовка статті до друку.

3. T. Maksymyuk, J. Gazda, M. Liyanage, L. Han, B. Shubyn, B. Strykhaliuk, O. Yaremko, M. Jo, and M. Dohler, “AI-enabled blockchain framework for dynamic spectrum management in multi-operator 6G networks,” *Lecture Notes in Electrical Engineering*, vol. 831, 2022, pp. 322–338.

Особистий внесок здобувача: розроблення структурно-функціональної моделі інформаційно-комунікаційної системи, прогнозування часових характеристик в мережах мобільного зв'язку 6G, обговорення результатів, підготовка статті до друку.

4. A. Luntovskyy, B. Shubyn, T. Maksymyuk, and M. Klymash, "5G slicing and handover scenarios: compulsoriness and machine learning," *Lecture Notes in Networks and Systems*, vol. 212, 2021, pp. 223–255.

   Особистий внесок здобувача: проведення аналізу сучасних підходів до застосування машинного навчання в середовище мереж мобільного зв'язку 5G, розроблення імітаційної моделі застосування машинного навчання для оптимізації процесу хендоверу, обговорення результатів, підготовка статті до друку.

5. A. Luntovskyy and B. Shubyn, "Energy efficiency for IoT," Studies in Computational Intelligence, vol. 976, 2021, pp. 199–215

   Особистий внесок здобувача: проведення розширеного аналізу функціонування сучасних IoT систем з метою виділення основних викликів та протирічь, розробка методології оцінки енергоспоживання IoT пристроїв, обговорення результатів, підготовка статті до друку.

6. B. Shubyn, T. Maksymyuk, J. Gazda, B. Rusyn, and D. Mrozek, "Federated learning: A solution for improving anomaly detection accuracy of autonomous guided vehicles in smart manufacturing," *Lecture Notes in Electrical Engineering*, vol. 1198, 2024, pp. 746–761.

   Особистий внесок здобувача: проведення дослідження можливих архітектурних рішень інтеграції федеративного навчання в середовище інтелектуального виробництва, розробка підходів до оцінки прогностичних можливостей моделей машинного навчання з використанням федеративного навчання, експериментальна оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

7. A. Luntovskyy, L. Globa, and B. Shubyn, “From big data to smart data: The most effective approaches for data analytics,” Lecture Notes in Networks and Systems, vol. 152, 2021, pp. 23–40.

   Особистий внесок здобувача: проведення розширеного аналізу сучасних підходів до побудови аналітики в інтелектуальних інформаційно-комунікаційних системах. обговорення результатів, підготовка статті до друку.

8. P. Grzesik, P. Benecki, D. Kostrzewa, B. Shubyn, and D. Mrozek, “On-edge aggregation strategies over industrial data produced by autonomous guided vehicles,” Lecture Notes in Computer Science, vol. 13353, 2022, pp. 458–471.

   Особистий внесок здобувача: Розробка та впровадження підходу до збору даних з автономно керованих пристроїв Formica-1 в середовищі інтелектуального виробництва, обговорення результатів, підготовка статті до друку.

9. A. Volovyk, Y. Pyrih, O. Urikova, A. Masiuk, B. Shubyn, and T. Maksymyuk, “Dynamic system state estimation with resilience to observation data anomalies,” *Contemporary Mathematics* (Singapore), vol. 5, no. 1, 2024.

   Особистий внесок здобувача: розробка імітаційної моделі для виявлення аномалій, опрацювання результатів експериментальних досліджень, обговорення результатів, підготовка статті до друку.

10. T. Maksymyuk, J. Gazda, B. Shubyn *et al.*, “Metaverse of Things in 6G era: An emerging fusion of IoT, XR, edge AI and blockchain technologies,” *Lecture Notes in Electrical Engineering*, vol. 965, 2023, pp. 546–564.

    Особистий внесок здобувача: розроблення структурно-функціональної моделі проведення обчислень в інформаційно-комунікаційних системах, обговорення результатів, підготовка статті до друку.

11. B. Shubyn, P. Grzesik, T. Maksymyuk, D. Kostrzewa, P. Benecki, J.-H. Syu, J. C.-W. Lin, V. Sunderam, and D. Mrozek, “Resource consumption of federated learning approach applied on edge IoT devices in the AGV environment,” in

Computational Science – ICCS 2023, pp. 492–504, Springer Nature Switzerland, 2023.

Особистий внесок здобувача: розробка підходу до оцінки споживання ресурсів периферійних автономно керованих пристроїв розумного виробництва під час процесу навчання моделей використовуючи підходи федеративного навчання, експериментальна оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

12. P. Benecki, D. Kostrzewa *et al.*, "Towards detection of anomalies in automated guided vehicles based on telemetry data," *Lecture Notes in Computer Science*, vol. 14838, 2024, pp. 192–207.

Особистий внесок здобувача: розробка моделі машинного навчання з метою виявлення аномалій в автономно керованих пристроях на основі даних телеметрії, проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

13. Модель інтеграції федеративного навчання в мережі мобільного зв'язку п'ятого покоління. Шубин Б.П., Максимюк Т.А., Яремко О.М., Фабрі Л.П., Мрозек Д. Інфокомунікаційні технології та електронна інженерія. – 2022. – Т. 2, № 1. – С. 26–35.

Особистий внесок здобувача: побудова методу інтеграції федеративного навчання в середовищу мережі мобільного зв'язку, експериментальна оцінка прогностичної точності запропонованого підходу, обговорення результатів, підготовка статті до друку.

14. Метод адаптивного логічного розділення мережі 5G на основі глибокого навчання. Максимюк Т.А., Шубин Б.П., Мисаковець Д.О., Андрущак В.С., Думич С.С. Вчені записки Таврійського національного університету ім. В. І. Вернадського. Серія «Технічні науки». – 2020. – Т. 31(70), № 5. – С. 36–42.

Особистий внесок здобувача: опрацювання результатів експериментальних досліджень, проведення аналізу даних в мережах мобільного зв'язку 5G, обговорення результатів, підготовка статті до друку.

15. Управління мережами мобільного зв’язку 5G за допомогою використання технологій штучного інтелекту. Шубин Б.П., Климаш М.М., Масюк А.Р., Осташевський А.І. Інфокомунікаційні технології та електронна інженерія. – 2021. – Т. 1, № 1. – С. 1–10.

    Особистий внесок здобувача: опрацювання результатів експериментальних досліджень, експериментальна оцінка прогностичної точності рекурентних нейронних мереж в мережах мобільного зв’язку 5G, обговорення результатів, підготовка статті до друку.

Публікації, які засвідчують апробацію матеріалів дисертації:

16. B. Shubyn, D. Mrozek, L. Fabry, T. Maksymyuk, E. M. Amhoud, and J. Gazda, “Federated learning techniques for 5G mobile networks,” in *Proc. 16th Int. Conf. Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 653–657.

    Особистий внесок здобувача: розробка методу інтеграції федеративного навчання в середовище мереж мобільного зв’язку 5G, розробка середовища для моделювання та проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

17. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, and D. Mrozek, “Forecasting of energy consumption for anomaly detection in automated guided vehicles: Models and feature selection,” in *Proc. IEEE Int. Conf. Systems, Man and Cybernetics (SMC)*, 2022, pp. 2073–2079.

    Особистий внесок здобувача: розробка моделі машинного навчання з метою прогнозування енергоспоживання автономно керованих пристроїв, розробка імітаційної моделі для виявлення аномалій, проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

18. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, and D. Mrozek, “Optimizing telemetry signal influence for power consumption prediction,” in *Companion Proc. 2023 Genetic and Evolutionary Computation Conf.*, 2023, pp. 51–52.

Особистий внесок здобувача: розробка підходу до обробки та очистки телеметричних даних з метою отримання кращої прогностичної точності моделей машинного навчання, проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

19. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, J.-H. Syu, J. C.-W. Lin, V. Sunderam, and D. Mrozek, “Effective prediction of energy consumption in automated guided vehicles with recurrent and convolutional neural networks,” in *Proc. IEEE Int. Conf. Big Data (BigData)*, 2023, pp. 5024–5030.

    Особистий внесок здобувача: дослідження прогностичної точності сучасних архітектур рекурентних нейронних мереж в середовищі інтелектуального виробництва, проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

20. T. Maksymyuk, N. Lutsiv, B. Shubyn, J. Gazda, and O. Ivakhiv, “Feature engineering for deep learning-based anomaly detection in 5G and beyond,” in *Proc. IEEE Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, 2023, pp. 1110–1113.

    Особистий внесок здобувача: розроблено й обґрунтовано методики інженерії ознак для виявлення аномалій у мережах 5G, сформовано та підготовлено репрезентативні вибірки даних для машинного навчання, проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

21. P. Benecki, D. Kostrzewa, B. Shubyn *et al.*, “Enhancing anomaly detection in automated guided vehicles through feature weight optimization,” in *Companion Proc. 2024 Genetic and Evolutionary Computation Conf. (GECCO)*, 2024, pp. 79–80.

    Особистий внесок здобувача: розроблено та обґрунтовано метод оптимізації ваг ознак з метою підвищення точності виявлення аномалій в автоматично керованих пристроях у середовищі інтелектуального

виробництва, розроблено імітаційну модель для виявлення аномалій, проведення експериментальної оцінки запропонованих підходів, обговорення результатів, підготовка статті до друку.

22. A. Luntovskyy and B. Shubyn, “Advanced architectures for IoT scenarios,” in Proc. Int. Conf. Smart and Sustainable Technologies (SpliTech), 2020.

    Особистий внесок здобувача: проведення розширеного аналізу існуючих архітектурних рішень роботи IoT систем, розробка методології їх оцінки, обговорення результатів, підготовка статті до друку.

23. A. Luntovskyy, B. Shubyn, T. Maksymyuk, and M. Klymash, “Highly-distributed systems: What is inside?” in *Proc. IEEE Conf. Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 207–211.

    Особистий внесок здобувача: проведення розширеного аналізу функціонування розподілених систем, обговорення результатів, підготовка статті до друку.

24. A. Luntovskyy, T. Zobjack, B. Shubyn, and M. Klymash, “Energy efficiency and security for IoT scenarios via WSN, RFID and NFC,” in *Proc. IEEE Ukrainian Microwave Conf. (UkrMiCo)*, 2021, pp. 1–6.

    Особистий внесок здобувача: проведення розширеного аналізу функціонування IoT систем з метою визначення основних викликів та протирічь в інформаційно-комунікаційних системах автоматизованого управління, обговорення результатів, підготовка статті до друку.

25. M. Buchyn, A. Helesh, and B. Shubyn, “Information security during electronic voting: Threats and mechanisms for ensuring,” in *Proc. IEEE 4th Int. Conf. Advanced Information and Communication Technologies (AICT)*, 2021, pp. 266–269, doi: 10.1109/AICT52120.2021.9628971.

    Особистий внесок здобувача: проведення розширеного аналізу протоколів до безпеки конфіденційних даних, дослідження способів забезпечення безпеки даних, обговорення результатів, підготовка статті до друку.

    .

ЗМІСТ

ВСТУП 20

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА МОДЕЛЕЙ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ 27

1.1 Трансформація сучасних інтелектуальних інформаційних систем у рамках парадигми Індустрії 5.0 27

1.2 Тенденції переходу від хмарних до граничних обчислень в сучасних інформаційно-комунікаційних системах 32

1.3 Технологія федеративного навчання як відповідь на виклики конфіденційності та затримки 34

1.3.1 Класифікація архітектур інформаційно-комунікаційних систем для федеративного навчання 34

1.3.1.1 Централізоване федеративне навчання 34

1.3.1.2 Децентралізоване федеративне навчання 36

1.3.1.3 Напівцентралізоване федеративне навчання 38

1.3.2 Класифікація методів федеративного навчання за типами обробки даних в інформаційно-комунікаційних системах 40

1.4 Перспективи інтеграції федеративного навчання в середовище інформаційно-комунікаційних систем 42

1.5 Існуючі обмеження стосовно інтеграції федеративного навчання в середовище інформаційно-комунікаційних систем 44

1.6 Висновки до розділу 47

РОЗДІЛ 2. РОЗРОБЛЕННЯ МЕТОДІВ ТА МОДЕЛЕЙ ІНТЕГРАЦІЇ ФЕДЕРАТИВНОГО НАВЧАННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ 48

2.1 Розроблення структурно-функціональної моделі інформаційно-комунікаційної системи автоматизованого управління 48

2.1.1. Функціональна модель площини пристроїв інформаційно-комунікаційної системи автоматизованого управління 49
2.1.2. Функціональна модель площини передавання даних в інформаційно-комунікаційній системі 52
2.1.3. Функціональна модель площини автоматизованої інфраструктури в інформаційно-комунікаційній системі 54
2.1.4. Функціональна модель площини інтелектуальної обробки даних в інформаційно-комунікаційній системі 56
2.2 Розроблення методу середньозваженого оцінювання впливу локальних моделей при оновленні агрегованої моделі федеративного навчання 57
2.2.1 Проблема агрегації моделей у федеративному навчанні 57
2.2.2 Математичні моделі усереднення параметрів у федеративному навчанні 60
2.2.3 Методи персоналізованого усереднення параметрів для окремих клієнтів у федеративному навчанні 62
2.2.4 Методи на основі шарів та співставлення 63
2.2.5 Метод середньозваженого оцінювання впливу локальних моделей при оновленні агрегованої моделі федеративного навчання 65
2.3 Розроблення методу багатораундного федеративного навчання для систем автоматизованого управління 70
2.3.1 Методи покращення адаптивності моделей федеративного навчання в динамічних умовах 70
2.3.2 Методи дистиляції знань при гетерогенній архітектурі моделей федеративного навчання 73
2.3.3 Алгоритми ресурсно-орієнтованих граничних обчислень 75
2.3.4. Метод багатораундового федеративного навчання для індустріальних середовищ з високою динамікою 80
2.4 Висновки до розділу 83

РОЗДІЛ 3. ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ 85
3.1 Методика та результати експериментальної оцінки базового алгоритму федеративного навчання 85
3.2 Моделювання удосконаленого алгоритму федеративного навчання на даних телеметрії AGV Formica-1 при різній кількості раундів тренування ... 89
3.2.1 Усереднення локальних моделей за метрикою MSE 91
3.2.2. Оцінювання точності багатораундного усереднення 93
3.2.3 Оцінювання точності багатораундного усереднення з кумулятивним розширенням навчальних вибірок 98
3.3 Висновки до розділу 104
РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ІНДУСТРІАЛЬНОЮ ІНФРАСТРУКТУРОЮ 105
4.1 Структурно-функціональна модель інтелектуальної інформаційно-комунікаційної системи для автоматизованого управління інфраструктурою 105
4.2 Структурно-функціональна модель інтелектуального автономного мобільного робота Formica-1 108
4.3 Реалізація процесу збору даних з автономно керованих пристроїв розумного виробництва. 113
4.4. Експериментальні дослідження енергоспоживання на периферійному пристрої AGV при різних сценаріях федеративного навчання 115
4.4.1 Оцінка енергоспоживання при використанні LSTM у межах 1-раундового федеративного навчання 116
4.4.2 Оцінка енергоспоживання при використанні LSTM у межах 4-раундового федеративного навчання 116

4.4.3 Оцінка енергоспоживання при використанні LSTM у межах 8-раундового федеративного навчання 117
4.5 Моделі та архітектури розгортання федеративного навчання в індустріальних інформаційно-комунікаційних системах 121
4.5.1 Локалізоване федеративне навчання на виробничих серверах 121
4.5.2 Граничне федеративне навчання безпосередньо на AGV-пристроях .. 123
4.5.3 Порівняльний аналіз та критерії вибору архітектур федеративного навчання 124
4.6. Висновки до розділу 125
ВИСНОВКИ 127
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 130
ДОДАТОК А. АКТИ ВИКОРИСТАННЯ ТА ВПРОВАДЖЕННЯ 143
ДОДАТОК Б. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ 147

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

1. ML – Machine Learning;
2. FL – Federated Learning;
3. IoT – Internet of Things;
4. IIoT – Industrial Internet of Things;
5. DS – Distributed Systems;
6. AGV - Autonomous Guided Vehicles;
7. LSTM – Long Short-Term Memory;
8. OPC UA – Уніфікована архітектура обміну даними на відкритій платформі;
9. ІІКС – інтелектуальна інформаційно-комунікаційна система;
10. M2M – міжмашинна взаємодія.

ВСТУП

Актуальність теми. Поточні тенденції цифрової трансформації, відображені у концепції переходу від Індустрії 4.0 до Індустрії 5.0, активно стимулюють широке впровадження Інтернету речей, периферійних обчислень, штучного інтелекту та автономних роботизованих систем, які в сукупності формують єдину інтелектуальну інформаційно-комунікаційну інфраструктуру, яку можна використати для автоматизації виробничих та невиробничих процесів у різних галузях економіки. За даними провідних міжнародних аналітичних агентств, упродовж останнього десятиліття кількість пристроїв Індустріального Інтернету речей (IIoT), інтегрованих у виробничу або транспортну інфраструктуру, збільшилася більш ніж утричі, а обсяг даних, які генеруються такими пристроями, перевищує сотні петабайт на добу. Це, у свою чергу, спричиняє експоненційне зростання навантаження на канали зв’язку та центри оброблення даних. Аналіз існуючих інформаційно-комунікаційних систем автоматизованого управління свідчить про їх обмежену масштабованість і відмовостійкість при поточних темпах зростання кількості інтелектуальних кінцевих пристроїв та мобільних агентів, таких як автономно-керовані транспортні засоби (AGV – Autonomous Guided Vehicles) та безпілотні літальні апарати (БПЛА). Іншим обмежуючим фактором є висока складність розробки інтелектуальних методів автоматизованого управління інфраструктурою, як з точки зору вартості розгортання або оренди надпотужних дата-центрів, так і з точки зору наявності репрезентативних навчальних вибірок даних для навчання нейронних мереж. Додатковим обмеженням при формуванні ефективних навчальних вибірок для інтелектуальних алгоритмів, є політика доступу та обміну даними, зокрема і тими, які містять елементи комерційної таємниці та інтелектуальної власності. Для розв’язку даної проблеми, з’явилась методологія федеративного навчання, яка передбачає децентралізоване навчання на локальних пристроях, з подальшою агрегацією параметрів моделей (ваг або їх градієнтів) у єдину

модель, яка синхронізується на всіх пристроях. Такий підхід забезпечує збереження конфіденційності персональних даних та дає змогу адаптувати моделі до неоднорідних умов середовища.

Вагомий внесок у дослідження систем автоматизованого управління інфраструктурою внесли R. Isermann, праці якого стали методологічною базою для побудови модулів кіберфізичних об'єктів, а також J. Lee зі своїми науковими роботами з превентивного обслуговування виробничих ліній, які демонструють практичну інтеграцію аналітики з автоматизованими системами управління. Серед українських вчених, варто відзначити фахівців, які активно працюють над автоматизованими системами управління індустріальними процесами, серед яких В. Теслюк, І. Цмоць, М. Медиковський; фахівців з машинного навчання та штучного інтелекту: Н. Шаховська, В. Лукін, В. Хавалко, С. Субботін, В. Висоцька, А. Саченко; та фахівців з інформаційно-комунікаційних систем: М. Климаш, І. Демидов, М. Бешлей, О. Шпур. Серед фахівців, що безпосередньо розвивають методи федеративного навчання, варто відзначити вчених H. B. McMahan, D. Ramage, V. Smith, P. Kairouz, M. Bennis, J. Gazda, M. Dohler.

Проте, в контексті федеративного навчання є ряд протиріч, які ускладнюють його інтеграцію в індустріальних системах. Зокрема, динамічна природа даних IIoT призводить до того, що навчальні вибірки для окремих локальних агентів не завжди складаються із незалежних ідентично розподілених масивів даних, і відповідно, не гарантують збіжність глобальної моделі. Різні статистичні розподіли локальних агентів, унеможливлюють ефективне узагальнення особливостей усіх сценаріїв функціонування на рівні агрегованої моделі. Окрім того, обмежені ресурси кінцевих інтелектуальних пристроїв не дають змогу навчати локальні моделі на достатньо великих та інформативних вибірках даних, що, у свою чергу, обмежує точність агрегованої моделі.

Розв'язання цих суперечностей дасть змогу досягти синергетичного ефекту від широкого впровадження інтелектуальних інформаційно-

комунікаційних систем автоматизованого управління виробничими та невиробничими інфраструктурами, за рахунок експоненційного зростання обсягів даних для навчання і врахування досвіду усіх існуючих інтелектуальних агентів (пристроїв) при оновленні агрегованих моделей.

Таким чином, актуальною **науковою задачею дисертаційної роботи** є розроблення нових та вдосконалення існуючих методів та моделей федеративного машинного навчання для інформаційно-комунікаційних систем автоматизованого управління, з метою підвищення точності прийняття рішень в умовах неповноти й нестаціонарності даних та обмежених обчислювальних ресурсів кінцевих пристроїв.

Зв’язок роботи з науковими програмами, планами і темами. Дисертація виконувалася відповідно до тематичних планів науково-дослідних робіт Національного університету “Львівська політехніка”. Зокрема, в рамках держбюджетних науково-дослідних робіт «Розроблення новітньої децентралізованої мережі мобільного зв'язку на основі блокчейн-архітектури та штучного інтелекту для впровадження технологій 5G/6G в Україні» (ДБ/Блокчейн), (2020–2022 рр.), № держреєстрації 0120U100674; «Розроблення інноваційних методів та моделей побудови інтелектуальних інформаційно-комунікаційних систем для цифровізації промисловості» (2022–2024 рр.), № держреєстрації 0122U000817; «Розроблення інноваційних методів та засобів розгортання інтелектуальної інформаційної інфраструктури для подвійного використання в умовах цифрової трансформації України (2023–2025 рр.), № держреєстрації 0123U100232.

Крім того, дослідження виконувалось в межах програми Norway Grants 2014–2021, що реалізується національним центром досліджень та розвитку Польщі, у рамках проєкту «Автономні транспортні візки, інтегровані з колаборативними роботами для інтелектуальної промисловості» (контракт № NOR/POL-NOR/CoBotAGV/0027/2019-00).

Метою дисертаційної роботи є розроблення моделей та методів федеративного машинного навчання для підвищення ефективності інформаційно-комунікаційних систем автоматизованого управління виробничими та невиробничими інфраструктурами.

Для досягнення поставленої мети в роботі розв’язано такі завдання:

1. Аналіз сучасних методів та моделей побудови інформаційно-комунікаційних систем автоматизованого управління індустріальною інфраструктурою з використанням елементів штучного інтелекту.
2. Розроблення структурно-функціональної моделі інтелектуальної інформаційно-комунікаційної системи для автоматизованого управління інфраструктурою.
3. Розроблення методу середньозваженого оцінювання впливу локальних моделей при оновленні агрегованої моделі федеративного навчання.
4. Розроблення методу багатораундного федеративного навчання для кінцевих пристроїв з обмеженими обчислювальними ресурсами.
5. Розроблення алгоритмічно-програмного забезпечення інтелектуальної інформаційно-комунікаційної системи для практичної реалізації розроблених методів федеративного навчання.
6. Експериментальні дослідження розроблених методів та моделей для автоматизованого управління інтелектуальними роботизованими системами в реальному індустріальному середовищі.

Об’єкт дослідження – процеси оброблення даних при федеративному машинному навчанні в інформаційно-комунікаційних системах.

Предмет дослідження – методи, моделі та програмно-апаратні засоби інтелектуальних інформаційно-комунікаційних систем.

Методи дослідження. В процесі досліджень використано методи теорії ймовірності та математичної статистики, методи та засоби штучного інтелекту, та методи імітаційного моделювання. Для дослідження використано дані та програмно-апаратні інтелектуальні роботизовані системи індустріальної

інформаційно-комунікаційної системи реального виробництва в рамках співпраці з закордонними навчальними закладами та виробництвами.

Наукова новизна одержаних результатів полягає у тому, що:

1. *Вперше розроблено* метод багатораундного федеративного навчання, який на відміну від відомих, використовує хронологічну стратифікацію навчальної вибірки, з поетапним усередненням агрегованих моделей кожного раунду, що дало змогу знизити складність обчислень для мобільних кінцевих пристроїв федеративного навчання при збереженні точності результуючої агрегованої моделі.
2. *Вперше розроблено* структурно-функціональну модель інтелектуальної інформаційно-комунікаційної системи, яка на відміну від відомих, базується на відокремленні площини пристроїв, площини передавання даних, площини автоматизованої інфраструктури та площини інтелектуальної обробки даних, що взаємодіють на основі спільного онтологічного ядра, що дало змогу забезпечити інтероперабельність та обмін локальними навченими моделями між різними виробничими та невиробничими інфраструктурами в процесі федеративного навчання.
3. *Удосконалено* метод обчислення параметрів агрегованої моделі, шляхом введення додаткового середньозваженого критерію оцінювання ефективності локальних моделей кінцевих пристроїв, що дало змогу підвищити ефективність процесу федеративного навчання за рахунок зниження вагомості статистичних викидів та помилок локальних моделей при обчисленні агрегованої моделі.

Практичне значення одержаних результатів. Практична цінність роботи полягає у впровадженні отриманих наукових методів, алгоритмів та алгоритмічно-програмного забезпечення у реальній інформаційно-комунікаційній системі виробництва. Окремі наукові результати також використані в навчальному процесі та науково-дослідних роботах, що підтверджується актами впровадження. Зокрема:

1. Розроблене універсальне програмно-апаратне забезпечення для розгортання інтелектуальної інформаційно-комунікаційної інфраструктури на прикладі реального виробництва має практичну цінність для індустрії за рахунок можливості його використання в широкому спектрі кінцевих пристроїв та галузей застосувань.
2. Розроблений алгоритм обчислення агрегованих моделей федеративного навчання забезпечує підвищення достовірності прогнозування у задачах регресії, що підтверджується зниженням похибки при прогнозуванні енергоспоживання автономних транспортних засобів на 19% при їх функціонуванні у реальному виробничому середовищі.
3. Розроблений алгоритм багатораундного федеративного навчання дає змогу знизити похибку прогнозування агрегованих моделей до 10% в залежності від умов функціонування та кількості раундів для навчання.
4. Розроблений алгоритм багатораундного федеративного навчання підвищує енергетичну ефективність процесу федеративного навчання на кінцевих пристроях на 37% при використанні 4 раундів навчання та на 50% - при використанні 8 раундів навчання при забезпеченні аналогічної точності прогнозування часових характеристик індустріальної системи.

Особистий внесок здобувача. Основний зміст роботи, всі теоретичні та практичні результати, дослідження і висновки, які представлено до захисту, одержані автором особисто. У працях (Додаток Б), опублікованих у співавторстві, внесок Шубина Б.П. є вирішальним, зокрема авторові належать: структурно-функціональна модель інтелектуальної інформаційно-комунікаційної системи на основі федеративного навчання, метод обчислення параметрів агрегованої моделі, метод багатораундного федеративного навчання, методика оцінки енергетичної ефективності кінцевих пристроїв в процесі федеративного навчання, модель інтеграції федеративного навчання на основі хмарних сервісів, моделювання та прогнозування трафіку в інформаційно-комунікаційних системах та мережах мобільного зв’язку.

Апробація результатів дисертації. Основні наукові результати і положення дисертаційної роботи представлялися та були обговорені на міжнародних та всеукраїнських науково-технічних конференціях: International Conference on Computational Science – ICCS (Лондон, Велика Британія – 2022; Прага, Чехія – 2023; Малага, Іспанія – 2024); IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering – TCSET (Славське-Львів, Україна – 2020, 2022, 2024); IEEE International Conference on Problems of Infocommunications, Science and Technology – PIC S&T (Харків, Україна – 2020); IEEE International Conference on Advanced Information and Communication Technologies – AICT (Львів, Україна – 2021); IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics – UkrMiCo (Київ, Україна – 2021); IEEE International Conference on Systems, Man and Cybernetics – SMC (Прага, Чехія – 2022); IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems – IDAACS (Дортмунд, Німеччина – 2023); IEEE International Conference on Big Data – BigData (Сорренто, Італія – 2023); ACM Genetic and Evolutionary Computation Conference – GECCO (Лісабон, Португалія – 2023; Мельбурн, Австралія – 2024); International Conference on Smart and Sustainable Technologies – SpliTech (Спліт, Хорватія – 2020), International Conference Infocommunications – Present and Future – IPF (Одеса. Україна – 2020).

Публікації. За темою дисертаційної роботи опубліковано 25 наукових праць, серед яких: 2 статті у наукових фахових періодичних виданнях України; 12 статей у наукових періодичних виданнях інших держав, які включені до наукометричних баз Scopus/Web of Science; 1 стаття у періодичному виданні України, 10 публікацій у матеріалах науково-технічних конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел із 188 найменувань та додатків. Повний обсяг дисертації складає 150 сторінок, основний зміст викладено на 102 сторінках, де наведено 48 рисунків.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА МОДЕЛЕЙ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

1.1 Трансформація сучасних інтелектуальних інформаційних систем у рамках парадигми Індустрії 5.0

Упродовж останнього десятиліття концепція переходу від Індустрії 4.0 до Індустрії 5.0 сформувала якісно нові вимоги до створення кіберфізичних виробничих комплексів, у яких дані розглядаються як критичний актив, що визначає конкурентоспроможність підприємства та національної економіки в цілому (рис. 1.1) [1]. Масове розповсюдження пристроїв Інтернету речей, посилене стрімким розвитком мобільних мереж п’ятого та шостого поколінь, появою периферійних обчислень і сервісів штучного інтелекту, сприяло формуванню багаторівневих інформаційно-комунікаційних інфраструктур, що синхронно інтегрують сенсорні мережі, хмарні та туманні обчислення, а також автономні роботизовані системи [2, 3]. За таких умов пріоритет набувають методи, здатні забезпечити безперервний збір, оброблення й аналітику великих потоків неоднорідних даних у реальному часі з гарантованою конфіденційністю та високою відмовостійкістю [4]

Сучасні архітектури інтелектуальних інформаційно-комунікаційних систем умовно поділяють на централізовані хмароцентричні та децентралізовані периферійно орієнтовані рішення. У першому випадку аналітичні модулі розгортаються у віддалених дата-центрах, що полегшує масштабування обчислювальних ресурсів, однак збільшує латентність і створює «вузьке місце» у вигляді комунікаційних каналів [5]. Децентралізована парадигма, заснована на граничних обчисленнях, переносить обчислювальні процеси ближче до джерел даних, зменшуючи затримки та обсяги транзитного трафіку, водночас висуваючи високі вимоги до енергоефективності й гетерогенності програмно-апаратних платформ кінцевих пристроїв [6].

Рисунок 1.1. Порівняння концепцій Індустрії 4.0 та 5.0.

Оптимальним компромісом постає ієрархічна модель RAMI (Reference Architectural Model Industrie) 4.0 з її горизонтальною інтеграцією технологічних, інформаційних та бізнес-рівнів, розширена в Індустрії 5.0 за рахунок людського чинника та принципів сталого розвитку [7] (рис. 1.2).

Рисунок 1.2. Еталонна модель концепцій RAMI 4.0 з інтеграцією людського фактора.

Методологічне підґрунтя побудови ІІКС формують моделі цифрового двійника, багаторівневого агентного управління та інтегрованої аналітики. Принцип цифрового двійника, запропонований J. Lee для прогнозного обслуговування, дозволяє відтворювати у віртуальному просторі динамічний стан об’єкта упродовж усього життєвого циклу, що забезпечує оперативну валідацію керувальних дій та мінімізує простої виробничих ліній [8, 9]. Агенти розглядаються як автономні програмно-апаратні сутності, здатні на основі локальних спостережень приймати рішення та координувати поведінку з іншими агентами через протоколи взаємодії. Подібна багаторівнева система самоконфігурації та самооптимізації ґрунтується на принципах теорії управління R. Isermanna, де інтелектуальні сенсори та приводи утворюють замкнені контури із вбудованою діагностикою й адаптацією параметрів (рис. 1.3).

Рисунок 1.3. Графічне представлення циклу побудови ІІКС.

З появою великих розподілених наборів даних, сформованих мільйонами IIoT-пристроїв, особливої популярності набули методи машинного та глибинного навчання [10, 11]. Для класифікації та прогнозування використовуються згорткові, рекурентні, а також гібридні нейронні мережі з увагою [12-16], що забезпечують високі показники точності навіть за наявності зашумлених або пропущених даних [17]. Проте централізоване тренування таких моделей стикається з обмеженнями доступу до конфіденційної інформації, великими обсягами переданих даних та високими витратами на обчислювальну інфраструктуру [18]. Альтернативою став підхід федеративного навчання, при якому оптимізовані на локальних пристроях моделі передають до центрального оркестратора лише вагові коефіцієнти або їх градієнти [19, 20]. Така схема істотно підвищує рівень конфіденційності, одночасно зменшуючи пропускне навантаження мережі, однак загострює проблему статистичної неоднорідності (non-IID) даних та конвергенції глобальної моделі (рис. 1.4). [21, 22]

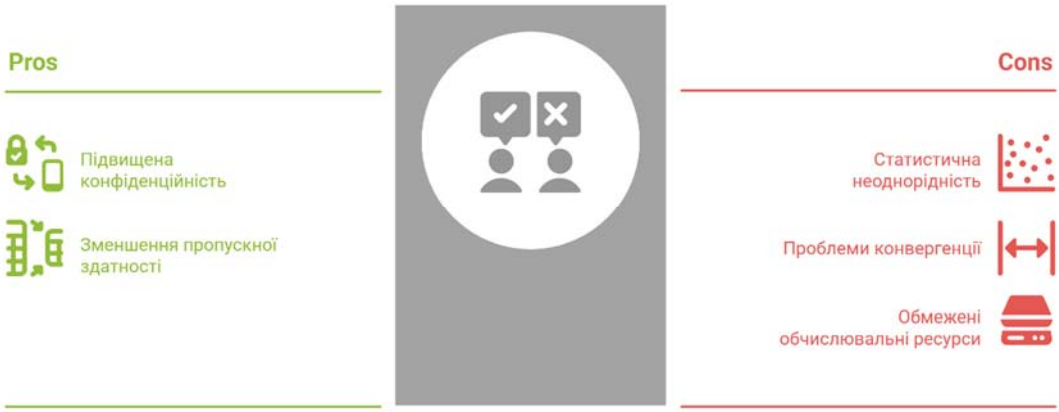


Рисунок 1.4. Графічне протиставлення переваг та недоліків федеративного навчання.

Незважаючи на значний прогрес, існує низка відкритих питань. По-перше, відсутність універсальної методики валідації гібридних моделей на реальних виробничих даних ускладнює порівняння результатів різних досліджень [23]. По-друге, зростаюча складність алгоритмів вимагає енергоефективних апаратних прискорювачів і стандартизованих інтерфейсів взаємодії між компонентами різних виробників [24]. По-третє, сучасні підходи до захисту даних ґрунтуються переважно на криптографічних протоколах, тоді як в Індустрії 5.0 важливо забезпечити ще й етичне регулювання штучного інтелекту, що враховує прозорість і підзвітність прийнятих рішень [25].

Синтез цифрових двійників, багаторівневих агентних моделей і федеративного машинного навчання формує теоретичне й практичне підґрунтя для розроблення нових методів, здатних забезпечити високу точність та оперативність ухвалення рішень навіть за умов неповноти, неоднорідності й швидкої зміни даних [26]. Саме вирішення цих питань становить основу подальших досліджень, спрямованих на підвищення ефективності та стійкості сучасних індустріальних екосистем [27]. З урахуванням викладених факторів, спостерігається активне впровадження великими виробничими компаніями новітніх технологій для моніторингу та глибшого розуміння власних операцій, а також для їх реалізації в режимі реального часу, що, у свою чергу, трансформує класичне виробництво в інтелектуальне.

1.2 Тенденції переходу від хмарних до граничних обчислень в сучасних інформаційно-комунікаційних системах

Експоненційне зростання обсягів промислової телеметрії є наслідком появи мільйонів IIoT-вузлів та широкого охоплення мобільними мережами 5G/6G – загострює обмеження традиційної хмарної парадигми. Централізовані дата-центри, що спираються на вертикальну передачу усіх «сирих» вимірювань, потребують значних витрат пропускної здатності та породжують небажану латентність, неприйнятну для керування в реальному часі [28]. До того ж передавання повних наборів даних поза периметром підприємства підвищує ризик витоку конфіденційної інформації та ускладнює дотримання регуляторних норм.

Хмарні сервісні платформи, такі як Google Cloud, Amazon Web Services, Microsoft Azure пропонують еластичне масштабування та широкий інструментарій оркестрації моделей машинного навчання, однак їх продуктивність визначається довжиною мережевого шляху до кінцевого вузла. У випадках, коли допуск затримки обмежується десятками мілісекунд, навіть оптимізовані CDN-механізми не гарантують детермінованого часу відгуку [29]. Водночас централізація створює «єдину точку збоїв»: у разі відмови каналу або атак на хмарний сегмент порушується робота всієї аналітичної системи.

Парадигма граничних (edge) обчислень компенсує ці недоліки, переміщуючи обробку даних «ближче до події». Edge-вузли, такі як промислові шлюзи та мобільні одноплатні комп’ютери, виконують фільтрацію, агрегацію та попереднє навчання моделей машинного навчання безпосередньо у виробничому цеху чи на борту робота, скорочуючи обсяг переданих даних і зменшуючи затримку реакції до одиниць мілісекунд [29]. Розвиток 5G-архітектури з підтримкою Mobile Edge Computing та профілів URLLC ще більше наближає хмарні сервіси до периферії, дозволяючи динамічно розміщувати мікросервіси аналітики безпосередньо в мережевій інфраструктурі.

Практично ефективною виявилася гібридна двошарова модель, у якій первинна обробка та аналітика виконуються на Edge-вузлах засобами Apache Flink чи Kafka Streams, а довгострокове навчання глибоких моделей здійснюється у хмарі з використанням GPU-кластерів. Така кооперація розподіляє навантаження, оскільки на рівні периферії забезпечується миттєва реакція та локальне прийняття рішень, у той час як у хмарному середовищі накопичуються історичні дані для ретроспективного аналізу та періодичного удосконалення моделей (рис. 1.5).

Рисунок 1.5. Графічне порівняння переваг хмарних та граничних обчислень.

Попри переваги, навіть гібридна схема стикається з двома системними протиріччями. По-перше, конфіденційні виробничі дані все ж потребують передавання до центру для фінального донавчання, що може порушувати політики локального зберігання. По-друге, малопотужні Edge-пристрої обмежені в обчислювальній та енергетичній можливостях, тому не здатні довго підтримувати складні архітектури глибоких нейронних мереж. Ці чинники створюють передумови для переходу до федеративного навчання, де ядро машинної обробки залишається на периферії, а до центру надходять лише

вагові коефіцієнти моделей, зберігаючи конфіденційність і різко зменшуючи трафік. Таким чином, у контексті Індустрії 5.0, саме поєднання Edge-аналітики з федеративними підходами формує технічну основу для енергоефективних та безпечних інформаційно-комунікаційних систем виробничого середовища.

1.3 Технологія федеративного навчання як відповідь на виклики конфіденційності та затримки

1.3.1 Класифікація архітектур інформаційно-комунікаційних систем для федеративного навчання

Поява багаторівневих інформаційно-комунікаційних інфраструктур з переважаючою складовою граничних обчислень та вимогами часу реакції в межах кількох мілісекунд зумовила пошук методів машинного навчання, які одночасно захищають первинні дані й уникають перевантаження каналів. Такою технологією стала концепція федеративного навчання (FL), запропонована Google у 2017 р. і нині стандартизована в 3GPP та ISO/IEC [19, 20]. Її принциповою відмінністю від класичних схем є розподілений характер тренування: моделі оптимізуються локально на периферійних пристроях або цехових серверах, а до координатора передаються лише вагові коефіцієнти чи їхні градієнти.

Федеративне навчання передбачає три ключові архітектурні підходи, а саме централізований, децентралізований і напівцентралізований, що ґрунтуються на різних концепціях багатосторонніх обчислень. Ці категорії відповідають різним обчислювальним структурам, які визначають правила обміну даними та оновлення моделей між учасниками.

1.3.1.1 Централізоване федеративне навчання

Централізоване федеративне навчання (рис. 1.6) передбачає модель, у якій центральний сервер координує агрегацію локально навчених моделей від кількох клієнтів. Такий підхід дозволяє здійснювати спільне навчання моделей із збереженням конфіденційності даних кожного учасника.

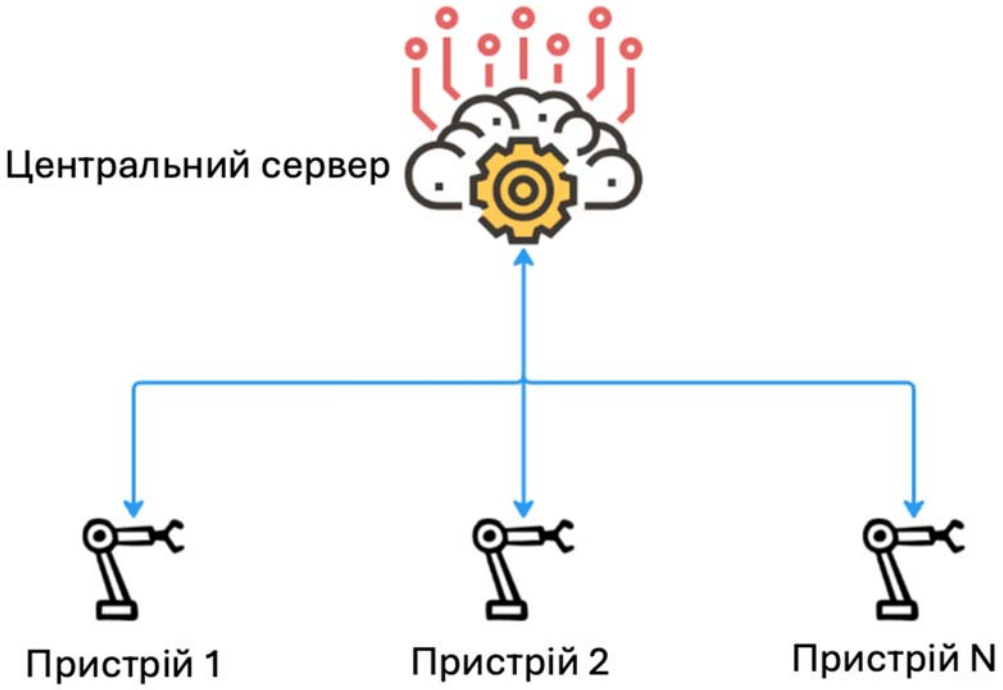


Рисунок 1.6. Централізоване федеративне навчання

Для забезпечення конфіденційності даних у централізованому федеративному навчанні використовуються різні механізми захисту. Одним з провідних підходів є диференційна конфіденційність, що вводить випадковий шум у дані або параметри моделі і знижує ризик витоку інформації. У централізованій архітектурі цей підхід реалізують на двох рівнях, центральному (CDP) і локальному (LDP). Методи CDP, зокрема біноміальний механізм [30], багатовимірний механізм Скеллама [31] та баєсівська диференційна конфіденційність [32], підвищують захист даних за мінімальних втрат точності. Гібридний підхід NbAFL [33] додає шум безпосередньо до ваг на стороні клієнта. У схемах LDP, до яких належать RAPPOR [34] і Shuffle Privacy [35], дані випадковим чином перетворюються на пристрої користувача ще до передавання, що гарантує високий рівень конфіденційності кожного учасника.

Централізоване федеративне навчання спрямоване на формування моделей з високою здатністю до узагальнення різнорідних клієнтських вибірок. Неоднорідність даних може знижувати точність прогнозу. Базовий алгоритм FedAvg [36] показує задовільні результати для незалежно та однаково розподілених вибірок. За гетерогенних даних доцільно застосовувати

персоналізовані клієнтські моделі або агностичне федеративне навчання [37], які враховують специфіку кожного клієнта і водночас підтримують цілісність глобальної моделі.

Ефективність централізованої схеми зменшується зі зростанням кількості клієнтів, оскільки основним вузьким місцем залишаються комунікаційні витрати на обмін параметрами між клієнтами і сервером. Статичні стратегії вибору клієнтів, наприклад випадкове підключення [36] або методи на основі рівнів [38], оптимізують використання ресурсів без погіршення якості навчання. Централізований підхід і надалі відіграє суттєву роль, адже забезпечує впорядковану координацію процесу і відкриває можливості для підвищення конфіденційності, точності та ефективності. Подальші дослідження мають спрямовуватися на інтеграцію новітніх технологій для подолання наявних викликів.

Класична архітектура федеративного навчання містить центральний сервер агрегації, який утворює єдину точку відмови, створює потенційні вузькі місця продуктивності та підвищує ризики для конфіденційності через наявність одного довіреного координатора. Децентралізоване федеративне навчання, схематично подане на рис. 1.7, усуває ці недоліки, адже власники даних взаємодіють безпосередньо і виконують агрегування параметрів колективно.

1.3.1.2 Децентралізоване федеративне навчання

У децентралізованому FL оновлення моделей і їхнє агрегування виконуються колективно всередині мережі вузлів-учасників, зазвичай із використанням протоколів безпечних багатосторонніх обчислень (MPC) або блокчейн-архітектур [39, 40]. У децентралізованому федеративному навчанні агрегування параметрів відбувається без опорного сервера, а власники даних обмінюються інформацією безпосередньо. Для збереження конфіденційності локальних вибірок у такій взаємодії найчастіше використовують протоколи багатосторонніх обчислень. До поширених підходів належать зашифровані схеми, секретне розділення та гомоморфне шифрування [41–43]. Зазначені

методи дають змогу виконувати колективні обчислення над вагами моделі, не розкриваючи приватних даних учасників. Блокчейн-платформи також розглядають як різновид децентралізованого федеративного навчання, оскільки вони забезпечують прозорість процесів і можливість незалежної верифікації, хоча вимагають додаткових заходів для захисту індивідуальних даних [39, 40].

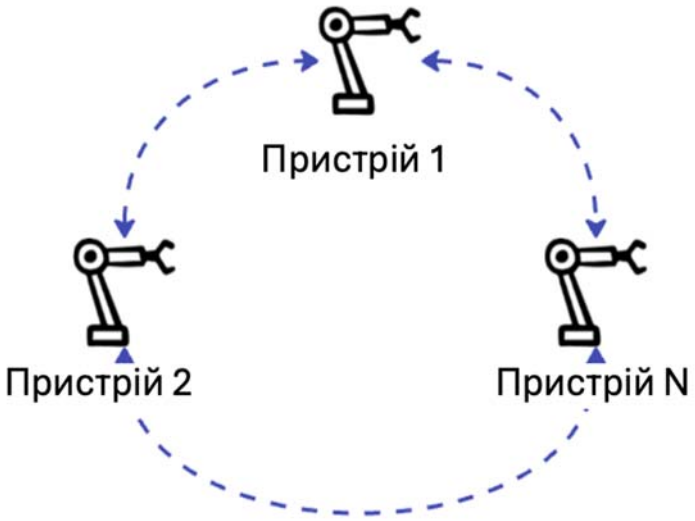


Рисунок 1.7 Децентралізоване федеративне навчання

Секретне розділення ділить локальні градієнти на кілька частин так, що кожен клієнт зберігає лише власну «долю», а відновлення повного вектора параметрів можливе лише за умови наявності достатньої кількості частин [41, 42]. Підхід добре масштабується з огляду на кількість учасників та спричиняє помірне обчислювальне навантаження. Проте універсальні протоколи багатосторонніх обчислень, зокрема SPDZ [46], досі створюють істотні комунікаційні витрати. Ранні реалізації федеративних систем на базі SPDZ поєднували секретне розділення Шаміра з подібними техніками, гарантуючи конфіденційність у середовищах часткової довіри [44, 45]. Комбінація секретного розділення і гомоморфного шифрування дає змогу зберегти точність моделі та підвищити рівень захисту [43], тоді як сучасні схеми агрегування оптимізують комунікаційний граф між учасниками [47].

Гетерогенність даних у децентралізованих мережах зумовлює істотні розбіжності статистичних розподілів між клієнтами, що уповільнює збіжність

алгоритмів і знижує точність глобальної моделі [48, 49]. Для зменшення негативного впливу неоднорідності пропонують коригувальні та ансамблеві підходи. Алгоритм SCAFFOLD вводить контрольні змінні, які компенсують клієнтські зміщення та прискорюють збіжність, зосереджуючись на зменшенні кількості переданих параметрів [49]. Ансамблеві методи, зокрема FedBoost, які покращують здатність моделі до узагальнення й забезпечують гарантовані межі похибки, хоча ускладнюють практичне розгортання через додаткову складність [50, 51].

Комунікаційні витрати залишаються одним із головних обмежень децентралізованого федеративного навчання, особливо під час тренування великих моделей глибинного навчання. Техніки стискання покликані зменшити обсяг передаваних даних ціною допустимого зменшення точності [52]. Первинні підходи впровадили схеми комунікаційного кодування, що мінімізують середньоквадратичну похибку без жорстких припущень щодо розподілу даних. Далі увагу зосередили на стисканні параметрів, вибірковій передачі підмножин і квантизації, наприклад FTTQ [53, 54]. Алгоритми FedCOM та FedCOMGATE поєднують стискання з періодичними оновленнями і гарантують збіжність як у однорідних, так і в гетерогенних умовах [55]. У рамках блокчейн-фреймворків стискання додатково підвищує безпеку та спрощує кешування контенту, що демонструє потенціал децентралізованого підходу підтримувати стабільну продуктивність разом з підвищеною конфіденційністю та ефективністю [56].

1.3.1.3 Напівцентралізоване федеративне навчання

Напівцентралізоване федеративне навчання, показане на рисунку 1.8, формує проміжну архітектуру між повністю централізованими та децентралізованими схемами. Централізована модель потребує значних мережевих ресурсів, а децентралізована обмежена масштабованістю багатосторонніх обчислень.

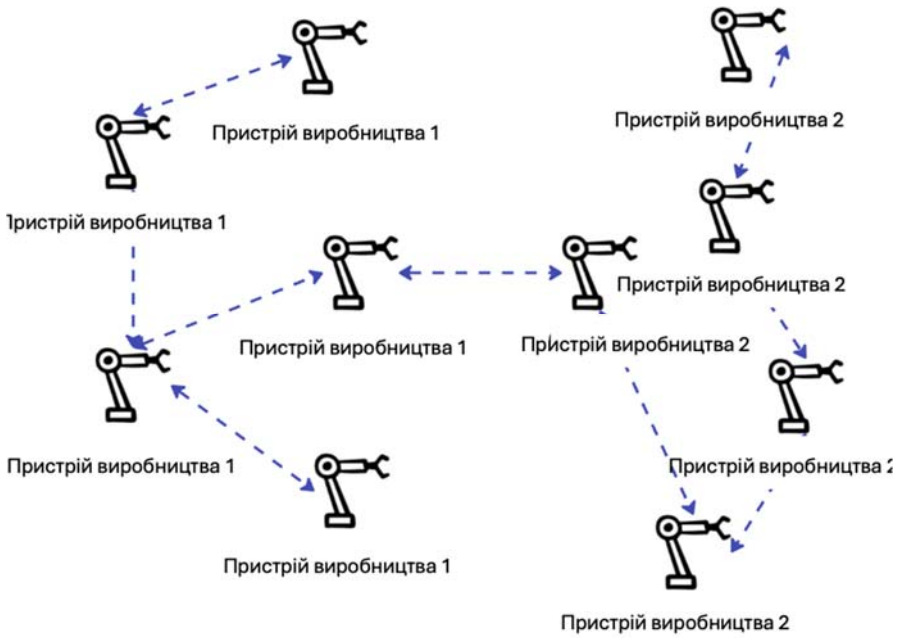


Рисунок 1.8. Напівцентралізоване федеративне навчання.

Напівцентралізований підхід запроваджує дворівневу структуру. Частина учасників виконує роль агентів і представляє кластери клієнтів. Локальні пристрої передають оновлення своєму агентові, а агенти обмінюються параметрами через децентралізований протокол колективних обчислень. Така організація зменшує обсяг переданої інформації й водночас зберігає ефективність та масштабованість, властиві централізованим системам.

Узагальнене порівняння даних підходів представлено на рис. 1.9.

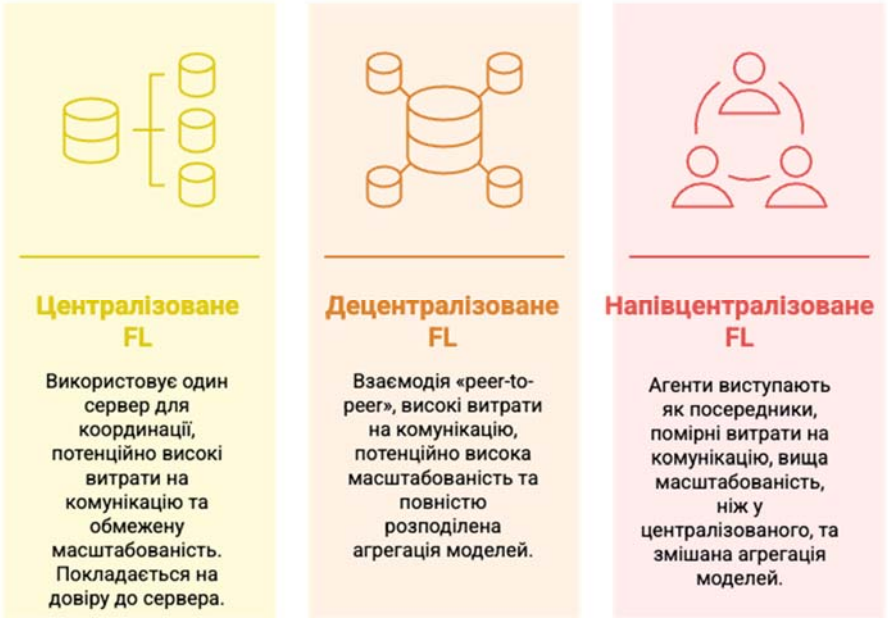


Рисунок 1.9. Порівняння підходів федеративного навчання

1.3.2 Класифікація методів федеративного навчання за типами обробки даних в інформаційно-комунікаційних системах

Логічна структура федеративного навчання залежить від подібності чи відмінності простору ознак і множини ідентифікаторів вибірок у різних власників даних. На цій підставі виокремлюють горизонтальну, вертикальну та перенесену форми. Горизонтальне федеративне навчання, або навчання на основі зразків, застосовують там, де простір ознак збігається, а множини ідентифікаторів різняться. Дані різних лікарень можуть містити однакові медичні показники, але стосуватися різних пацієнтів. У літературі наведено приклади використання HFL для класифікації електроенцефалограм з різних пристроїв та оптимізації потоків даних у мережах шостого покоління [17].

Вертикальне федеративне навчання, відоме як навчання на основі ознак, актуальне тоді, коли набори даних належать тим самим користувачам, проте містять різні типи ознак. Прикладом слугує кооперація фінансових установ, які об’єднують показники з різних підсистем для створення узгодженої моделі оцінювання кредитоспроможності [18].

Федеративне перенесене навчання застосовують у випадку, коли відмінності наявні і в просторі ознак, і в наборі ідентифікаторів. Метод дозволяє побудувати спільне представлення на підмножині схожих зразків. Такий підхід використано у системах моніторингу здоров’я на основі носимих пристроїв та у внутрішньому позиціонуванні з використанням Wi-Fi [20].

Поряд із класичними формами дослідники пропонують спеціалізовані архітектури, що долають обмеження схеми сервер – клієнт. Фреймворк MMVFL забезпечує конфіденційний розподіл міток між багатьма учасниками у вертикальній конфігурації. Середовище FEDF підтримує паралельне навчання моделей на географічно розподілених вибірках і тим самим підвищує точність і приватність. Персоналізоване навчання реалізовано у PerFit, де глобальна модель адаптується до індивідуальних вузлів Інтернету речей без втрати кооперативних переваг [57].

Для розумних міських систем запропоновано архітектуру StarFL, яка поєднує централізовані та децентралізовані механізми й обробляє великі міські масиви даних з дотриманням вимог конфіденційності [58]. Модель HFCL розв'язує проблему обмежених ресурсів частини периферійних пристроїв. Активні вузли виконують градієнтні обчислення локально, а пасивні передають дані на сервер параметрів [59]. У схемі CFL вузли обмінюються моделями без центрального сервера, що підвищує стійкість системи та зменшує залежність від хмарних сервісів [60].

Перелік наведених підходів свідчить, що гібридні та децентралізовані варіанти федеративного навчання здатні одночасно підвищувати безпеку, масштабованість і обчислювальну ефективність систем зі значною кількістю учасників (рис. 1.10).

Рисунок 1.10. Порівняння архітектур федеративного навчання

Для спрощення масштабу досліджень, у межах цієї дисертаційної роботи основну увагу приділено горизонтальному федеративному навчанню, оскільки саме цей підхід найкраще відображає структуру даних в індустріальних інформаційних системах. У виробничому середовищі численні вузли генерують

телеметрію з тотожним набором ознак, але різними множинами спостережень, що робить HFL придатним механізмом для колективного тренування моделей із збереженням конфіденційності. Локалізація даних дає змогу дотримуватися нормативних вимог і одночасно зменшувати мережеві витрати, що важливо в архітектурах граничних обчислень. Крім того, подібність технологічних процесів у різних підрозділах сприяє обміну знаннями та прискорює адаптацію локальних моделей, забезпечуючи масштабованість і надійність виробничих застосувань федеративного навчання.

1.4 Перспективи інтеграції федеративного навчання в середовище інформаційно-комунікаційних систем

Результати пілотних упроваджень федеративного навчання у глобальних мегаполісах переконливо демонструють його потенціал як методологічного підґрунтя для формування сучасної інформаційно-комунікаційної інфраструктури. Так, у Сінґапурі та Барселоні локальне навчання моделей розпізнавання дорожніх ситуацій безпосередньо на пристроях відеоспостереження з подальшим агрегуванням параметрів у муніципальному дата-центрі дало змогу зменшити мережевий трафік на 67 % порівняно із централізованими схемами, водночас утримавши точність класифікації на рівні 93–95 % [61]. Подальші дослідження у симуляційному середовищі Simulation of Urban MObility (SUMO) засвідчили, що використання технології Meta-Federated Learning у транспортній мережі з 420 перехресть підвищує точність прогнозування завантаженості смуг на 9–12 % відносно класичного FedAvg і скорочує середню тривалість поїздок на 18 % завдяки швидкій адаптації до локальних аномалій трафіку [62]. Аналогічні тенденції зафіксовано в системах балансування навантаження енергоспоживання: відмова від централізованого тренування на користь FL-платформ знизила середньодобове навантаження мережі з 2,3 % до 1,6 % і обмежила пікові відхилення на 14 %, причому всі операції залишилися у межах вимог стандартів NERC CIP щодо локального розміщення технологічних даних [63].

Утім, розгортання урбаністичних FL-платформ виявило низку системних бар’єрів. По-перше, необхідність синхронізувати гетерогенні периферійні вузли з нестабільними каналами зв’язку та обмеженими енергоресурсами ускладнює підтримку детермінованих часових вікон агрегації. По-друге, різнорідність правових режимів у суміжних муніципалітетах ускладнює міжмістовий обмін градієнтами й потребує єдиної регуляторної рамки. Сучасні дослідження пропонують вирішувати ці проблеми шляхом впровадження багатоярусних схем федеративного навчання з делегуванням проміжної агрегації на рівень районних хмар, інтеграції міських цифрових двійників для сценарного аналізу та залучення мереж 6G із нативною підтримкою URLLC-каналів, що забезпечують субмілісекундні цикли оновлення моделей у критично важливих сервісах.

Комплементарні експерименти в мобільних мережах п’ятого покоління засвідчили, що використання FL для виявлення аномалій у слайсі «інтернет речей» підвищує точність детектування DDoS-атак до 96,7 % проти 90,4 % у класичних IDS-рішеннях, а оптимізований розподіл трафіку зменшує середню затримку пакетів на 18 % [64]. Тим самим підтверджується доцільність включення федеративних механізмів до сервісної архітектури MEC-вузлів та NWDAF-аналітики.

У промислових середовищах високий ступінь фрагментації даних і суворі вимоги щодо їх конфіденційності, зумовлені контрактними обмеженнями, роблять централізовані сховища вразливими як технічно, так і регуляторно. Федеративне навчання, впроваджене, зокрема, на транспортних роботах AGV, дозволяє здійснювати локальне моделювання на базі периферійних IoT-сенсорів і передавати тільки параметри моделей до хмарного брокера, мінімізуючи ризик витоку й одночасно забезпечуючи достатню репрезентативність глобальної моделі (рис. 1.11) [65]. При цьому енергоспоживання кінцевих пристроїв оптимізується завдяки адаптивному плануванню клієнтів, а репутаційні механізми всередині двоступеневих архітектур (REACT) нейтралізують вплив зловмисних оновлень [66].

1.5 Існуючі обмеження стосовно інтеграції федеративного навчання в середовище інформаційно-комунікаційних систем

Інтеграція федеративного навчання в сучасні інформаційно-комунікаційні системи автоматизованого керування інфраструктурою Інтернету речей породжує низку взаємопов'язаних викликів, що охоплюють технічний, організаційний та регуляторний виміри. Першою фундаментальною проблемою є необхідність залучати великі масиви різнорідних даних для підвищення узагальнювальної здатності моделей за одночасного дотримання вимог конфіденційності. Відмова від централізованого накопичення сирих даних знижує ризик прямого витоку, проте ставить вимогу до захищеної агрегації градієнтів і до застосування криптографічного захисту каналів передавання.

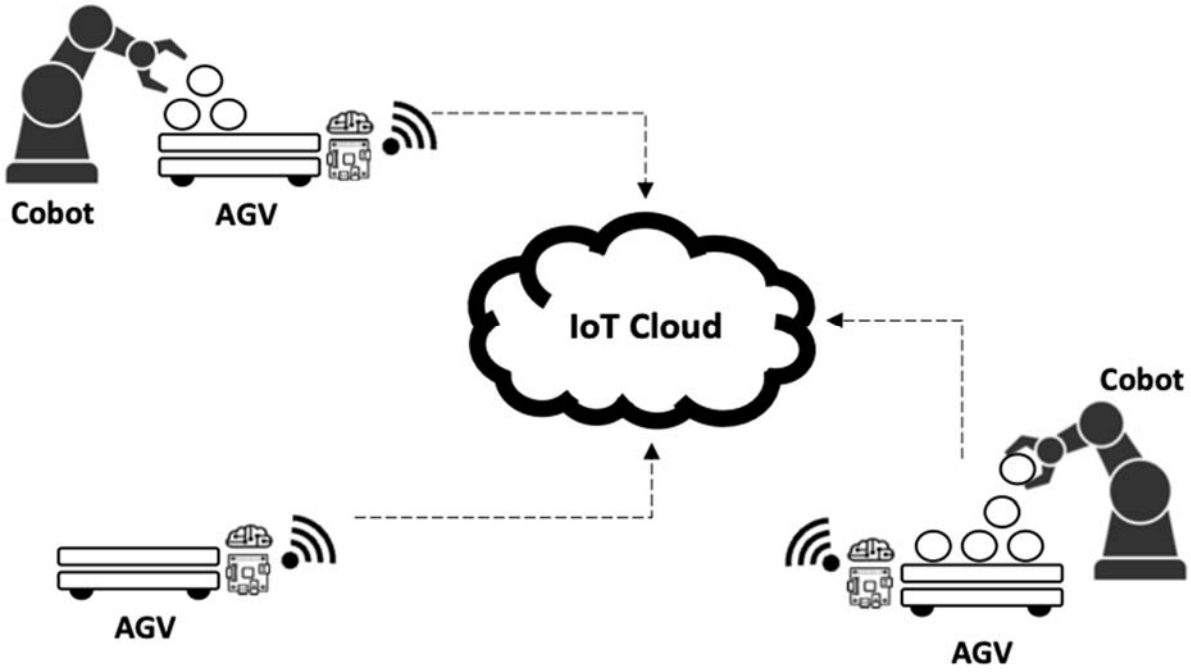


Рисунок 1.11. Приклад інтеграції федеративного навчання в індустріальних системах.

Другою точкою напруження виступає суперечність між статистично неоднорідною природою потоків IIoT-телеметрії та потребою у гарантованій збіжності глобальної моделі. Локальні вузли формують вибірки з відмінною статистикою. Це може призвести до ситуації, коли глобальний класифікатор не відображає особливостей рідкісних або критично важливих сценаріїв. Надання

таким вузлам підвищеної ваги зменшує дисперсію похибки, проте негативно впливає на стабільність і збільшує час збіжності, що несумісно з вимогами керування в режимі реального часу.

Третій виклик пов’язаний з обмеженими ресурсами крайових пристроїв. Зростання складності моделей, наприклад використання трансформерів для аналізу мультимодальних даних, конфліктує з енергетичними можливостями сенсорних вузлів та мобільних роботів. Компресія градієнтів, квантизація ваг і розріджені цикли оновлення зменшують навантаження на обчислювальні й мережеві ресурси, проте можуть погіршувати точність, особливо за швидкої деградації обладнання чи раптових змін технологічних умов.

Четвертий рівень проблем пов’язаний з обмеженою пропускною здатністю мережевої інфраструктури. Пакети Ultra Reliable Low Latency Communications забезпечують детерміноване керування технологічними процесами й мають співіснувати з трафіком федеративних сесій. Пріоритезація управлінського трафіку звужує часові вікна для колективного навчання. Збільшення частоти агрегацій ризикує перевантажити канал і підвищити латентність до значень, що є неприпустимими для виробничих циклів.

П’ятий блок викликів стосується кібербезпеки. Відсутність сирих даних у транспортному шарі не усуває ризиків отруєння моделі, крадіжки або виведення приватної інформації з оновлень ваг. Захист від цих загроз вимагає застосування схем secure aggregation, перевірки правдоподібності градієнтів і механізмів відхилення злоякісних клієнтів. Такі заходи підвищують обчислювальні витрати й ускладнюють масштабування федерації.

Важливим є і регуляторний аспект. Підприємства, що працюють у різних юрисдикціях, мають дотримуватися локальних вимог до конфіденційності. Часто ці вимоги не узгоджуються між собою. Уніфікація політик доступу до моделі в умовах мультинаціональної федерації потребує гібридних схем ліцензування та атестації безпеки, що подовжує цикл розроблення та сертифікації.

Окремо варто згадати проблему стандартизації. Інтероперабельність протоколів OPC UA, MQTT та DDS, а також оркестраторів на основі Kubernetes Edge залишається обмеженою. Різні реалізації механізмів оновлення контейнерів і обліку версій моделей ускладнюють міжплатформну міграцію сервісів та стримують масштабування інформаційно-комунікаційних систем.

Подолання перелічених обмежень потребує системних досліджень, координації зусиль промислових та академічних спільнот і розроблення нових стандартів на перетині обчислювальної інженерії та технічного регулювання. Це, у свою чергу, потребує розроблення моделей, методів та алгоритмічно-програмного забезпечення для підвищення точності алгоритмів федеративного навчання в інформаційно-комунікаційних системах автоматизованого управління виробничими та невиробничими інфраструктурами (рис. 1.12).

Рисунок 1.12. Структурно-функціональна схема досліджень в дисертаційній роботі

1.6 Висновки до розділу

Проведений аналіз підтвердив, що перехід від Індустрії 4.0 до Індустрії 5.0 формує нові вимоги до кіберфізичних виробничих та невиробничих комплексів. У цих умовах ієрархічна модель RAMI 4.0, доповнена чинником людини та принципами сталого розвитку, розглядається як оптимальна структура інтеграції технологічного, інформаційного й бізнес рівнів. Визначено, що сучасні архітектури інтелектуальних інформаційно-комунікаційних систем еволюціонують від централізованих хмарних до децентралізованих рішень. Поєднання Edge-аналітики з технологією федеративного навчання дає змогу зберегти конфіденційність даних і значно скоротити обсяг передаваних через мережу даних. Федеративне навчання проаналізовано у трьох архітектурних формах, централізовану, децентралізовану та напівцентралізовану. Показано, що централізована схема забезпечує впорядковану координацію процесів, проте створює єдину точку відмови та зростаючі комунікаційні витрати. Децентралізована модель усуває цей недолік, але потребує ресурсоємних протоколів багатосторонніх обчислень. Напівцентралізований підхід пропонує компроміс, делегуючи агрегацію обраним агентам і тим самим зменшуючи трафік без втрати масштабованості.

За типами структурованості даних виділено горизонтальне, вертикальне та перенесене федеративне навчання. Горизонтальна форма збігається з особливостями промислових вибірок, де різні вузли генерують дані з однаковими ознаками, але різними інстанціями. Саме тому горизонтальне федеративне навчання обрано в цій дисертаційній роботі як базовий об'єкт дослідження для інформаційно-комунікаційних систем виробничого середовища. Окреслено основні обмеження інтеграції федеративного навчання у промислові ІК-системи. До них належать протиріччя між необхідністю залучення великих масивів даних та вимогами конфіденційності, проблема статистичної неоднорідності вибірок, обмежені обчислювальні та енергетичні ресурси крайових вузлів.

РОЗДІЛ 2. РОЗРОБЛЕННЯ МЕТОДІВ ТА МОДЕЛЕЙ ІНТЕГРАЦІЇ ФЕДЕРАТИВНОГО НАВЧАННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1 Розроблення структурно-функціональної моделі інформаційно-комунікаційної системи автоматизованого управління

Поточні виклики та обмеження, сформульовані у попередньому розділі визначили потребу у багатоплощинній ієрархічній архітектурі, яка поєднує розподілену обробку на рівні кінцевих пристроїв з федеративним навчанням на рівні індустріальних доменів та глобальним агрегуванням моделей у хмарних платформах. Така модель покликана забезпечити масштабованість та відмовостійкість систем автоматизованого управління індустріальною інфраструктурою.

У даній роботі запропоновано ієрархічну структурно-функціональну модель інформаційно-комунікаційної інфраструктури, яка розмежовує функції збору даних, їх первинної обробки, прийняття рішень та реалізації функцій управління [67, 68] (рис. 2.1).

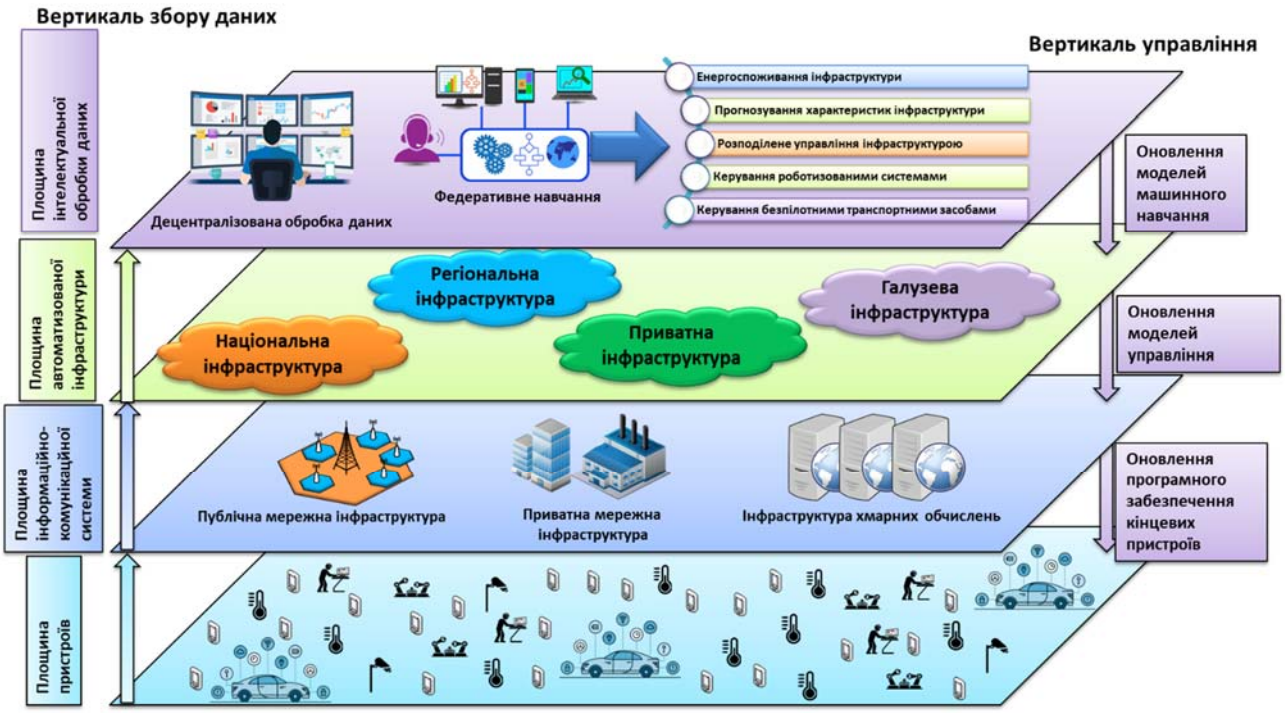


Рисунок 2.1. Структурно-функціональна модель інформаційно-комунікаційної системи автоматизованого управління гетерогенними інфраструктурами

2.1.1. Функціональна модель площини пристроїв інформаційно-комунікаційної системи автоматизованого управління

Нижній рівень інтелектуальної інформаційно-комунікаційної інфраструктури виконує повний локальний цикл навчання на вузлах інфраструктури. Кінцеві пристрої або виконавчі вузли зберігають синхронізовані часові ряди і зберігають їх у власній пам’яті. При необхідності може здійснюватися адаптивна фільтрація для відкидання випадкових збурень та вирівнювання частоти дискретизації [69]. Далі виконується обчислення векторів ознак, сформованих так, щоб їх можна було обробляти малорозмірними нейронними мережами.

Після накопичення достатнього обсягу даних, кінцевий вузол проводить локальне навчання нейронної мережі, із заздалегідь узгодженою архітектурою. Для цього завантажуються останні ваги моделі, які є відомими в пам’яті пристрою, і запускається процес навчання з використанням стохастичного градієнтного спуску та зворотного поширення помилки. Після завершення локального навчання, кожен пристрій передає оновлені вагові коефіцієнти моделі до верхньої площини інтелектуальної обробки даних використовуючи API-запити.

Нижній рівень ієрархії охоплює широкий спектр кінцевих інтелектуальних пристроїв, що відрізняються функціональним призначенням і умовами експлуатації. У дискретному виробництві до цього шару належать програмовані логічні контролери, роботизовані осередки складання, автоматичні конвеєри та автономні транспортні візки. Кожний модуль обладнано сенсорами положення, зусилля та вібрації, а також виконавчими приводами з цифровим зворотним зв’язком. У середовищі процесного виробництва функціонують інтелектуальні регулятори тиску, витрати й температури, які перетворюють аналогові сигнали у стандартизовані телеметричні пакети й здійснюють локальне навчання моделей прогнозного обслуговування (рис. 2.2).

У розумній міській інфраструктурі нижній шар формують відеокамери з вбудованими нейронними прискорювачами, інтелектуальні світлофори, датчики якості повітря та смарт-лічильники енергоресурсів. Кожний вузол агрегує багатомодальні дані, виконує легкі операції прогнозування або розпізнавання й передає оновлені ваги у транспортну площину з урахуванням поточного енергетичного профілю мережі живлення.

Рисунок 2.2. Типи та функціональні особливості кінцевих пристроїв в запропонованій архітектурі.

Для безпілотного транспорту типовими компонентами є блоки керування силовими установками автомобілів, лідари, радари та високочастотні модулі V2X (рис. 2.3). На борту дронів установлено одноплатні комп’ютери з енергоефективними графічними ядрами, які обробляють потоки з оптичних і тепловізійних камер. Локальне навчання виконується у часових вікнах між маневрами, тому архітектура підтримує асинхронний режим обміну, не перериваючи навігаційні цикли.

Запропонована ієрархія забезпечує інтероперабельність завдяки двом ключовим механізмам. По-перше, усі крайові вузли використовують єдину описову модель даних, засновану на узгодженому онтологічному ядрі. Це дає змогу роботизованому маніпулятору, міському світлофору й безпілотному автомобілю однаково позначати часові мітки, типи сенсорів і рівні пріоритетності трафіку. По-друге, контейнери з агентами локального навчання поширюються через спільний репозиторій і реалізують стандартизований інтерфейс середовища виконання. Один і той самий модуль фільтрації даних може працювати в OPC UA на виробництві, у ROS 2 на дроні або в мережі розумного міста без перекомпіляції вихідного коду програмного забезпечення (рис. 2.4).

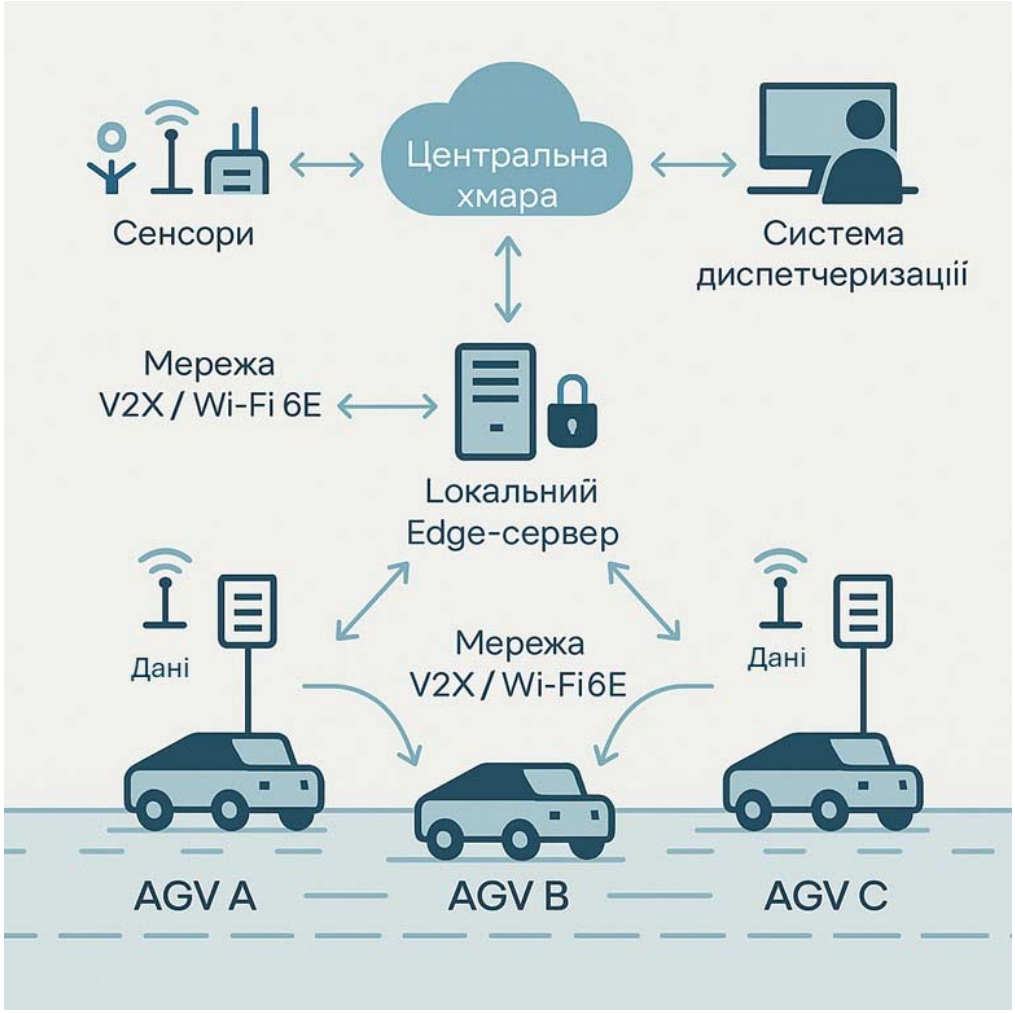


Рисунок 2.3. Концептуальна схема інтеграції федеративного навчання для безпілотних пристроїв в рамках інфраструктури розумних міст.

Єдність формату даних та контейнеризованого програмного стека дає змогу різним галузям обмінюватися ваговими оновленнями за спільними протоколами без додаткових перетворень. У результаті виробнича модель виявлення аномалій може бути використана як початкова ініціалізація для детектора дефектів дорожнього покриття, а статистика енергоспоживання міських ліхтарів дозволить покращувати прогноз ресурсу акумуляторів логістичних роботів. Таким чином, архітектура створює умови для горизонтального перенесення знань, знижуючи вартість розгортання інтелектуальних функцій у кожній галузі та прискорюючи їхню адаптацію до змінних умов експлуатації.

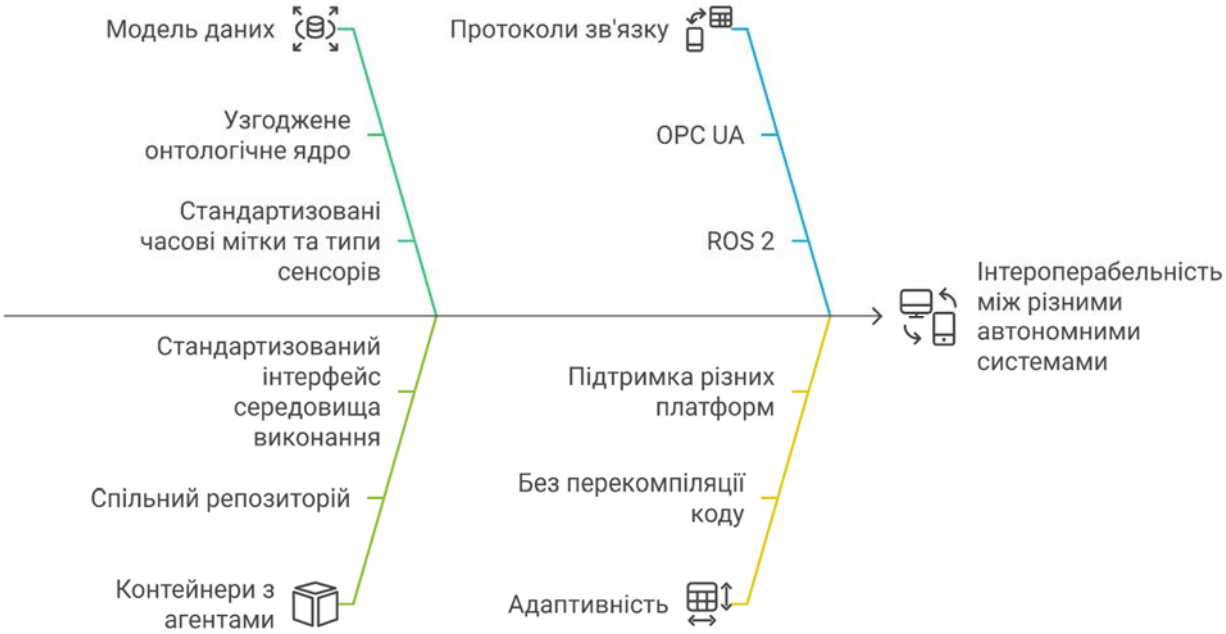


Рисунок 2.4. Інтероперабельність між кінцевими пристроями в межах інтелектуальної інформаційно-комунікаційної системи автоматизованого управління інфраструктурою.

2.1.2. Функціональна модель площини передавання даних в інформаційно-комунікаційній системі

Площина передавання даних виконує функцію єдиного логічного каналу між пристроями рівнем та верхніми рівнями обробки даних. Передусім вона забезпечує адресацію та контекстну аутентифікацію кожного вузла. Кожний пристрій під час приєднання реєструється у локальному домені і отримує

унікальний ідентифікатор сесії, пов’язаний із криптографічними ключами. Завдяки цьому будь-яке повідомлення, що покидає пристрій, уже містить перевірені атрибути походження, а отже додаткова перевірка на проміжних опорних точках не потрібна, що дає змогу знизити затримку.

Друга ключова функція полягає у класифікації пакетів за параметрами якості обслуговування. На вході до транспортної площини кожен кадр маркується міткою пріоритету, що відображає вимоги URLLC, eMBB або mMTC [68]. Цю мітку успадковують усі подальші протокольні інкапсуляції, тому незалежно від того, чи проходить трафік через публічний стільниковий сегмент, чи через приватну мережу виробництва, комутатори й маршрутизатори застосовують однакову політику планування ресурсів (рис. 2.5). При конфлікті ресурсів та потребі передавання даних у реальному часі, планувальник виділяє канал для URLLC і відтермінує еластичний трафік, зберігаючи детермінований час затримки для критичних даних. В окремих випадках на рівні мережі мобільного зв’язку 5G, забезпечується логічне розділення ресурсів, яке дає змогу створити ізольовані підмережі (Network Slicing), індивідуально для кожної індустріальної інфраструктури [70, 71].

Рисунок 2.5. Функціональні вимоги до площини передавання даних в залежності від обраної політики планування ресурсів.

Таким чином, площина передавання даних формує захищений, гнучкий і детермінований шлях від крайових пристроїв до інтелектуальних сервісів. Вона гарантує сталий час доставки для критичних пакетів, мінімізує зайві накладні

витрати на сигнальний трафік, підтримує безперервність сесій при мобільності вузлів і забезпечує контекстну обізнаність верхніх рівнів про здоров’я мережевої інфраструктури.

2.1.3. Функціональна модель площини автоматизованої інфраструктури в інформаційно-комунікаційній системі

Площина автоматизованої інфраструктури формує середній рівень ієрархії та відокремлює ресурси за доменною належністю (рис. 2.6). Національний домен об’єднує критичні об’єкти енергетики, транспорту та зв’язку. Його ядро становить державний центр керування, де розгорнуто сховища журналів подій, сертифікаційний орган і реєстр політик безпеки. Усі нижчі сегменти успадковують ці політики у вигляді підписаних шаблонів, тому правила аутентифікації, шифрування та зберігання телеметрії залишаються уніфікованими незалежно від рівня.

Регіональний домен охоплює групу виробничих майданчиків або міських кластерів. Тут функціонують диспетчерські алгоритми, що оптимізують баланс енергоспоживання, резерв технічного персоналу й мережеву топологію з урахуванням поточних погодних та логістичних умов. Логіку реалізовано через мікросервіси, розгорнуті у приватному хмарному середовищі OpenShift. Внутрішній сервісний шина обмінюється подіями асинхронно, отже відмова окремого мікросервісу не блокує роботу домену.

Приватний домен відповідає окремому виробничому підприємству чи складу. Тут працюють системи керування реального часу SCADA і MES, а також локальні брокери моделей машинного навчання. Диспетчер відстежує стан обладнання через цифрові двійники та за потреби запускає локальне перенавчання. Ресурсами керує Kubernetes Edge, який автоматично масштабує контейнери відповідно до навантаження та обмежень живлення.

Галузеві домени формуються консорціумами підприємств однієї вертикалі, наприклад фармацевтики або харчової промисловості. У них підтримують єдину таксономію даних та узгоджують еталони якості продукції.

Галузевий диспетчер аналізує агреговану статистику дефектів і розподіляє рекомендації щодо параметрів технологічних ліній.

Зв’язок між доменами здійснюється стандартизованими північними інтерфейсами. У транспортному шарі використовуються зашифровані тунелі IPSec з електронною ідентифікацією вузлів через X.509. На рівні прикладних сервісів діє REST-API з описом у форматі OpenAPI та графова модель даних, сумісна з OPC UA. Інтерфейс передає агреговані показники продуктивності, плани виробництва і запити на резервування ресурсів. Подібна уніфікація знижує накладні витрати, адже новий регіональний або приватний сегмент підключається до існуючої інфраструктури, імпортує актуальні політики і негайно включається до обміну.

Характеристика	Національний домен	Регіональний домен	Приватний домен	Секторний домен
Обсяг	Критичні об'єкти енергетики, транспорту, зв'язку	Група виробничих майданчиків або міських кластерів	Єдине виробниче підприємство або склад	Консорціуми підприємств однієї вертикалі
Основний елемент	Державний центр контролю	Алгоритми диспетчеризації	Системи реального часу SCADA та MES	Диспетчер промисловості
Функціональність	Сховища журналів подій, сертифікаційний орган, реєстр політик безпеки	Оптимізує баланс споживання енергії, резерв технічного персоналу, мережеву топологію	Моніторить стан обладнання через цифрові двійники	Аналізує агреговану статистику дефектів і розподіляє рекомендації
Технологія	Підписані шаблони	Мікросервіси, розгорнуті у приватному хмарному середовищі OpenShift	Kubernetes Edge	Уніфікована таксономія даних

Рисунок 2.6. Структурно-логічне розділення інфраструктури за типом та масштабом системи автоматизованого управління.

Децентралізація площини автоматизованої інфраструктури унеможливлює виникнення єдиної точки відмови. Якщо відбувається аварія в одному регіоні, керування не потребує переміщення до іншого центру, оскільки кожен домен оперує автономно. Водночас централізоване зберігання політик і глобальних журналів забезпечує цілісність управлінської моделі та спрощує аудит. Капітальні витрати на масштабування знижуються, бо розгортання

нового домену обмежується інсталяцією локального кластера контейнерів і набір політик не вимагає переробки.

2.1.4. Функціональна модель площини інтелектуальної обробки даних в інформаційно-комунікаційній системі

Площина інтелектуальної обробки даних розташована на верхньому рівні ієрархії та оперує не чистими потоками телеметрії, а винятково параметрами, отриманими після локального навчання моделей на крайових пристроях. Увесь функціональний ланцюг починається з приймання знеособлених вагових векторів брокером повідомлень, перевіркою їх цифрових підписів та сумісності версій. Підсистема валідації та нормалізації контролює розмір тензорів, виявляє аномальні значення, і за потреби накладає диференційно-приватний шум, щоб забезпечити дотримання регуляторних вимог конфіденційності.

Після успішної перевірки зважені моделі надходять до ядра федеративного агрегатора. На цьому етапі кожному клієнтові призначається коефіцієнт впливу, що враховує локальну похибку, обсяг даних та час затримки пакета. Узагальнений вектор параметрів формується стійким усередненням, доповненим адаптивним фільтром, який пригнічує залишкові статистичні викиди та запобігає деградації глобальної моделі.

Сформована модель фіксується у репозитарії версій із хеш-підписом і метаданими про показники точності на валідаційній вибірці. Застосована політика поетапного розгортання дає змогу спочатку поширити оновлення вузькому колу контрольних клієнтів і лише після позитивних показників оновлюється для всіх кінцевих пристроїв. Оркестратор оновлень постійно відстежує точність моделі, затримку передавання даних та енергетичні обмеження, коригуючи таким чином частоту відправлення пакетів або ініціюючи додаткові локальні навчання для сегментів, у яких зростає похибка.

Площина інтелектуальної обробки забезпечує замкнений цикл безперервного вдосконалення, при якому локальні пристрої навчають моделі на власних даних, надсилають анонімні ваги нейронної мережі, а агрегатор формує

та верифікує глобальну версію, після чого оновлені параметри повертаються у площину пристроїв. Це гарантує постійне підвищення точності прогнозів без ризику витоку конфіденційної інформації та надлишкового передавання даних (рис. 2.6).

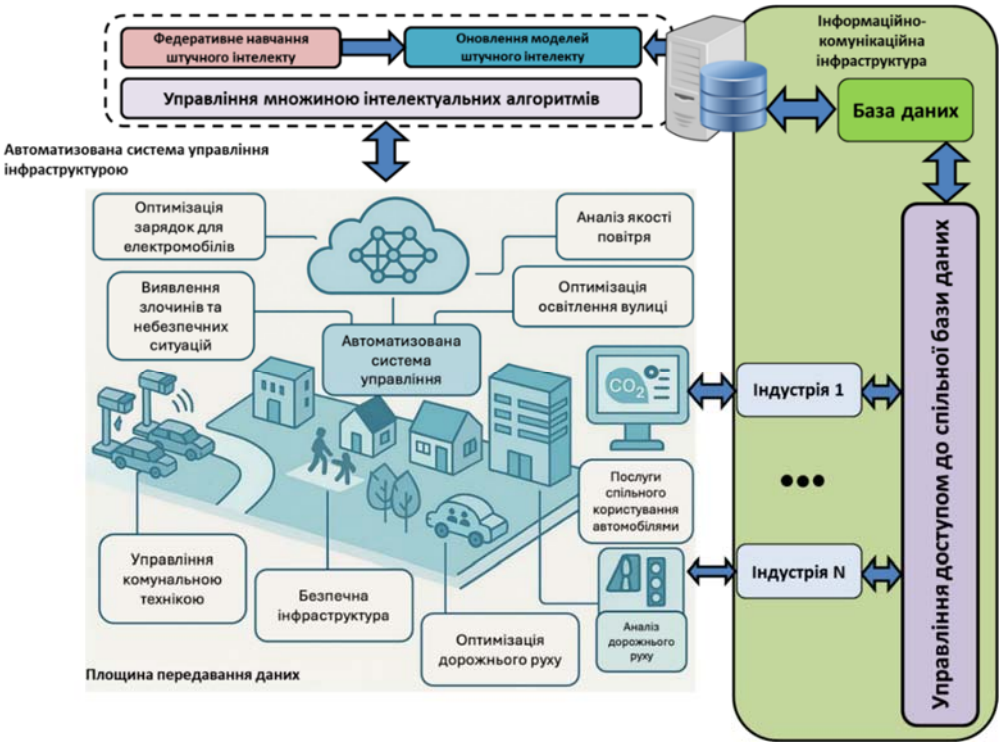


Рисунок 2.6. Структурно-функціональна модель взаємодії площини передавання даних та площини інтелектуальної обробки даних в контексті федеративного навчання.

2.2 Розроблення методу середньозваженого оцінювання впливу локальних моделей при оновленні агрегованої моделі федеративного навчання

2.2.1 Проблема агрегації моделей у федеративному навчанні

В основі технології федеративного навчання є процес агрегації результатів паралельного навчання на окремих вузлах у єдину глобальну модель. Аналіз передумов, які стимулюють дослідження нових алгоритмів агрегації, доцільно здійснювати крізь призму системних, статистичних та регуляторних факторів, що обумовлюють обмеження базової схеми FedAvg і потребу в її еволюції (рис. 2.7.)

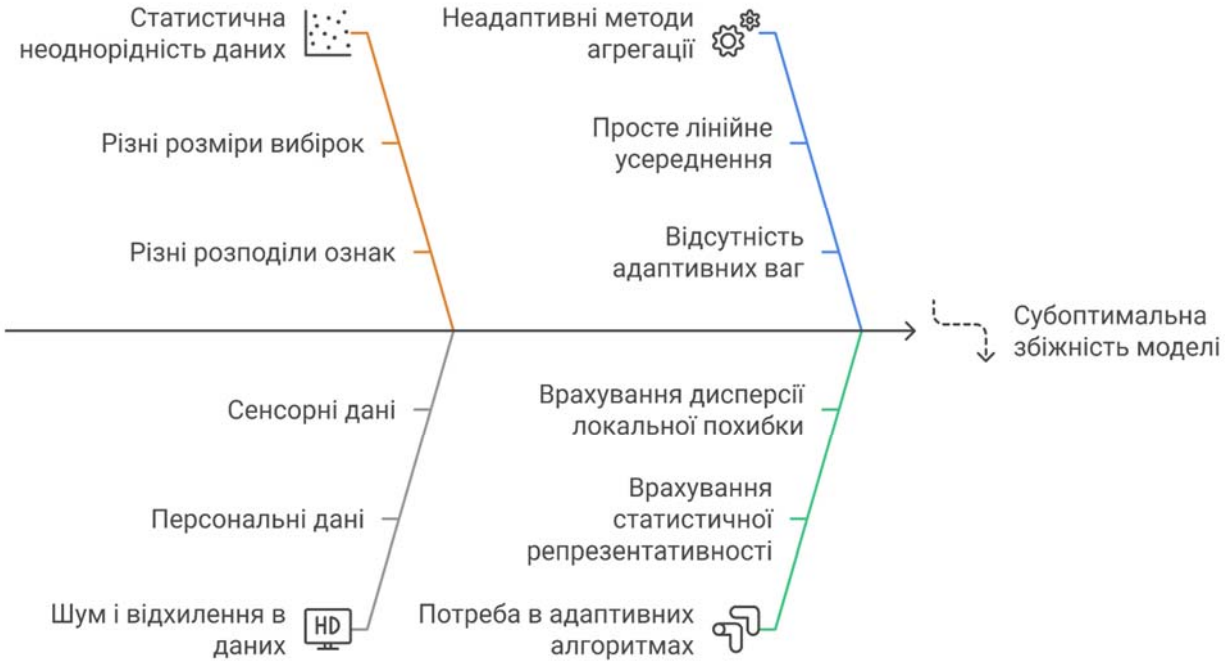


Рисунок 2.7. Класифікація обмежуючих факторів, які впливають на агрегацію моделей федеративного навчання.

Статистична неоднорідність даних є ключовим фактором для пошуку шляхів удосконалення методів агрегації, оскільки локальні вибірки відрізняються як за обсягом, так і за розподілами ознак. Окрім того, дані часто містять шуми та відхилення різного роду, що є характерним для персональних або сенсорних даних. У такому випадку просте лінійне усереднення параметрів, закладене в класичному алгоритмі FedAvg, призводить до субоптимальної збіжності або навіть до дивергенції глобальної моделі. Ця обставина зумовлює потребу в алгоритмах, які адаптивно обчислюють ваги клієнтських оновлень, враховуючи їхню статистичну репрезентативність, дисперсію локальної похибки та відстань до глобального мінімуму.

Другою важливою передумовою є системна гетерогенність клієнтів. Периферійні вузли відрізняються обчислювальною продуктивністю, ємністю батареї та пропускною здатністю каналу. У таких умовах одночасна синхронна агрегація підвищує затримку та створює «вузькі місця», коли найповільніший клієнт стримує прогрес усієї системи. Це визначає інтерес до асинхронних і частково синхронних схем, які використовують стохастичні або часові ваги,

щоб мінімізувати негативний вплив відставання та забезпечити стабільність збіжності.

Третій фактор випливає з комунікаційних обмежень. Для мереж мобільного зв’язку та IoT-систем характерні обмеження радіочастотного ресурсу, енергоспоживання та вартості передавання великих за обсягом тензорів з параметрами нейронних мереж. Унаслідок цього активно досліджуються методи скорочення обсягу трафіку: квантування градієнтів, субпросторове усереднення, стиснення та скетчування оновлень, а також багатоетапні ієрархічні схеми, у яких локальні підмережі виконують попередню агрегацію перед передаванням результатів до центрального сервера.

Четверта передумова має регуляторно-конфіденційний характер. Засилля нормативів, подібних до GDPR та HIPAA, посилює вимоги до захисту особистих даних і мотивує використання додаткових механізмів приватності, зокрема диференційного шуму та криптографічних протоколів безпечної агрегації. Введення таких протоколів змінює властивості градієнтів (наприклад, робить їх зашумленими або частково зашифрованими), що, у свою чергу, потребує спеціально налаштованих алгоритмів об’єднання, здатних підтримувати точність моделі під впливом інформаційної втрати.

П'яту групу передумов формують загрози безпеки, пов’язані з потенційно зловмисними або скомпрометованими клієнтами. Вживлення отруєних градієнтів, генерація прихованих функцій та різноманітні атаки підривають достовірність централізованого усереднення. У відповідь розвиваються стійкі до аномалій методи, що застосовують стійкі статистики для ідентифікації та нейтралізації зловмисних оновлень без різкого зменшення швидкості збіжності.

Окремо слід виокремити питання персоналізації та справедливості. У багатьох прикладних сценаріях мета полягає не стільки у отриманні єдиної максимальної загальної точності, скільки у забезпеченні прийнятної якості для всіх груп користувачів, включаючи міноритарні. Це стимулює створення багатоцільових або клієнт-орієнтованих підходів, де механізм об’єднання враховує ваги клієнтів пропорційно до їхній соціальної важливості.

Окрім того, розвиток нових мережних архітектур, поява хмарно-граничних обчислень, 6G-мереж із інтегрованою підтримкою інтелектуальних функцій та блокчейн-орієнтованих схем реєстрації оновлень створює нові топологічні ієрархії, де класичний центральний сервер поступається місцем децентралізованим архітектурам [72]. Для таких топологій необхідні алгоритми, які здатні ефективно поєднувати часткові результати на проміжних вузлах без втрати узгодженості та з гарантіями теоретичної оптимальності.

В сукупності, диверсифікована сукупність статистичних, системних, комунікаційних, регуляторних і безпекових факторів формує комплекс передумов, що роблять дослідження інноваційних алгоритмів агрегації у федеративному навчанні не лише актуальним, а й стратегічно важливим для розвитку повного спектра застосувань цієї технології від персональної медицини та смарт-міст до масових мереж інтелектуальних сенсорів та автономних транспортних систем.

2.2.2 Математичні моделі усереднення параметрів у федеративному навчанні

Одним із перших підходів до федеративної оптимізації став Федеративний стохастичний градієнтний спуск (FedSGD), представлений авторами у [73]. У FedSGD кожен клієнт k навчає локальну модель, обчислюючи градієнти за допомогою градієнтного спуску на міні-вибірках протягом однієї локальної епохи, після чого передає градієнти на центральний сервер. Сервер агрегує отримані градієнти та оновлює глобальну модель.

Математично параметри глобальної моделі w оновлюються за такою формулою:

$$\boldsymbol{w}_{t+1} = \boldsymbol{w}_t - \eta \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k\left(\boldsymbol{w}_t\right), \tag{2.1}$$

де: η - глобальна швидкість навчання, K - загальна кількість клієнтів, n - кількість вибіркових даних у клієнта k, $n = \sum_{K=1}^{K} n_k$ - загальна кількість

вибіркових даних серед усіх клієнтів, $\nabla F_k(\mathrm{w}_\mathrm{t})$ градієнт, обчислений клієнтом k на ітерації t.

Попри концептуальну простоту, FedSGD демонструє повільну збіжність через високі комунікаційні витрати на кожному етапі навчання, оскільки оновлення передаються після кожної міні-вибірки. Для вирішення цієї проблеми, з'явився метод Federated Averaging (FedAVG) як розширення FedSGD [74]. На відміну від FedSGD, FedAVG дозволяє клієнтам виконувати кілька локальних епох навчання перед передаванням оновлених параметрів моделі на сервер. Замість надсилання сирих градієнтів клієнти передають оновлені ваги моделі після локального навчання.

Оновлення моделі у FedAVG відбувається за виразом:

$$\boldsymbol{w}_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \boldsymbol{w}_t^k, \tag{2.2}$$

де w_t^k – це локально навчені вагові коефіцієнти моделі клієнта *k* на ітерації *t*.

Завдяки можливості виконувати кілька локальних оновлень перед передаванням даних FedAVG значно зменшує кількість раундів обміну (CR), необхідних для збіжності. Однак цей метод має труднощі з неоднорідними даними, що може спричиняти розбіжність локальних моделей.

Для подолання труднощів, які виникають через нерівномірно розподілені набори даних, був запропонований FedProx як варіація FedAVG [6]. FedProx вводить проксимальний термін у локальну цільову функцію, що обмежує локальні оновлення, запобігаючи надмірному відхиленню від глобальної моделі. Це допомагає стабілізувати навчання в умовах високої неоднорідності даних.

Локальна цільова функція для кожного клієнта k в FedProx визначається як:

$$F_k(\boldsymbol{w}) = f_k(\boldsymbol{w}) + \frac{\mu}{2}\left|\boldsymbol{w} - \boldsymbol{w}_t\right|^2, \tag{2.3}$$

де $f_k(w)$ це оригінальна локальна функція втрат, μ це налаштовуваний параметр регуляризації, який контролює ступінь відхилення від глобальної моделі, w_t представляє параметри глобальної моделі.

Вибір параметра проксимальної умови μ є критичним, оскільки надмірно великі значення можуть надмірно обмежити локальні оновлення, перешкоджаючи адаптації до змін в локальних даних.

2.2.3 Методи персоналізованого усереднення параметрів для окремих клієнтів у федеративному навчанні

Федеративне навчання часто стикається зі статистичною гетерогенністю, коли локальні розподіли даних значно відрізняються серед учасників. Для вирішення цієї проблеми було запропоновано кілька методів персоналізованого FL (pFL), які дозволяють моделям адаптуватися до індивідуальних характеристик клієнтів, одночасно користуючись перевагами колективного навчання.

Автори [76] представили FedPer, який розділяє локальну модель на дві компоненти, а саме базові шари θ^s, які спільні для всіх учасників і оновлюються глобально та персоналізовані шари $\theta_{\mathrm{i}}^{\mathrm{p}}$,які є специфічними для кожного клієнта і і не розподіляються. Математично, параметри моделі, специфічні для клієнта, визначаються як:

$$\theta_i = \left\{ \theta^s, \theta_i^{(p)} \right\}, \forall \ \mathrm{i} \in \{1, 2, \ldots, \mathrm{N}\}, \tag{2.4}$$

де N — це загальна кількість клієнтів.

Під час навчання лише базові шари θ^s адресуються на центральному сервері за допомогою FedAVG:

$$\theta^s \leftarrow \sum_{i=1}^{N} \frac{n_i}{n} \theta_i^s, \tag{2.5}$$

де n_i позначає кількість локальних зразків даних для клієнта i , $n = \sum_{i=1}^{N} n_i$ це загальний розмір датасету.

На відміну від цього, персоналізовані шари залишаються локальними та налаштовуються індивідуально на кожному клієнті. Такий підхід дозволяє спільно використовувати механізм витягання ознак, зберігаючи персоналізацію для адаптації до конкретних завдань. Пізніше автори [75] дослідили зворотну конфігурацію, у якій базові шари були специфічними для клієнта, а лише шари вищого рівня залишалися спільними.

Автори у [76] запропонували FedMeta - підхід до федеративного мета-навчання, натхненний модельно-агностичним метанавчанням (Model-Agnostic Meta-Learning -MAML) [77]. Мета FedMeta - знайти початкову модель θ, яка зможе швидко адаптуватися до нових клієнтів із мінімальними оновленнями.

Це досягається шляхом оптимізації мета-цільової функції:

$$\min_{\theta} \sum_{i=1}^{n} \mathrm{L}\left(\theta - \alpha \nabla_{\theta} \mathrm{L}\left(\theta\right)\right), \tag{2.6}$$

де $\mathcal{L}_i(\theta)$ - локальна функція втрат для клієнта i, а α - розмір кроку адаптації.

Кожен клієнт виконує один або кілька градієнтних кроків:

$$\theta_i^{'} = \theta - \alpha \nabla_{\theta} \mathrm{L}\left(\theta\right), \tag{2.7}$$

перш ніж відправити адаптовані параметри θ_i', які потім агрегуються для уточнення мета-моделі.

FedMeta забезпечує швидку адаптацію до нових клієнтів, що робить його особливо корисним у сценаріях із динамічним розподілом даних, таких як персоналізовані системи рекомендацій або застосування в охороні здоров’я.

2.2.4 Методи на основі шарів та співставлення

Методи на основі шарів та співставлення, були розроблені для підвищення ефективності збіжності та адаптивності моделі.

Автори у [78] запропонували Федеративне Узгоджене Усереднення (FedMA), яке має на меті покращити агрегацію моделей FL, виконуючи узгодження шарів, а не усереднення параметрів елемент за елементом. Основна

ідея FedMA полягає в тому, що шари нейронних мереж у різних клієнтів можуть бути несумісними через відмінності у навчених поданнях ознак. Для вирішення цієї проблеми FedMA виконує вирівнювання шарів шляхом узгодження нейронів з подібними активаційними патернами.

Математично, FedMA слідує структурованій агрегації шарів:

$$\theta^{(l)} = \text{Match}\left(\theta_1^{(l)}, \theta_2^{(l)}, \ldots, \theta_N^{(l)}\right), \tag{2.8}$$

де $\theta^{(l)}$ позначає параметри шару l у глобальній моделі, а Match(·) позначає функцію узгодження шарів, яка вирівнює нейрони на основі схожості їхніх активацій серед клієнтів. Процес узгодження шарів мінімізує розбіжності між нейронами за допомогою алгоритму узгодження, заснованого на теорії оптимального транспорту, яка дозволяє знайти відповідність між нейронами з найменшими витратами:

$$\min_{\pi} \sum_{i,j} C_{ij}\pi_{ij}, \quad \text{s.t.} \sum_{j} p_i^{\pi_{ij}}, \sum_{i} q_j^{\pi_{ij}}, \tag{2.9}$$

де π_{ij} це відповідність між нейронами i та j, C_{ij} це вартість узгодження нейронів, а p_i, q_j — розподіли активацій відповідних нейронів.

Автори [79] запропонували алгоритм Federated Distillation (FedDist) як альтернативну парадигму FL, особливо для таких застосувань, як розпізнавання людської діяльності (HAR). Замість прямого усереднення ваг моделей, FedDist використовує дистиляцію знань для передачі знань від локальних моделей до глобальної моделі.

Глобальна модель оновлюється за допомогою специфічних для клієнта розподілів м'яких міток:

$$\theta_g = \sum_{i=1}^{N} \frac{n_i}{n} \theta_i, \tag{2.10}$$

де θ_g це агрегована глобальна модель, θ_i позначає локальну модель клієнта i, ni це кількість тренувальних зразків у клієнта i, а $n = \sum_{i=1}^{N} n_i$ це загальна кількість зразків серед усіх N клієнтів.

Однак замість прямого усереднення, FedDist вводить узгодження на рівні нейронів, обчислюючи метрики схожості між локальними моделями:

$$D\left(\theta_i,\theta_j\right)=\sum_l\sum_k\left|f_i^{(l)}\left(x_k\right)-f_j^{(l)}\left(x_k\right)\right|, \quad (2.11)$$

де $f_i^{(l)}(x_k)$ позначає активацію нейрону на шарі l для вхідних даних x_k під моделлю клієнта i.

Вирівнюючи активації нейронів замість прямого злиття ваг, FedDist вирішує проблеми, пов'язані з non-IID даними, та зменшує катастрофічне втручання між розбіжними оновленнями моделей. Однак цей метод має високе комунікаційне навантаження через додаткову мета-інформацію, необхідну для узгодження нейронів.

Методи на основі шарів та співставлення в FL надають більш складні механізми агрегації, що підвищують продуктивність моделей у гетерогенних середовищах. FedMA зосереджується на вирівнюванні шарів моделей серед клієнтів для покращення сумісності ваг, тоді як FedDist використовує дистиляцію знань для уточнення агрегації моделей. Ці техніки зменшують проблеми статистичної гетерогенності, хоча їх реалістичність залежить від компромісів між комунікаційними витратами та складністю агрегації.

2.2.5 Метод середньозваженого оцінювання впливу локальних моделей при оновленні агрегованої моделі федеративного навчання

Реалізація удосконаленої моделі федеративного навчання із додатковим критерієм зважування виконується послідовно в декілька логічно взаємопов’язаних кроків, кожен з яких має чітко визначену мету та набір внутрішніх процедур.

Крок 1. На початковому етапі формується множина учасників-клієнтів, периферійних обчислювальних вузлів, що володіють приватними вибірками даних. Для кожного учасника визначаються дві незалежні підмножини, базова вибірка, яка використовується для локального градієнтного навчання та тестова, призначена виключно для оцінювання достовірності локальної моделі. Подібне розділення забезпечує можливість обчислити локальну валідаційну

похибку, не зловживаючи глобальним тестовим набором і не порушуючи конфіденційності даних.

Крок 2. Кожен клієнт ініціалізує копію глобальної моделі та виконує кілька епох стохастичної оптимізації, використовуючи вибраний алгоритм (наприклад, Adam або SGD). Після завершення локального навчання вузол обчислює вектор параметрів θ_i, середнє значення локальної функції втрат на контрольній вибірці L_i, а також дисперсію миттєвих втрат σ^2_i, що характеризує стабільність навчання.

Крок 3. Клієнти відправляють на сервер лише вектори θ_i та пару статистичних показників (L_i, σ^2_i). Відсутність необроблених (сирих) даних гарантує конфіденційність, що є ключовою перевагою парадигми федеративного навчання у мобільних пристроях із вбудованими NPU-модулями.

Крок 4. Обчислення вагового коефіцієнта впливу кожної локальної моделі, з метою визначення моделей, які були натреновані краще та, відповідно, повинні мати більшу вагу під час оновлення глобальної моделі (рисунок 2.8). За допомогою метрик прогностичної точності моделі визначається вплив конкретної локальної моделі при формуванні глобальної моделі відповідно до виразу:

$$LM_{\underset{i}{\inf}} = \frac{1-\left(X_{lm_i} / X_{sum}\right)}{N-1}, \tag{2.12}$$

де X_{lmi} це метрика прогностичної точності моделі, X_{sum} це сума значень X_{lmi} від усіх клієнтів, а N це кількість AGV.

Для оцінки прогностичної точності моделей використовуються метрики функції втрат. Для регресійних задач використовується MSE та валідаційні втрати з метою порівняння отриманих результатів і визначення, яке з цих значень є більш доцільним для усереднення локальних моделей. Окрім цього, застосовується метрика середньої абсолютної відносної похибки, яка визначає точність методу прогнозування:

$$MAPE = \frac{1}{n}\sum_{i=1}^{n}\left|\frac{\left(y_i - \hat{y}_i\right)}{y_i}\right|. \quad (2.13)$$

де y це фактичне (спостережуване) значення, ŷ це відповідне прогнозоване значення, а n це кількість спостережень.

MAPE використовується як додаткова метрика для оцінювання відносної точності прогнозу, забезпечуючи інтерпретовані результати у відсотковому вираженні. Натомість MSE оцінює точність прогнозу, акцентуючи увагу на більших похибках шляхом піднесення відхилень до квадрату.

$$MSE = \frac{\sum_{i}^{n}\left(y_i - \hat{y}_i\right)^2}{n}, \quad (2.14)$$

де *y* це фактичне (спостережуване) значення, *ŷ* це відповідне прогнозоване значення, а *n* це кількість спостережень.

Валідаційні втрати використовується для оцінювання якості роботи моделі глибинного навчання на валідаційному наборі даних. Валідаційний набір є частиною загального датасету, що призначений для перевірки узагальнюючої здатності моделі.

$$Val_{loss} = \frac{1}{n}\sum_{i}^{n} f\left(\hat{y}_i, y_i\right), \quad (2.15)$$

де *f* це функція втрат.

Функція обчислення валідаційних втрат, як правило, аналогічна до тієї, що використовується під час навчання, і базується на сумі похибок (різниці між y та ŷ) для кожного спостереження у валідаційному наборі.

Крок 5. Оновлення вагових коефіцієнтів глобальної моделі, використовуючи вираз:

$$M = \sum_{i}^{N} m_i * LM_{\inf_i}, \quad (2.16)$$

де m_i це локальна модель на AGV_i, а символ $*$ позначає поелементне множення. Після нормування одержуємо систему ваг, що автоматично зменшує вплив

учасників із високими похибками або нестабільними градієнтами, тобто статистичними викидами.

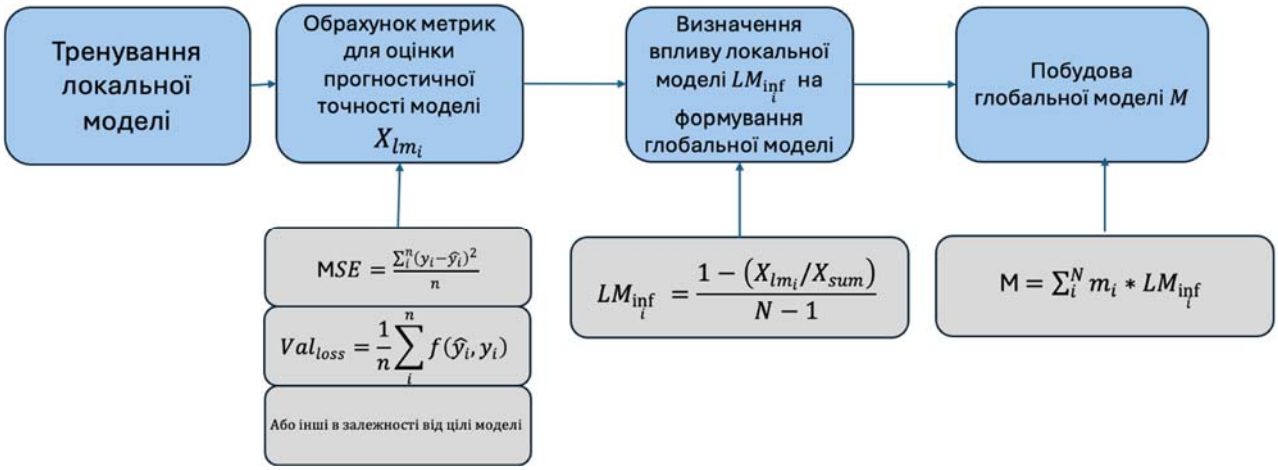


Рисунок 2.8. Блок-схема кроків 4 та 5 розробленого процесу оновлення моделі з введенням додаткового критерію зважування впливу локальних моделей на формування глобальної моделі.

Крок 6. Шостим кроком є перевірка оновленої глобальної моделі на незалежній серверній вибірці. Якщо приріст точності є статистично значущим, нові параметри розповсюджуються серед усіх клієнтів; інакше сервер може застосувати механізм повторної ітерації.

Крок 7. Клієнти одержують оновлену глобальну модель, після чого розпочинається новий цикл локального навчання. Така рекурентна процедура забезпечує монотонне зменшення середньої глобальної втрати аж до встановлення стаціонарної точки.

Крок 8. Завершальним кроком є аналітичний моніторинг. Сервер накопичує історію та застосовує методи часових рядів для раннього виявлення клієнтів-аномалій. Якщо коефіцієнт впливу учасника систематично прямує до нуля, йому видається рекомендація підвищити якість даних або пропускну здатність локального оптимізатора, що зменшує ресурсні витрати всієї федеративної екосистеми.

Введення додаткового критерію зважування впливу локальних моделей інтегрується у класичний цикл Federated Averaging без порушення

конфіденційності, забезпечуючи підвищення точності агрегованої моделі за рахунок автоматизованої фільтрації статистичних викидів і стабілізації процесу глобальної оптимізації.

В таблиці 2.1 представлено огляд основних алгоритмів агрегації у федеративному навчанні, підкреслюючи їх ключові ідеї, основні переваги, недоліки та відповідні посилання.

Таблиця 2.1. Огляд та порівняння методів агрегації глобальних моделей у федеративному навчанні

Алгоритм	**Основний принцип**	**Переваги**	**Недоліки**	**Посилання**
FedSGD	Мінімальна кількість епох; локальні градієнти надсилаються кожного раунду	1. Простий, легкий у реалізації 2.Встановлює базовий рівень для FL	1. Повільна збіжність (потрібно багато раундів) 2. Чутливий до неоднорідності даних (non-IID)	[80]
FedAvg	Виконання кількох локальних епох перед усередненням ваг на сервері	1. Менше комунікаційних витрат, ніж у FedSGD 2. Загалом хороша продуктивність	1. Погіршується при сильно неоднорідних даних 2. Не забезпечує повної персоналізації	[81]
FedProx	FedAvg + проксимальний член у локальній цільовій функції для зменшення розбіжності	1. Стійкіший до неоднорідності даних 2. Пом’якшує вплив гетерогенності пристроїв/даних	1. Додає локальні обчислювальні витрати (регуляризація) 2. Не забезпечує повної персоналізації	[82]
FedPer	Базові шари спільні; фінальні шари	1. Покращує точність у неоднорідних	1. Розділення моделі збільшує складність 2.	[83]

	персоналізовані для кожного клієнта	умовах 2. Часткова персоналізація	Додаткові витрати на керування шарами	
FedMA	Відповідність шарів (фільтрів, нейронів) між клієнтами	1. Зменшує комунікаційні витрати 2. Ефективний для задач CNN/LSTM	1. Складний, якщо архітектури різні 2. Не підходить для всіх типів моделей	[78]
Запропонований алгоритм	Зважене усереднення на основі продуктивності локальних моделей	1. Вищий вплив більш якісних локальних моделей 2. Підходить для неоднорідних даних	Потребує обрахунок додаткових метрик з метою оцінки точності прогнозування локальних моделей	Розділ 2.2.5

2.3 Розроблення методу багатораундного федеративного навчання для систем автоматизованого управління

2.3.1 Методи покращення адаптивності моделей федеративного навчання в динамічних умовах

Для покращення адаптивності та збіжності FL були досліджені методи на основі кластеризації та еволюційної оптимізації, зокрема генетичні алгоритми (GAs). Ці підходи покращують процес агрегації, динамічно групуючи схожих клієнтів або оптимізуючи параметри моделі для кращої персоналізації.

У роботі [84] запропоновано ієрархічне кластеризоване федеративне навчання (Hierarchical Clustering Federated Learning), де клієнти групуються в кластери на основі схожості їхніх даних. Замість безрозбірного агрегування оновлень від усіх клієнтів, сервер спочатку виконує кластеризацію, а потім застосовує агрегування моделей всередині кожного кластера.

Математично, HCFL призначає кожного клієнта i до кластера C_k на основі міри схожості:

$$d(i,j) = \left\| \theta_i - \theta_j \right\|_2, \tag{2.17}$$

де θ_i і θ_j це параметри локальних моделей клієнтів i та j, а d(i,j) позначає евклідову відстань між ними. Клієнти з мінімальною відстанню групуються в один кластер. Після формування кластерів сервер оновлює глобальну модель для кожного кластера, використовуючи функцію агрегування всередині кластера:

$$\theta_k = \sum_{i \in C_k} n_i N_k \theta_i, \tag{2.18}$$

де n_i розмір локального набору даних клієнта i, а N_k — загальна кількість клієнтів у кластері C_k

Зменшуючи розбіжність між моделями, HCFL прискорює збіжність у гетерогенних середовищах. Однак цей метод передбачає, що клієнти в межах одного кластера мають однорідні розподіли даних, що може не завжди відповідати реальності, обмежуючи його ширше застосування.

Окрім того, гетерогенність даних серед учасників FL створює серйозні виклики, часто призводячи до значної варіативності продуктивності моделей та нестабільності під час навчання. Для подолання цих проблем дослідники розробили вдосконалені статистичні методи та техніки узгодження ознак, спрямовані на ефективніше вирівнювання локальних клієнтських моделей. Такі підходи допомагають гармонізувати знання між різнорідними наборами даних, забезпечуючи надійну агрегацію моделей і покращуючи загальну стабільність навчання.

Зокрема в [85] запропоновано метод Federated Transfer Learning with Recursive Least Squares (FTL-RLS), орієнтований на розв’язання регресійних задач у неоднорідних розподілах даних. Ця техніка використовує метод Recursive Least Squares (RLS) як стратегію оптимізації, що значно зменшує комунікаційні витрати та забезпечує швидку збіжність.

Правило оновлення RLS визначається як:

$$\theta_{t+1} = \theta_t + P_t X_t^T \left(Y_t - X_t \theta_t \right), \tag{2.19}$$

де θ_t позначає параметри моделі, Pt позначає обернену коваріаційну матрицю, а X_t, Y_t це матриця ознак і цільові мітки на часовому кроці t. Хоча FTL-RLS забезпечує високу швидкість виконання та мінімізує обсяг переданих повідомлень, його основним обмеженням є застосовність лише до регресійних задач.

Автори в [86] запропонували метод Federated Feature Matching (FedFM) для зменшення гетерогенності даних у сценаріях федеративного навчання. Замість прямого усереднення параметрів моделі, FedFM вирівнює подання ознак між клієнтами, використовуючи узгодження на основі якірних точок. Оптимізаційна цільова функція для FedFM задається як:

$$\mathrm{LFdM} = \sum_{i=1}^{n} D_{\mathrm{KL}} \left(f_{\theta_i} \left(X_i \right) | f_{\theta_g} \left(X_i \right) \right), \tag{2.20}$$

де DKL позначає дивергенцію Кульбака-Лейблера між локальними енкодерами ознак f_{θ_i} та глобальним представленням ознак fθg. Зосереджуючись на узгодженні ознак замість усереднення параметрів, FedFM підвищує продуктивність моделі, водночас зменшуючи час комунікації.

Автори [87] запропонували метод FedSim, який використовує Principal Component Analysis (PCA) метод факторного аналізу в статистиці та кластеризацію методом к–середніх для зменшення розбіжностей у non-IID наборах даних. Замість однакового врахування всіх локальних моделей, FedSim групує клієнтів за подібністю ознак, формуючи кластери перед агрегуванням. Процес кластеризації формулюється як:

$$arg\,min_{\mathrm{S}} \sum_{j=1}^{k} \sum_{i \in S_j} \in \mathrm{S}_j \mid X_i - \mu_j \mid^2, \tag{2.21}$$

де S_j позначає кластер, μ_j – його центр, а X_i – це точки даних, призначені до цього кластера.

Хоча FedSim покращує персоналізацію та стабільність моделі, додаткові кроки кластеризації вводять обчислювальну складність.

Розглянуті вище статистичний підхід та метод узгодження ознак пропонують нові способи покращення FL шляхом покращення узгодження ознак, обробки регресійних задач та впровадження механізмів кластеризації. Проте, вони не враховують обчислювальну ефективність та комунікаційні витрати в реальних динамічних системах автоматизованого управління та прийняття рішень.

2.3.2 Методи дистиляції знань при гетерогенній архітектурі моделей федеративного навчання

Федеративне навчання традиційно передбачає, що всі учасники мають подібну архітектуру моделей. Однак у реальних сценаріях клієнти часто мають гетерогенні моделі через різні апаратні можливості, програмні фреймворки та вимоги до додатків. Ця архітектурна різноманітність створює труднощі для стандартних методів агрегації ваг, таких як FedAvg.

Для вирішення цієї проблеми були запропоновані підходи, засновані на дистиляції знань, що дозволяють співпрацювати між різними моделями шляхом обміну дистильованими знаннями, а не сирими параметрами моделей. Ці методи забезпечують ефективне навчання між гетерогенними архітектурами, зберігаючи при цьому конфіденційність та ефективність комунікації.

Автори у [88] запропонували підхід Federated Model Distillation (FedMD), який використовує дистиляцію знань та трансферне навчання для адаптації до гетерогенних архітектур моделей. На відміну від традиційних підходів до федеративного навчання, які агрегують ваги моделей, FedMD дозволяє клієнтам тренувати моделі з різними архітектурами, при цьому обмінюючись лише знаннями у вигляді м'яких міток. Ця техніка дає змогу клієнтам з різними обмеженнями обчислювальних ресурсів ефективно брати участь.

Математично, дистиляція знань формулюється як:

$$\mathrm{L_K} = \sum_{i=1}^{N} D_{\mathrm{KL}}\left(f_{\theta_i}(X) | f_{\theta_g}(X)\right), \tag{2.22}$$

де DKL позначає дивергенцію Кульбака-Лейблера між виходом локальної моделі $f_{\theta_i}(X)$ та глобальною опорною моделлю $f_{\theta g}(X)$. Ця дивергенція мінімізує різницю у навчених представленнях між різними архітектурами моделей. Попри свою гнучкість, FedMD не завжди демонструє кращу продуктивність порівняно з методами прямої агрегації моделей, такими як FedAvg чи FedProx, особливо у випадках, коли гетерогенність даних є надзвичайно високою.

Автори в [89] запропонували Model Heterogeneous Aggregation Training (MHAT) підхід, розроблений для сценаріїв федеративного навчання, де клієнти працюють з суттєво різними архітектурами моделей. Замість вирівнювання параметрів моделей, MHAT фокусується на вирівнюванні їхніх виходів, забезпечуючи узгодженість між різними архітектурами. Головна перевага MHAT полягає у зменшенні комунікаційних витрат, оскільки передаються лише ймовірності виходу моделі, а не повні ваги. Процес агрегації виконується за допомогою наступної формули:

$$L_{MHAT} = \sum_{i=1}^{N} | f_{\theta_i}(X) - f_{\theta_g}(X) |^2, \tag{2.23}$$

де функція втрат зменшує відхилення між виходом кожної локальної моделі та глобальним узгодженим результатом. Ця техніка дозволяє клієнтам із різними архітектурами нейронних мереж (наприклад, CNNs, Transformers або RNNs) брати участь у федеративному навчанні без необхідності уніфікації моделей.

Однак залишається проблема вибору відповідного відкритого набору даних для дистиляції знань, оскільки продуктивність MHAT залежить від репрезентативності спільних даних. Зазначені методи пропонують ефективні рішення для роботи з гетерогенністю моделей у федеративному навчанні, що дозволяє реалізовувати його в багатопристроєвих середовищах, де клієнти мають різні апаратні та програмні можливості.

У реальних сценаріях FL клієнти можуть мати різні обчислювальні ресурси, рівень мережевого з’єднання та доступність, що може спричиняти затримки. Асинхронне федеративне навчання (AsyncFL) вирішує цю проблему,

дозволяючи оновлювати глобальну модель без очікування всіх клієнтів, що підвищує ефективність навчання. Хоча підхід AsyncFL зменшує затримки та покращує масштабованість, він також створює нові виклики, такі як застарілі градієнти та складність агрегації оновлень.

Автори у [90] запропонували використовувати FedAsync - асинхронний метод FL, який дозволяє клієнтам надсилати оновлення на сервер незалежно, без необхідності синхронізації у фіксованих раундах навчання. Сервер агрегує отримані оновлення в режимі реального часу за допомогою правила зваженого оновлення:

$$\theta_{t+1} = (1 - \alpha_t)\theta_t + \alpha_t \theta_i, \tag{2.24}$$

де θ_{t+1} — оновлена глобальна модель, θ_i — локальне оновлення від клієнта i, а αt — адаптивна вага, що зменшує вплив застарілих оновлень.

Усуваючи необхідність глобальної синхронізації, FedAsync суттєво прискорює навчання, особливо в середовищах із повільними або періодично доступними клієнтами. Проте застарілі оновлення від затриманих клієнтів можуть погіршувати збіжність моделі, що потребує ретельного налаштування вагової функції для збереження стабільності навчання. Асинхронні методи продовжують відігравати ключову роль у забезпеченні масштабованих та ефективних моделей FL, особливо у IoT та індустріальних-середовищах, де гетерогенність пристроїв та переривчаста доступність створюють значні виклики.

2.3.3 Алгоритми ресурсно-орієнтованих граничних обчислень

Ресурсо-орієнтовані обчислення має на меті оптимізувати продуктивність системи шляхом зменшення енергоспоживання, мінімізації комунікаційних витрат та стимулювання участі пристроїв. Туманні обчислення (Fog-computing) розміщують хмарні сервіси ближче до кінцевих пристроїв користувачів, що забезпечує зниження затримок і зменшення використання смуги пропускання. Використовуючи архітектури туманних та граничних обчислень, системи

федеративного навчання можуть ефективно обробляти та агрегувати локальні оновлення, одночасно оптимізуючи енергоспоживання.

Автори у [91] запропонували енергоефективну архітектуру FL, яка динамічно регулює частоту процесора та потужність передавання для мінімізації використання ресурсів. Задача оптимізації була сформульована наступним чином:

$$\min_{\omega,P} \sum_{i=1}^{N} E_i(\omega, P), \tag{2.25}$$

де $E_i(\omega, P)$, представляє енергоспоживання пристрою і як функція параметрів моделі ω та потужності передавання P. Використовуючи динамічне масштабування напруги та частоти (DVFS), їхній підхід дозволив знизити енергоспоживання під час обчислень, при цьому зберігаючи ефективність збіжності FL.

Автори у [92] запропонували використовувати фреймворку ELFISH - архітектуру FL з обліком ресурсів, призначену для пришвидшення збіжності на кордонних пристроях. ELFISH використовує механізм обрізки, що враховує градієнт, зменшуючи надмірні обчислення та оптимізуючи вибір пристроїв, що беруть участь у кожному раунді навчання. Цей підхід зменшує вплив затримок, дозволяючи FL адаптивна вибирати високопродуктивні пристрої для локального навчання.

У [93] представлено Fog-enabled Federated Learning (FogFL), який інтегрує ієрархічну агрегацію в туманних мережах. Замість того, щоб централізувати оновлення на хмарному сервері, проміжні агрегації відбуваються на вузлах туманної мережі, що зменшує затримку зв'язку та усуває вузькі місця в обчисленнях. Крок локального оновлення задається наступним чином:

$$\theta_{t+1}^{\text{fog}} = \sum_{i=1}^{K} w_i \theta_{t,i}, \tag{2.26}$$

де $\theta_{t+1}^{\text{fog}}$ — це агрегована модель на рівні туманної мережі, θ_{ti} представляє локальні оновлення від пристрою і, а wi це присвоєна вага на основі внеску

пристрою. Така ієрархічна модель суттєво знижує витрати на пропускну здатність, зберігаючи точність моделі.

Зважаючи на гетерогенність учасників у FL, забезпечення рівноцінної участі пристроїв є важливим для запобігання паразитній поведінці та покращення надійності моделі. Для вирішення цієї проблеми було запропоновано кілька механізмів стимулювання. Автори у [94] використовували ігрову теорію Стакельберга для моделювання взаємодії між центральним сервером (лідером) та учасниками (послідовниками). Функція корисності для кожного клієнта була визначена як:

$$U_i\left(P_i, Q_i\right) = R_i\left(Q_i\right) - C_i\left(P_i\right), \tag{2.27}$$

де $R_i\left(Q_i\right)$ представляє функцію винагороди, яка залежить від внеску клієнта Q_i, а $C_i P_i$, це обчислювальні витрати на участь. Стратегія рівноваги заохочує раціональних клієнтів активно брати участь, одночасно зберігаючи баланс між точністю та витратами ресурсів.

Автори у [95] запропонували метод інтеграції федеративного навчання через блокчейн, який включає використання смарт-контрактів для забезпечення прозорих та захищених винагород для пристроїв, що беруть участь. Метод фіксував бали внеску за допомогою наступної формули:

$$S_i = \frac{\left\|\theta_g - \theta_i\right\|}{\left\|\theta_g\right\|}, \tag{2.28}$$

де S_i позначає бал внеску клієнта і на основі різниці між глобальною моделлю θ_g та локальною моделлю θ_i. Вищі бали внеску призводили до більших винагород, що ефективно заохочувало якісніші оновлення.

Автори у [96] запропонували використовувати FL для систем виявлення вторгнень у транспортних засобах (FL-VIDS), використовуючи механізм доказу авторства (PoA) для зменшення навантаження на зв’язок. На відміну від традиційного FL, де всі клієнти беруть участь у кожному раунді, PoA вибирає

підмножину вузлів з високим рівнем довіри, що оптимізує безпеку та зменшує затримки в навчанні.

Ресурсо-орієнтовані методи федеративного навчання відіграють ключову роль у його застосуванні в реальних умовах, особливо в середовищах із обмеженими енергетичними ресурсами та високими вимогами до затримок. Інтеграція туманних обчислень підвищує ефективність навчання завдяки ієрархічній агрегації моделей, а механізми стимулювання забезпечують справедливу участь і стійку співпрацю в децентралізованих мережах. На рис. 2.9 представлено порівняльний аналіз цих підходів.

Існуючі методи агрегації у федеративному навчанні (FL) пропонують різні підходи до вирішення таких викликів, як неоднорідність даних (non-IID), обмеження комунікації та персоналізація. Класичні алгоритми, такі як FedSGD і FedAvg, забезпечують просте навчання моделей, забезпечуючи безпеку даних проте без значних покращень точності моделей. Більш просунуті методи, такі як FedProx, підвищують стабільність моделей у умовах non-IID, але водночас створюють додаткове обчислювальне навантаження. Алгоритми FedPer і FedMA сприяють персоналізації та зменшенню комунікаційних витрат, однак вимагають модифікації структури моделі, що не завжди є практичним.

Окрім того, виявлення аномалій передбачає ідентифікацію спостережень, які не відповідають очікуваному шаблону в наборі даних. Це стало ключовою проблемою у дослідженні інтелектуальних пристроїв, зокрема AGV, у контексті розумного виробництва. Аномальні дані можуть вказувати на значущі та критичні події, що потребують негайної реакції. Виявлення аномалій є важливим напрямом аналізу даних і широко досліджується. У середовищі інтелектуального виробництва аномалія трактується як неочікувана зміна стану або поведінки системи IIoT, що відхиляється від норми. Раптовий вихід обладнання з ладу спричиняє небажане зниження якості продукції та загальної продуктивності. Виявлення аномалій допомагає зменшити ризики та наслідки таких ситуацій.

Рисунок 2.9. Порівняння ресурсно-орієнтованих методів федеративного навчання

Однак обмежена доступність історичних даних, а також вимоги до захисту промислової інформації ускладнюють процес виявлення аномалій у середовищі інтелектуального виробництва. Часто важко отримати дані, попередньо марковані як аномальні, і це також стосується інформації, зібраної з AGV. Тому критично важливим є застосування методів без учителя для класифікації даних як аномальних. Виявлення аномалій в AGV можна розглядати як задачу класифікації одного класу, де єдиним класом є нормальні (неаномальні) дані.

Типовий підхід до виявлення аномалій полягає в аналізі похибки між фактичними та прогнозованими значеннями досліджуваної ознаки. Модель прогнозування навчається на даних, що описують нормальну поведінку, і далі застосовується до майбутніх часових рядів для генерації очікуваної послідовності. Порівняння прогнозованих значень із фактичними дозволяє

оцінити ступінь аномальності. Таким чином, ефективність виявлення аномалій значною мірою залежить від якості застосованого методу прогнозування [86].

Для подолання вищезгаданих обмежень по енергоефективності та з метою покращення точності прогностичних можливостей моделей у даній роботі розроблено метод багатораундового федеративного навчання на основі хронологічної стратифікації навчальної вибірки.

2.3.4. Метод багатораундового федеративного навчання для індустріальних середовищ з високою динамікою

В цій роботі ми пропонуємо використовувати метод багатораундного федеративного навчання, який розглядається як механізм безперервної самоадаптації периферійних пристроїв в середовищі інтелектуальної інформаційно-комунікаційної системи .

Запропонований метод багатораундного федеративного навчання розглядається як невід'ємний елемент механізму безперервної самоадаптації периферійних пристроїв у складі інтелектуальної інформаційно-комунікаційної системи. На концептуальному рівні кожний цикл функціонування методу охоплює чотири взаємопов'язані етапи, які формують замкнений контур обміну знаннями між вузлами-агентами та централізованим хмарним оркестратором, забезпечуючи поступове удосконалення як локальних, так і глобальної моделей упродовж усього життєвого циклу системи.

Перший етап передбачає виконання локального тренування моделей безпосередньо на периферійних пристроях. У межах цього етапу агент оптимізує параметри власної нейронної мережі за допомогою стохастичного градієнтного спуску, використовуючи тільки внутрішні дані, що гарантує конфіденційність користувача. Важливою особливістю є застосування адаптивного плану навчання, який коригує швидкість оновлення ваг залежно від обчислювальних ресурсів пристрою, статистичної репрезентативності локальної вибірки та поточного рівня збіжності, що мінімізує ризик локальної дивергенції у разі неідеальних початкових умов.

Другий етап полягає у безпечному передаванні параметрів – ваг або їхніх градієнтів – до хмарного оркестратора. Для зменшення комунікаційного навантаження параметри попередньо квантуються та стискаються за допомогою алгоритмів скетчування, після чого до них додається диференційний шум, що забезпечує ε-діференційне збереження приватності. Передача здійснюється у зашифрованому вигляді, при цьому протокол асинхронної доставки дозволяє уникнути блокування системи на найповільніших («straggler») вузлах, зберігаючи цілісність інформаційного потоку.

На ***третьому етапі*** оркестратор формує актуальну глобальну модель шляхом зваженого усереднення отриманих оновлень. Вагові коефіцієнти обчислюються динамічно на підставі обсягу локальної вибірки, гісторії похибок, швидкості збіжності та довірчого індексу агента, що виробляється механізмом байєсівського оцінювання його минулої надійності. Для захисту від можливих «Byzantine»-атак оркестратор додатково застосовує робастні статистики (медіанне фільтрування та Trimmed-Mean), відсікаючи аномальні оновлення, здатні ввести модель у зону критичної нестабільності. У такий спосіб глобальна модель не лише агрегує розподілені знання, а й забезпечує стійкість до навмисних чи випадкових спотворень.

Четвертий етап охоплює зворотну синхронізацію, під час якої оркестратор ретранслює оновлені параметри до периферійних пристроїв. Щоб уникнути різких стрибків у значеннях ваг, пристрої застосовують техніку поступового змішування – екстраполюють глобальні параметри з урахуванням власної історії градієнтів. Така «тепла» ініціалізація зменшує часові витрати на повторну збіжність та дозволяє зберегти специфіку локальних моделей, критичну для задач персоналізованої інференції.

Ключова перевага запропонованого багатораундного методу полягає у його циклічності. Після завершення описаних етапів система автоматично переходить до нового раунду, ініціюючи повторний процес локального навчання на основі свіжих даних експлуатації. Це надає системі здатності до

безперервного самонавчання, що дає змогу оперативно реагувати на коливання трафіку або зміни експлуатаційних вимог. На відміну від класичної одноразової схеми FedAvg, де адаптація завершується після одиничної агрегації, запропонований підхід підтримує інкрементальне нарощування знань, уможливлюючи поступове вдосконалення точності та стійкості моделі без повного перезапуску системи.

Додатково циклічність сприяє формуванню історичної бази оновлень, що використовується для побудови предиктивної аналітики. Зокрема, оркестратор може прогнозувати темпи збіжності окремих агентів, оптимізувати графік їхньої участі у майбутніх раундах та проактивно корегувати величину комунікаційних квот. У підсумку система отримує механізм самоадаптивного балансування між обчислювальними, енергетичними та мережними ресурсами, що суттєво підвищує ефективність у порівнянні з традиційними централізованими або статичними підходами. Запропонований метод формує органічно інтегровану процедуру багатораундного федеративного навчання, яка сполучає локальну конфіденційність та безперервну самоадаптацію системи, що у комплексі забезпечує стійке підвищення якості глобальної моделі за мінімально можливих витрат на зв’язок та обчислення. Блок-схема реалізації даного методу представлена на рис. 2.10.

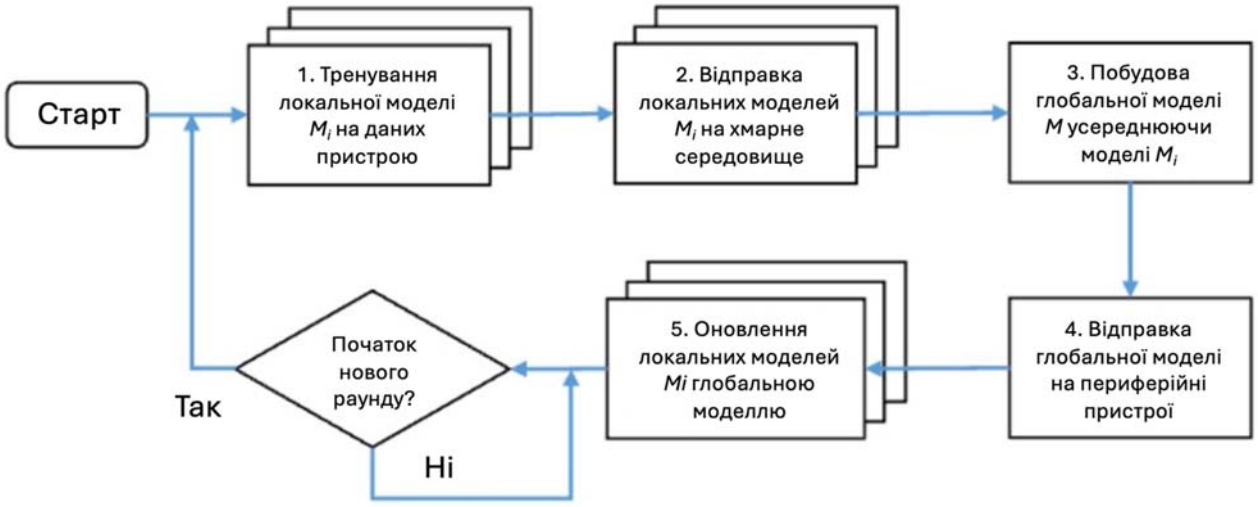


Рисунок 2.10. Блок-схема роботи одного раунду розробленого алгоритму.

Синергетичний приріст ефективності запропонованого багатораундного методу федеративного навчання забезпечується його інтеграцією з методом середньозваженого оновлення параметрів, детально обґрунтованим у підрозділі 2.2. Останній модифікує вагові коефіцієнти клієнтських оновлень пропорційно поточній прогностичній точності кожного пристрою, що дає змогу нейтралізувати вплив неінформативних або часово деградованих вибірок без жорстких порогових обмежень і водночас зберігати релевантні локальні особливості моделей. Окрім того, для підвищення відмовостійкості системи реалізовано механізм компенсації інформаційних втрат у разі непередбаченого від’єднання вузла-агент. В такому випадку, оркестратор зберігає останню перевірену конфігурацію глобальної моделі та автоматично ініціює повторно під’єднані пристрої в наступний навчальний раунд. Сукупність зазначених технічних рішень забезпечує поступове нарощування точності глобальної моделі без переривання виробничого циклу, зменшує енергоспоживання периферійних вузлів і істотно підвищує відмовостійкість системи керування, утворюючи науково обґрунтовану основу для довготривалого самонавчання інтелектуальних інформаційно-комунікаційних систем у промислових застосуваннях.

2.4 Висновки до розділу

У розділі сформовано цілісну методологічну основу інтеграції федеративного навчання в інформаційно-комунікаційні системи автоматизованого управління, що охоплює всі ключові рівні від периферійних пристроїв до хмарного інтелектуального ядра. Спочатку побудовано ієрархічну структурно-функціональну модель, яка завдяки чіткій децентралізації ресурсів та стандартизованим інтерфейсам забезпечує масштабованість, відмовостійкість і горизонтальний перенос знань між галузями. Виокремлення площин пристроїв, передавання даних, автоматизованої інфраструктури та

інтелектуальної обробки створює логічно замкнений цикл, у якому телеметрія трансформується в узгоджені оновлення моделей без втрати конфіденційності.

На основі аналізу системних, статистичних, комунікаційних і регуляторних викликів обґрунтовано необхідність удосконалення класичних алгоритмів FedSGD та FedAvg. Запропонований метод середньозваженого оцінювання впливу локальних моделей вводить динамічні вагові коефіцієнти, що коригуються показниками прогностичної точності та стабільності навчання кожного клієнта. Такий підхід усуває негативний внесок неінформативних або зашумлених вибірок, автоматично фільтрує статистичні викиди й підвищує точність глобальної моделі без додаткового розкриття даних.

Розроблена багатораундна стратегія федеративного навчання реалізує безперервну самоадаптацію периферійних вузлів завдяки циклічному обміну знаннями з хмарним оркестратором. Поєднання асинхронного передавання зашифрованих градієнтів, робастної агрегації з байєсівською оцінкою надійності клієнтів і поступового змішування ваг під час зворотної синхронізації забезпечує стійкість до атак, знижує затримку та мінімізує енергоспоживання. Інтеграція цієї стратегії з методом середньозваженого оновлення параметрів створює синергетичний ефект, що гарантує монотонне покращення точності без переривання виробничих процесів.

Додатково запропоновано ресурсно-орієнтовані алгоритми граничних та туманних обчислень, а також механізми стимулювання участі клієнтів, які оптимізують розподіл обчислювальних і мережевих ресурсів у гетерогенних середовищах. У сукупності ці результати формують науково обґрунтовану платформу для довготривалого самонавчання інтелектуальних інформаційно-комунікаційних систем, здатних оперативно реагувати на динаміку технологічних та експлуатаційних умов, зберігаючи при цьому високий рівень конфіденційності, відмовостійкості та ефективності.

РОЗДІЛ 3. ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

У цьому розділі наведено методологічні засади та результати експериментальної верифікації запропонованої моделі децентралізованої обробки даних на базі федеративного машинного навчання, адаптованої до вимог індустріального середовища. Особливу увагу приділено двом групам експериментів: тестуванню базової версії алгоритму на наборі даних Numenta Anomaly Benchmark (NAB) [97] та перевірці удосконаленого алгоритму з багатораундним усередненням на телеметричних даних автономно керованого пристрою Formica-1.

3.1 Методика та результати експериментальної оцінки базового алгоритму федеративного навчання

Для первинної верифікації запропонованої парадигми використано набір даних Numenta Anomaly Benchmark (NAB), що містить вимірювання температури внутрішнього компонента великої промислової машини й забезпечує прозору структуру та якісну анотацію аномалій. Температурний режим, зокрема стан підшипників, є ключовим індикатором справності обладнання: відхилення температури може спричинити раптові зупинки лінії, надмірне енергоспоживання та скорочення ресурсу автономних транспортних роботів. Дані накопичувалися безперервно протягом сімдесяти діб із дискретністю п’ять хвилин, що забезпечило достатній часовий горизонт для аналізу динамічних трендів.

Експеримент проводився в імітаційному середовищі, яке відтворювало архітектуру федеративного навчання: моделі штучного інтелекту тренувалися безпосередньо на периферійних вузлах, що відстежують роботу автономних мобільних роботів-транспортерів. Виключення локальних серверів підвищувало рівень інформаційної безпеки, оскільки первинні дані не покидали пристрої, та одночасно зменшувала комунікаційне навантаження. Вихідний температурний

датасет стратифіковано на чотири логічно незалежні частини: три підмножини (≈ 30 % кожна) призначалися для навчання трьох віртуальних клієнтів, що репрезентували різні виробничі ділянки, тоді як решта 10 % використовувалася виключно для підсумкової валідації. На кожному клієнті здійснювалося локальне навчання рекурентної мережі LSTM, здатної враховувати часову кореляцію показників.

Агрегування параметрів здійснено за допомогою класичного алгоритму FedAvg, після завершення локального навчання вектори ваг передавалися до центрального координатора, де їх рівнозначно усереднювали; сформована глобальна модель розповсюджувалася назад на периферійні вузли, утворюючи спільну базу знань для всієї федерації. Прогностична здатність перевірялася шляхом екстраполяції температури на заданий момент у майбутньому.

Ефективність підходу оцінювали за середньоквадратичною помилкою (MSE), кореневою середньоквадратичною помилкою (RMSE) та середньою абсолютною відносною помилкою (MAPE). Аналіз результатів показав, що глобальна модель перевершує кожну з локальних у середньому на 3–5 %, що доводить переваги обміну параметрами навіть за статистично неоднорідних вибірок. Такий результат підтверджує практичну здійсненність федеративного навчання у виробничому середовищі автономних роботів без централізованої обробки даних і закладає підґрунтя для подальшого вдосконалення алгоритму шляхом адаптивного зважування внеску клієнтів.

Результати моделювання, представлені на рис. 3.1, показують, що клієнт 2 відтворює температурну динаміку з мінімальними MSE, RMSE та MAPE: тренди прогнозованих і фактичних значень практично збігаються. Для клієнтів 1 та 3 точність нижча; особливо помітне погіршення після часової позначки 1500, коли помилки зростають, а розходження кривих стає суттєвим. Глобальна модель забезпечує проміжні показники, узагальнюючи локальні закономірності, проте висвітлює потребу в адаптивному врахуванні якості окремих клієнтів для подальшого підвищення точності прогнозування.

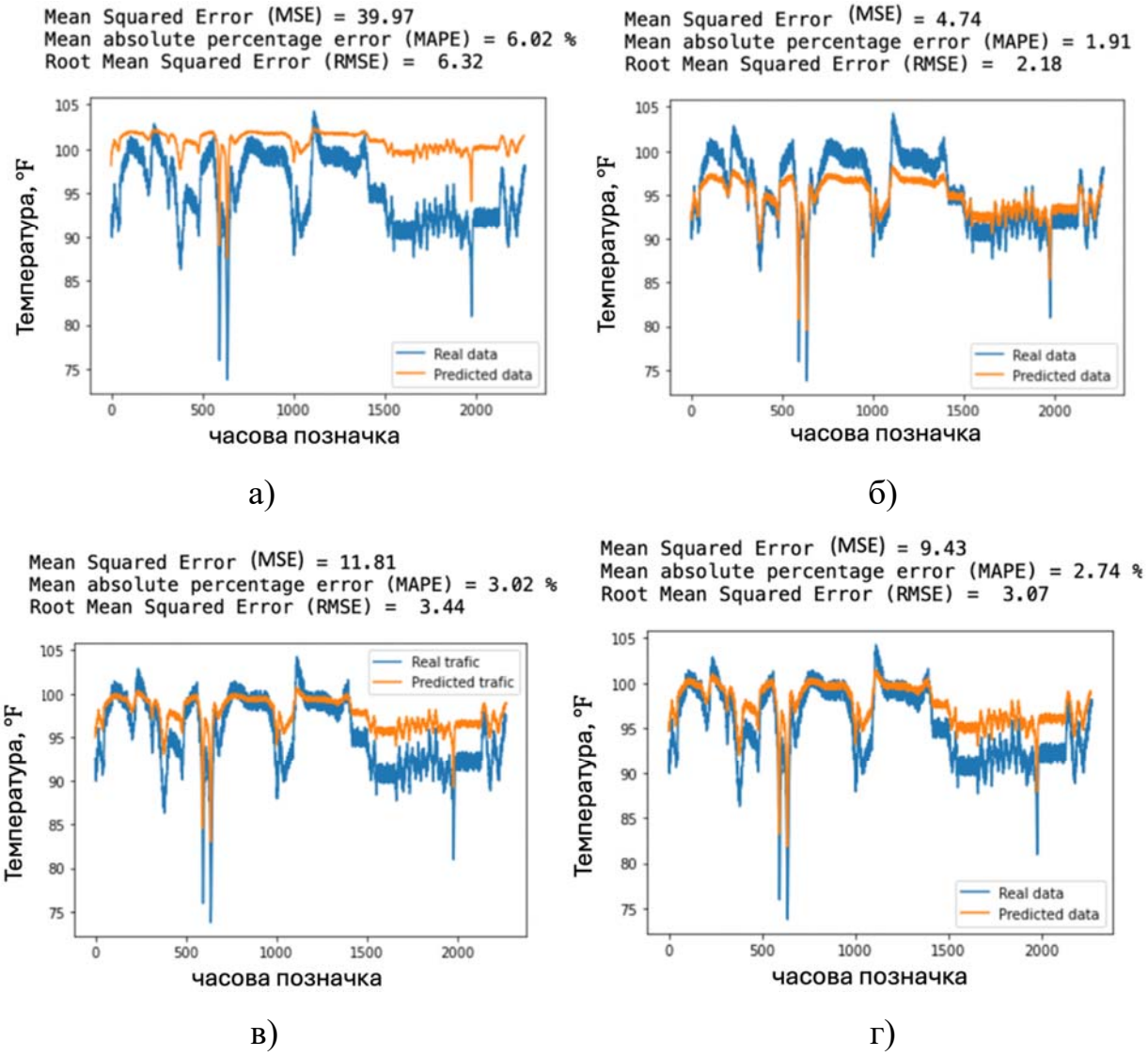


Рисунок 3.1. Порівняння реальних та прогнозованих значень для локальних – а), б), в) та глобальної – г) моделей.

Щоб наочно порівняти точність прогнозування моделей, зобразімо їх на одному графіку (рис. 3.2). Результати свідчать, що глобальна модель демонструє вищу точність порівняно з локальними моделями віртуальних клієнтів. Найбільше покращення зафіксовано для першого клієнта: під час навчання лише на його власних даних середньоквадратична помилка (MSE) становила 39,97, тоді як після агрегування ваг і формування глобальної моделі вона зменшилася до 9,43.

Для третього клієнта поліпшення точності менш виражене: до оновлення глобальної моделі показник MSE дорівнював 11,81. Дані другого клієнта виявилися найрепрезентативнішими, оскільки до агрегування його значення MSE становило лише 4,74, що забезпечило найнижчу помилку прогнозування температури.

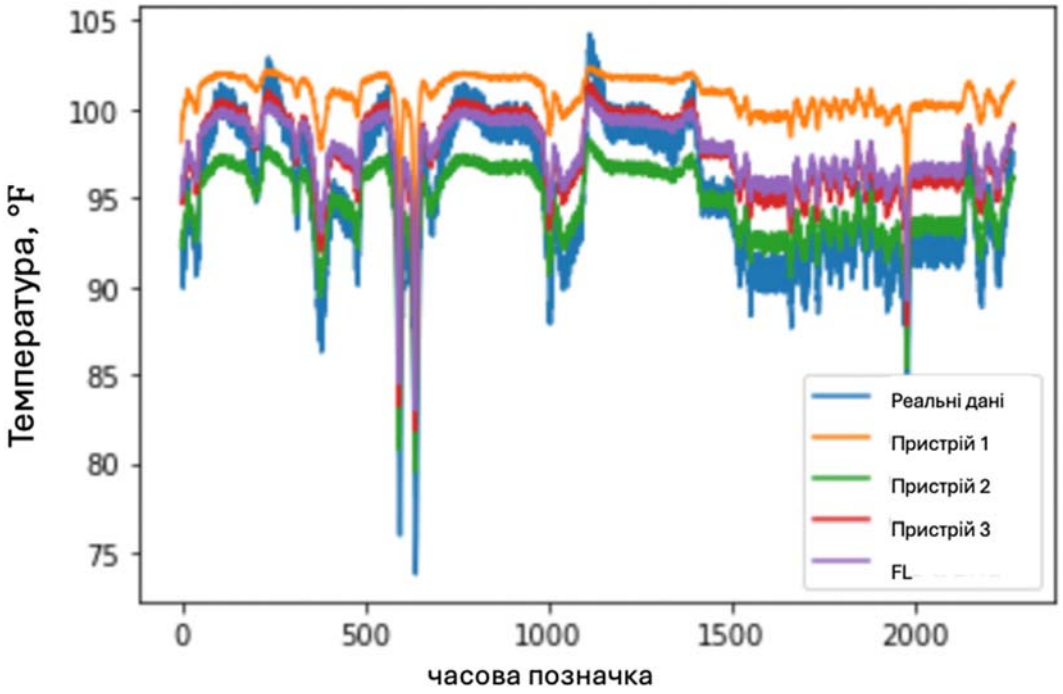


Рисунок 3.2. Порівняння точності прогнозування локальних моделей і глобальної агрегованої моделі.

Пристроям-клієнтам 1 і 3, результати роботи яких наведено на рис. 3.1,а та 3.1, в, не мали достатньої кількості навчальних прикладів, тому точність їхніх прогнозів виявилася нижчою. Параметри другого клієнта (рис. 3.1, б), збагачені репрезентативнішим набором даних, після агрегування підвищили точність глобальної моделі на тестовій вибірці. Водночас до глобальної моделі потрапили й похибки, зумовлені неповною інформативністю даних клієнтів 1 і 3, що спричинило неідеальні, хоч і кращі порівняно з локальними моделями 1 і 3, показники прогнозування у відповідному інтервалі.

Експеримент засвідчив загальне зростання точності прогнозування серед усіх віртуальних клієнтів, що підвищує точність оцінки температурних сигналів

автономних мобільних роботів (AGV) й підтверджує доцільність упровадження федеративного навчання у завданнях виявлення аномалій у розумному виробництві. Дослідження також довело, що технологія FL дає змогу зберегти конфіденційність даних без втрати точності прогнозування.

Порівняльний аналіз точності прогнозування локальних клієнтів і зведеної моделі показав, що навіть за рівноважного усереднення ваг федеративне навчання забезпечує стійкіше узагальнення, тоді як окремі моделі схильні до надмірної спеціалізації на власних підмножинах даних. Виявлений ефект став підґрунтям для подальшого вдосконалення стратегії агрегації з урахуванням індивідуальної якості локальних моделей.

3.2 Моделювання удосконаленого алгоритму федеративного навчання на даних телеметрії AGV Formica-1 при різній кількості раундів тренування

Експериментальна серія з автономним візком Formica-1 дала змогу сформувати репрезентативний масив телеметричних вимірювань, до якого увійшли миттєве й кумулятивне енергоспоживання, напруга тягового акумулятора, частота обертання двигунів, струмові навантаження, інтегральна пройдена відстань, температури підшипників, сигнали приводу транспортувального штифта та миттєва механічна частота. У межах зазначеного масиву як цільовий було обрано параметр «миттєва споживна потужність, Вт», оскільки саме енергоспоживання є ключовим індикатором технічного стану силових агрегатів: відхилення цієї величини нерідко свідчить про зародження дефектів, які можуть спричинити незапланований простій обладнання або знизити енергоефективність виробництва [98].

Для перевірки дієздатності удосконаленого алгоритму федеративного навчання було розгорнуто середовище моделювання, у якому кілька віртуальних клієнтів емулювали окремі візки AGV [99-102]. Дані реальних пристроїв завантажувалися на відповідні клієнтські вузли, після чого

виконувалося локальне навчання LSTM-моделі. Експеримент складається з двох взаємопов’язаних частин. По-перше, встановлювалася придатність різних критеріїв агрегації шляхом усереднення локальних ваг за мінімумом валідаційної похибки та за середнім значенням MSE. По-друге, аналізувався вплив багатораундного узгодження на точність прогнозу. Для цього телеметрію сегментували на логічні раунди, причому розглядалися дві стратегії формування навчальних вибірок. У першій стратегії кожний раунд оперував винятково новою порцією даних, тоді як у другій до поточного набору додавалися приклади з попередніх раундів, що відтворює реальну практику кумулятивного накопичення досвіду в експлуатаційних умовах.

Перед початком циклу федеративного навчання було побудовано еталонну модель LSTM, натреновану централізовано на повному масиві телеметрії. Вона забезпечила на тестовій вибірці значення MSE=1029 і стала вихідною точкою для подальшого оцінювання ефективності запропонованих алгоритмів федеративного навчання (рис. 3.3). Усі подальші експерименти з FL проводилися при однакових гіперпараметрах локального тренування, що дало змогу коректно порівняти приріст точності, обумовлений саме механізмом багатораундного агрегування та вибором критерію зважування локальних моделей.

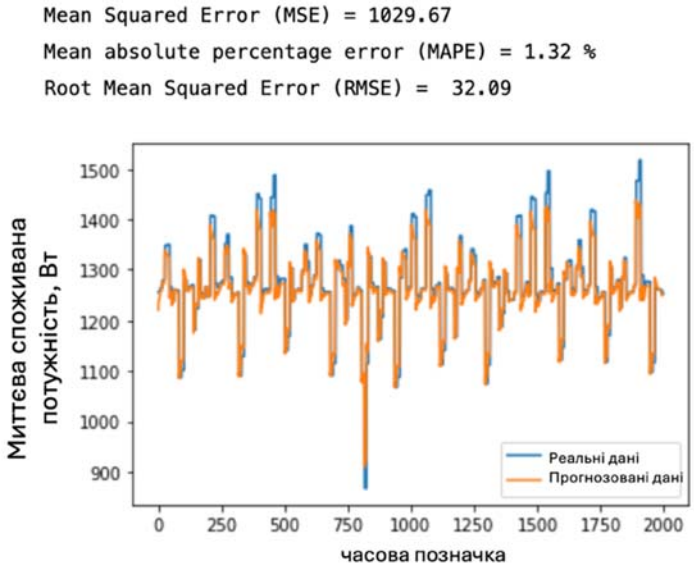


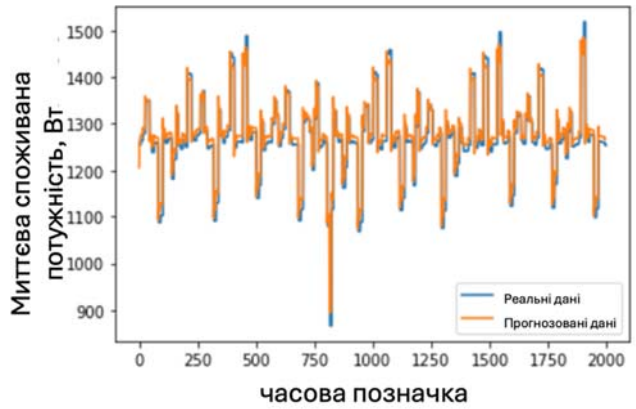
Рисунок 3.3. Порівняння реальних та прогнозованих значень окремої моделі LSTM, навченої на всьому навчальному наборі даних

3.2.1 Усереднення локальних моделей за метрикою MSE

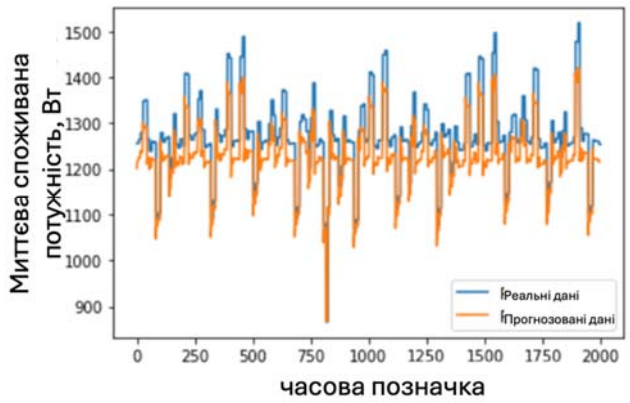
Для дослідження ефективності різних схем агрегації було застосовано стратифікований розподіл телеметрії AGV Formica-1: три підвибірки по 28,6 % кожна використовувалися як навчальні дані для трьох віртуальних клієнтів, а залишкові 14 % забезпечували незалежний тест. На кожному клієнті відбувалося локальне навчання LSTM-мережі; після завершення тренування вагові коефіцієнти моделі зберігалися у вигляді тензора параметрів, а додатково фіксувалися значення середньоквадратичної помилки (MSE) та валідаційної втрати.

Подальше формування глобальної моделі здійснювалося на центральному координаторі у двох варіантах. У першому варіанті коефіцієнт впливу кожної локальної моделі визначався на основі інверсії її MSE, у другому - на основі інверсії валідаційних втрат; обидва значення нормалізувалися за формулою 2.12, що передбачає ділення на N-1, де N - кількість клієнтів. Під час обчислення усередненого тензора параметрів ваги кожного клієнта множилися на відповідний нормалізований коефіцієнт (формула 2.16), після чого здійснювалося підсумовування. Отримані дві глобальні моделі на основі MSE та на основі втрат повернуто на периферійні вузли для подальшого прогнозування миттєвого енергоспоживання.

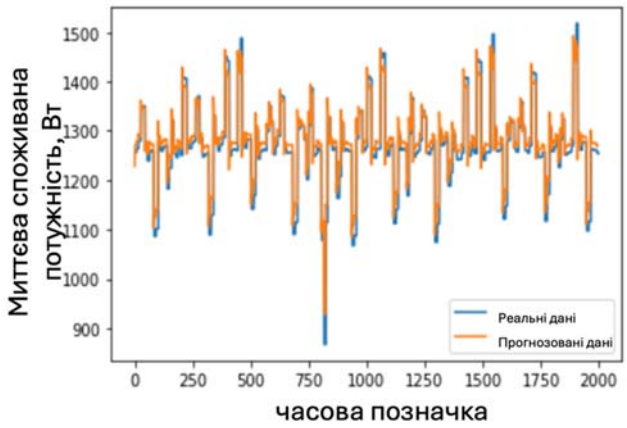
Порівняльний аналіз, виконаний за метрикою MSE, показав, що варіант із зважуванням, базованим на валідаційних втратах, забезпечує дещо нижчу похибку на тестовій вибірці порівняно з підходом, який використовує MSE, що підтверджується графічними залежностями на рис. 3.4 (локальні моделі) та рис. 3.5 (глобальні моделі). Отримані результати свідчать про доцільність урахування валідаційних характеристик локальних агентів під час агрегації, оскільки такий підхід краще відображає узагальнену здатність моделі до прогнозування на невідомих даних.



а) MSE=630

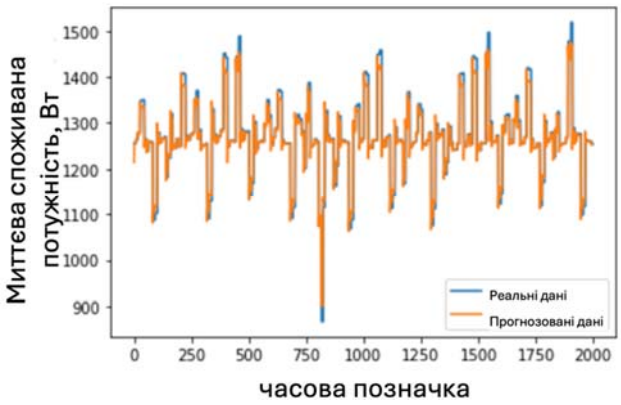


б)MSE = 3258

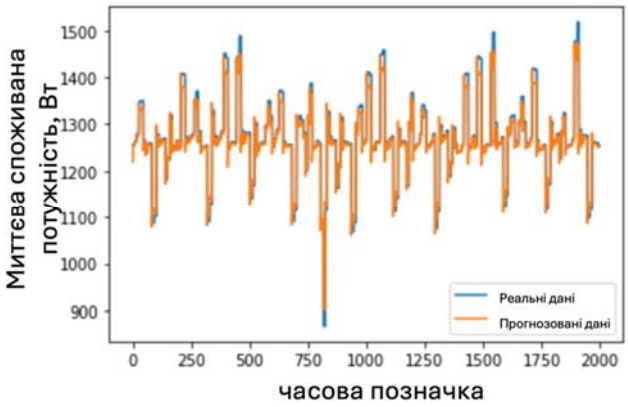


в) MSE=2915

Рисунок 3.4. Порівняння точності прогнозування локальних моделей на тестових даних



а) MSE = 878



б) MSE = 908

Рисунок 3.5. Порівняння точності прогнозування глобальних моделей при агрегуванні локальних моделей на основі MSE метрики - а) та валідаційних втрат - б).

Отримані експериментальні результати свідчать, що обидві глобальні моделі, сформовані шляхом федеративної агрегації, перевершують за точністю кожну з локальних моделей на тестовій вибірці. Таке підвищення точності зумовлене ефектом кумулятивного обміну знаннями між клієнтами, який урівноважує статистичні відмінності окремих підмножин телеметрії. Додаткове зіставлення двох стратегій вагового усереднення показало, що найнижчого значення похибки вдалося досягти при використанні коефіцієнтів, обчислених на основі інверсії MSE, оскільки ця модель забезпечила більш точне відтворення профілю миттєвого енергоспоживання.

Загалом, обидва варіанти федеративної агрегації демонструють кращі показники, ніж еталонна централізована LSTM-модель без застосування федеративного навчання (рис. 3.3). Таким чином, федеративний підхід не лише гарантує збереження конфіденційності промислових даних, а й підвищує точність прогнозування критичних параметрів стану автономних транспортних роботів, що підтверджує його доцільність для застосувань автоматизованого управління індустріальною інфраструктурою.

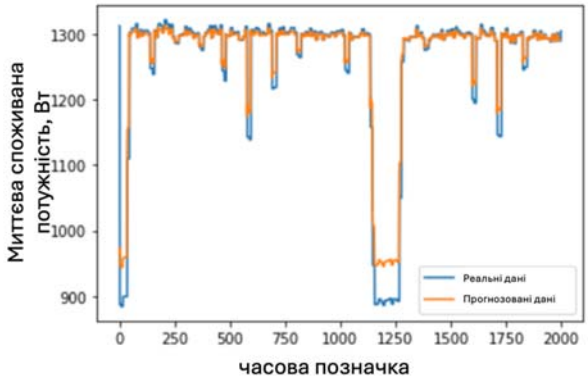
3.2.2. Оцінювання точності багатораундного усереднення

Мета другого експерименту полягала у вивченні змін глобальної моделі під час послідовних раундів федеративного навчання, коли дані кожного клієнта поділялися на кілька часових фрагментів. На кожному раунді локальні мережі тренувалися на новій частині вибірки, після чого їхні параметри агрегувалися у координатора й поверталися клієнтам у складі оновленої глобальної моделі. Організація експерименту передбачала три конфігурації з двома, чотирма та вісьмома раундами, а експеримент проходив за нижченаведеною послідовністю.

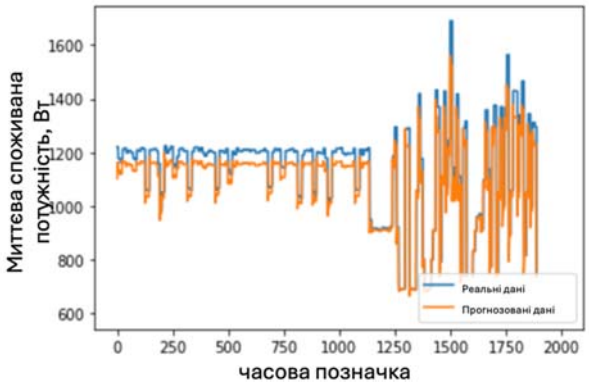
1. Дані кожного клієнта поділялися на відповідну кількість частин. Під час першого раунду локальні LSTM-моделі навчалися на першій частині.

2. Після завершення тренування виконувалося вагове усереднення, що дало першу глобальну модель.
3. Клієнти завантажували отриману глобальну модель і навчалися на другій частині власних даних.
4. Агреговані параметри формували чергову глобальну модель.

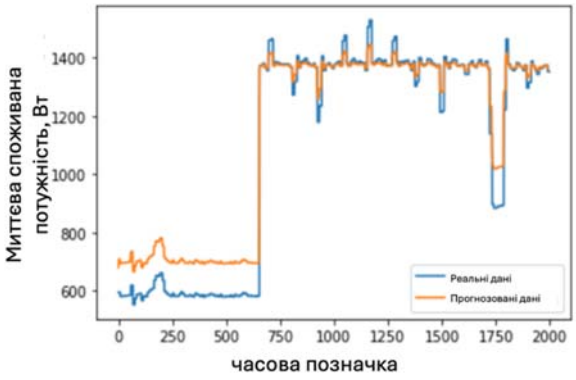
Кроки навчання і агрегації повторювалися до завершення вибраної кількості раундів. У першому експерименті вагові коефіцієнти для усереднення визначалися через MSE, обчислену на даних поточного раунду. У другому для тієї самої мети використано MSE, розраховану на кумулятивному наборі, що містив усі попередні раунди. Точність локальних моделей після першого раунду подана на рис. 3.6, а сформована глобальна модель представлена на рис. 3.8а. Під час другого раунду клієнти використали модель першого раунду і тренувалися на другій частині даних (рис. 3.7). Після повторного усереднення було отримано вдосконалену глобальну модель (рис. 3.8б).



а) MSE = 523

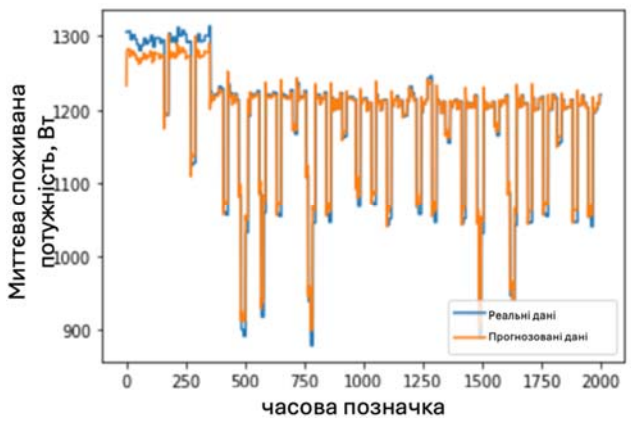


б) MSE = 5492

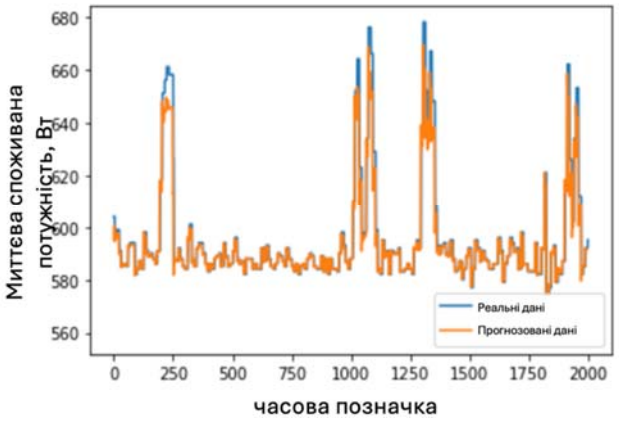


в) MSE = 5599

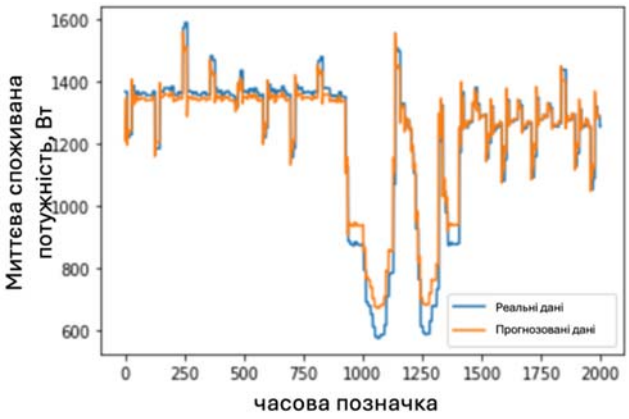
Рисунок 3.6. Точність прогнозування локальних моделей після першого раунду навчання.



а) MSE = 711

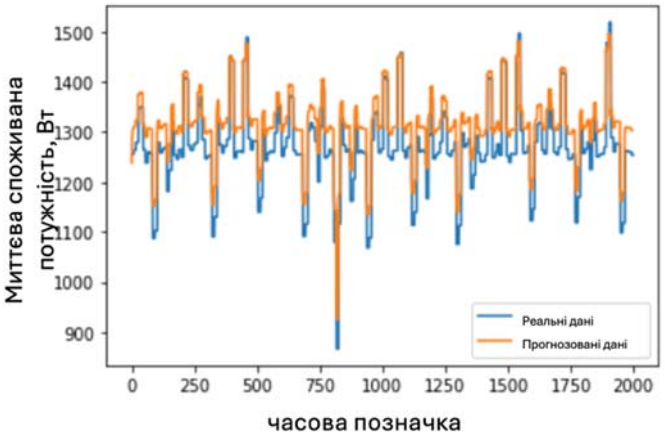


б) MSE = 31

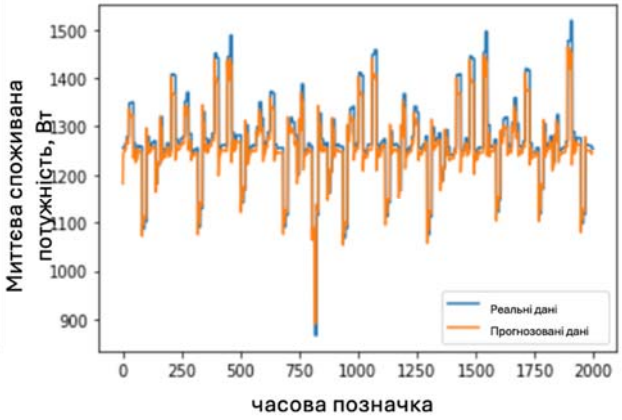


в) MSE = 2184

Рисунок 3.7. Точність прогнозування локальних моделей після другого раунду навчання.



а) MSE = 2831



б) MSE = 1096

Рисунок 3.8: Точність прогнозування глобальної моделі після першого раунду навчання - а) та другого раунду навчання - б).

У другій частині експерименту дані клієнтів було розділено на чотири частини, після чого було проведено чотири раунди усереднення. У кожному раунді середньоквадратичну похибку (MSE) обчислювали лише на основі навчальних даних, що використовувалися для тренування локальних моделей у відповідному раунді. Результати глобальних моделей після першого, другого, третього та четвертого раундів подано на рисунку 3.9 та в таблиці 3.1.

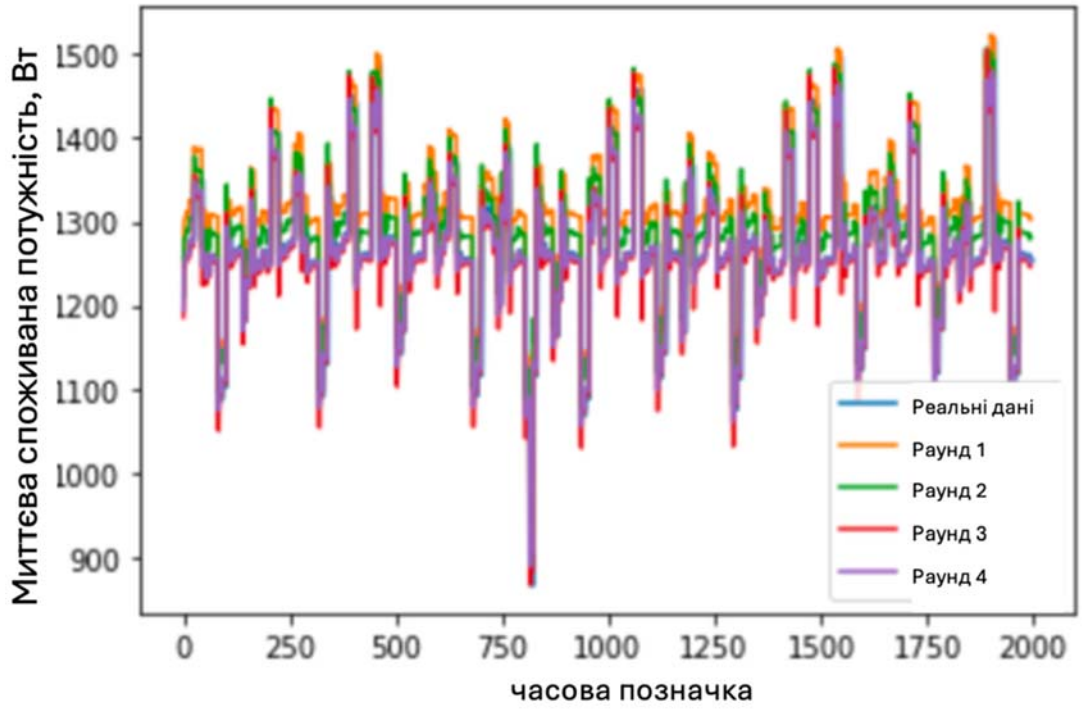


Рисунок 3.9. Порівняння точності глобальних моделей для кожного раунду в межах чотирираундного усереднення.

Таблиця 3.1. Точність для кожного раунду при чотирьох раундах

Раунд	MSE	MAPE
GM Раунд 1	2 898.24	3.89%
GM Раунд 2	1 422.04	2.28%
GM Раунд 3	1 004.86	1.32%
GM Раунд 4	868.15	1.02%

Аналіз отриманих даних показав поступове підвищення точності глобальної моделі зі збільшенням кількості раундів. Хоча сумарний обсяг вибірки у дво- та чотирираундних конфігураціях залишався незмінним, остаточна модель, сформована після чотирьох раундів, забезпечила значно

кращі прогностичні характеристики. Пояснення полягає у більшій кількості ітерацій узгодження локального досвіду, що сприяло глибшій адаптації агрегованих параметрів до статистичної структури даних. Постійне оновлення локальних мереж за рахунок включення нових фрагментів вибірки в кожному раунді дало змогу підвищити узагальнювальну здатність системи та зменшити похибку прогнозу миттєвого енергоспоживання автономних транспортних роботів.

У третій частині експерименту дані клієнтів було поділено на вісім частин, після чого було проведено вісім раундів усереднення. Результати глобальних моделей після першого, другого, третього, четвертого, п’ятого, шостого, сьомого та восьмого раундів наведено на рис. 3.10 та в таблиці 3.2.

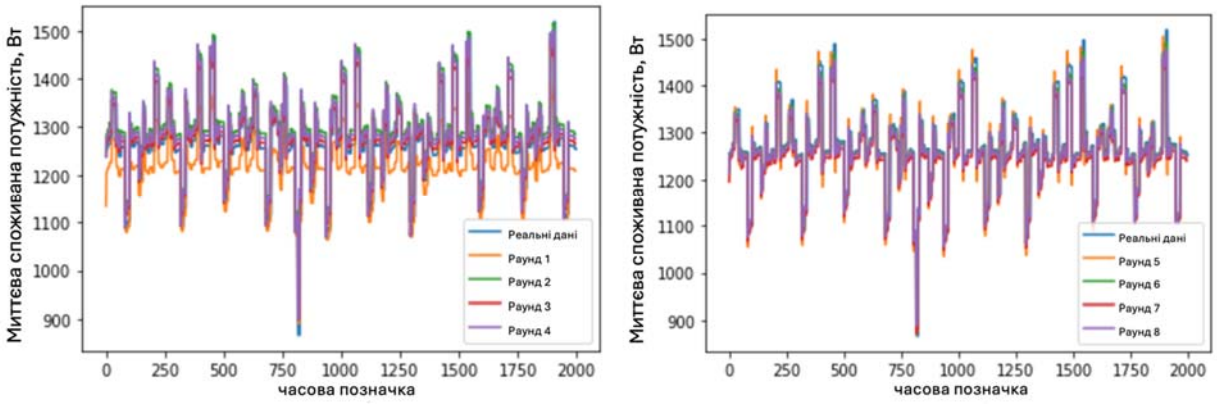


Рисунок 3.10. Порівняння точності глобальних моделей після раундів 1, 2, 3, 4, 5, 6, 7 і 8 у межах восьмираундного усереднення.

Таблиця 3.2. Точність для кожного раунду при восьми раундах

Номер раунду	**MSE**	**MAPE**
GM Раунд 1	3 923.97	4.24%
GM Раунд 2	1 646.56	2.62%
GM Раунд 3	933.92	1.37%
GM Раунд 4	1 202.75	1.94%
GM Раунд 5	956.82	1.23%
GM Раунд 6	840.35	0.92%
GM Раунд 7	1 096.57	1.66%
GM Раунд 8	890.85	1.12%

З результатів бачимо, що ефективність глобальної моделі після восьмого раунду є подібною до результатів попередньої частини експерименту, де використовувалося лише чотири раунди. Це свідчить про те, що глобальна модель була добре оптимізована в обох випадках. Однак також видно, що ефективність моделі не зростає стабільно, а фіксуються незначні флуктуації, як-от погіршення результатів у четвертому раунді.

Це можна пояснити тим, що в межах цього експерименту для запуску локальних моделей та обчислення MSE використовувалися лише нові навчальні дані відповідного раунду. Як наслідок, значення MSE між локальними моделями могли бути недостатньо корельованими, наприклад, через обмежений розмір даних у певній частині набору, що могло призвести до низького значення похибки.

Зважаючи на це, було вирішено провести додатковий експеримент, у якому для обчислення MSE локальних моделей використовувалися не лише нові навчальні дані, доступні на пристрої, а й історичні навчальні дані, які застосовувалися на клієнті в попередніх раундах.

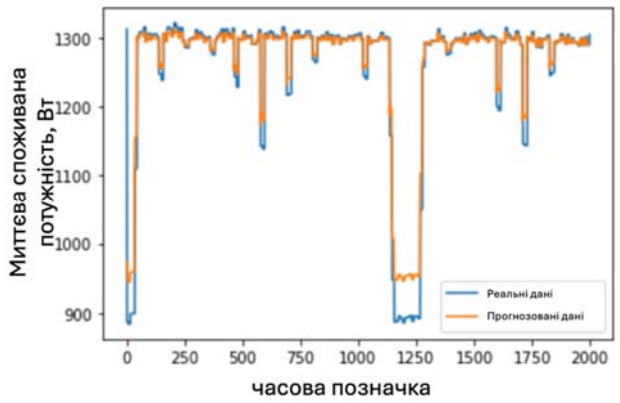
3.2.3 Оцінювання точності багатораундного усереднення з кумулятивним розширенням навчальних вибірок

У цьому дослідженні збережено структуру попереднього експерименту, коли телеметрія кожного клієнта була розподілена на два, чотири та вісім раундів федеративного навчання. Відмінність полягає у способі визначення вагових коефіцієнтів під час агрегації. Значення середньоквадратичної помилки для кожної локальної мережі обчислювали на всій доступній на момент раунду навчальній вибірці, тобто до даних поточного кроку додавали інформацію, накопичену на попередніх етапах.

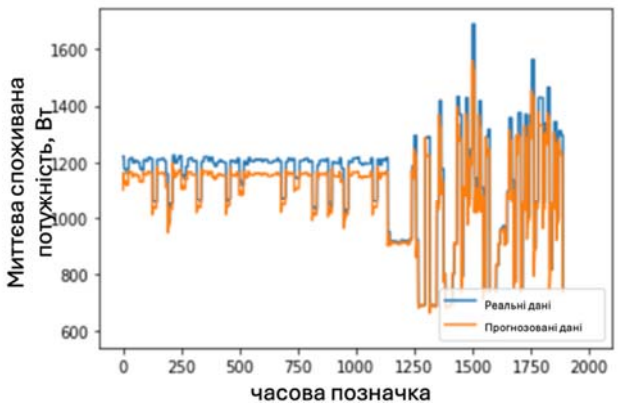
На конфігурації з двома раундами перша частина вибірки використовувалася для побудови початкових локальних моделей і формування базової глобальної мережі, тож результати повністю збіглися з результатами підрозділу 3.2.2. Зміни стали помітними під час другого раунду, коли кожен

клієнт уже мав в розпорядженні кумулятивний набір навчальних прикладів. Нові значення MSE, обчислені на розширених вибірках, скоригували вагові коефіцієнти й забезпечили точніше усереднення параметрів локальних мереж.

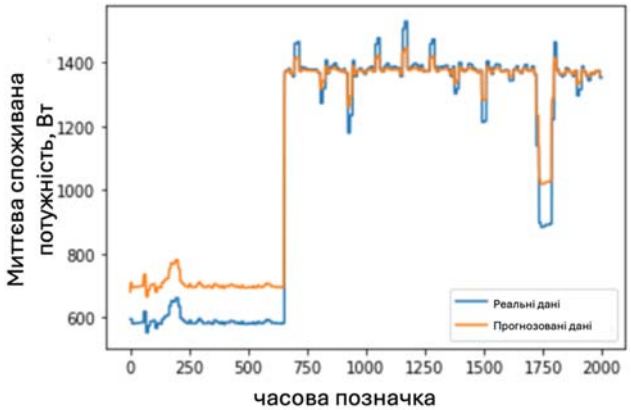
Графік на рис. 3.11 демонструє, що точність прогнозу після першого раунду збігається з результатами базового експерименту, оскільки обсяг даних залишався тотожним. На рис. 3.12 наведено ефективність локальних моделей після другого раунду. Порівняння двох підходів до обчислення MSE показує перевагу кумулятивної стратегії, яку ілюструє суттєве зменшення помилки глобальної мережі на рис. 3.13. Отже, використання розширеної навчальної вибірки для оцінювання MSE дає змогу точніше відобразити актуальний досвід клієнта, що підвищує якість агрегації та забезпечує поліпшення прогнозних властивостей системи.



а) MSE = 523

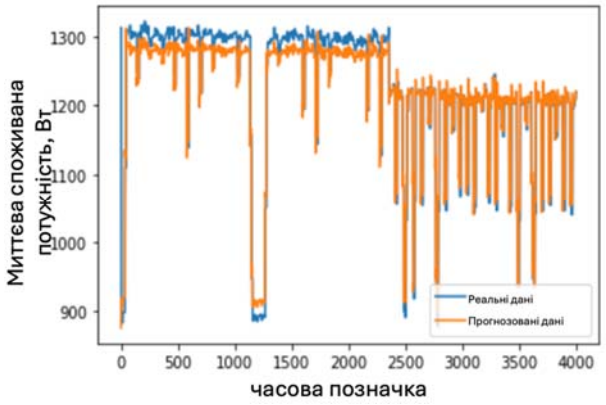


б) MSE = 5492

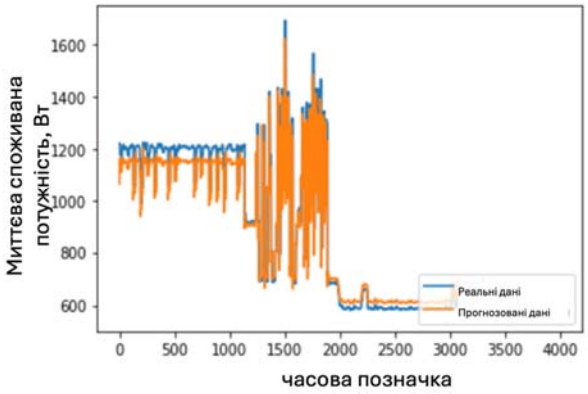


в) MSE = 5599

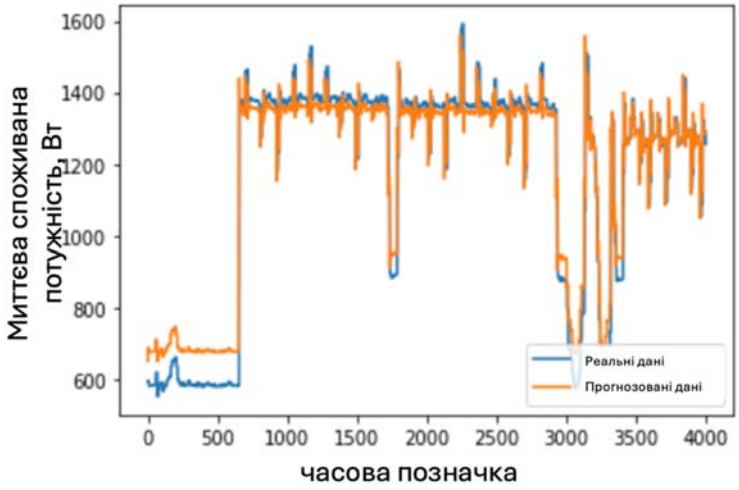
Рисунок 3.11: Точність прогнозування локальних моделей після першого раунду навчання



а) MSE = 633

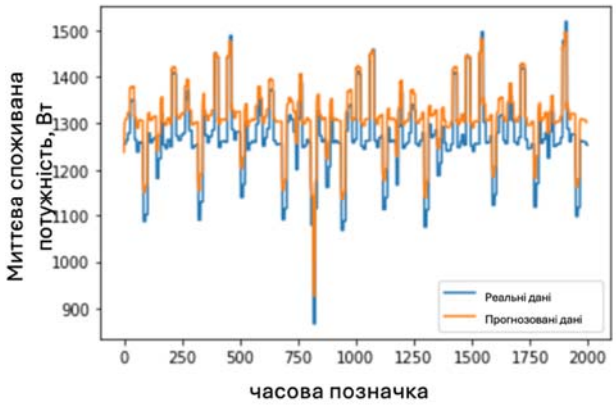


б) MSE = 3232

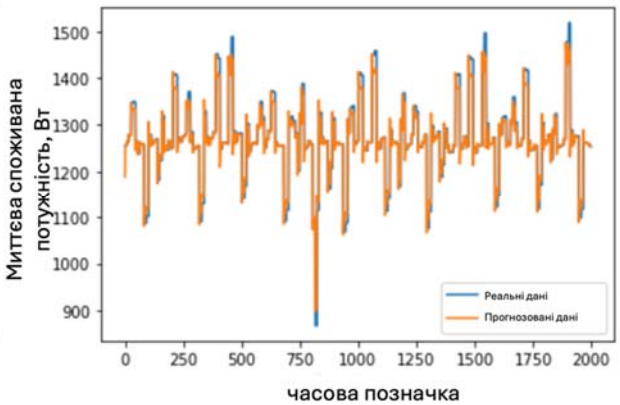


в) MSE = 2998

Рисунок 3.12: Точність прогнозування локальних моделей після другого раунду навчання



а) MSE = 2831



б) MSE = 911

Рисунок 3.13. Точність прогнозування глобальної моделі після першого раунду навчання - а) та другого раунду навчання - б).

У другій частині цього експерименту дані клієнтів було розподілено на чотири частини, після чого було проведено чотири раунди усереднення. Значення MSE обчислювались на основі навчального набору даних, що використовувався для тренування локальних моделей як у поточному, так і в попередніх раундах. Результати глобальних моделей після 1-го, 2-го, 3-го та 4-го раундів наведені на рисунку 3.14 та в таблиці 3.3.

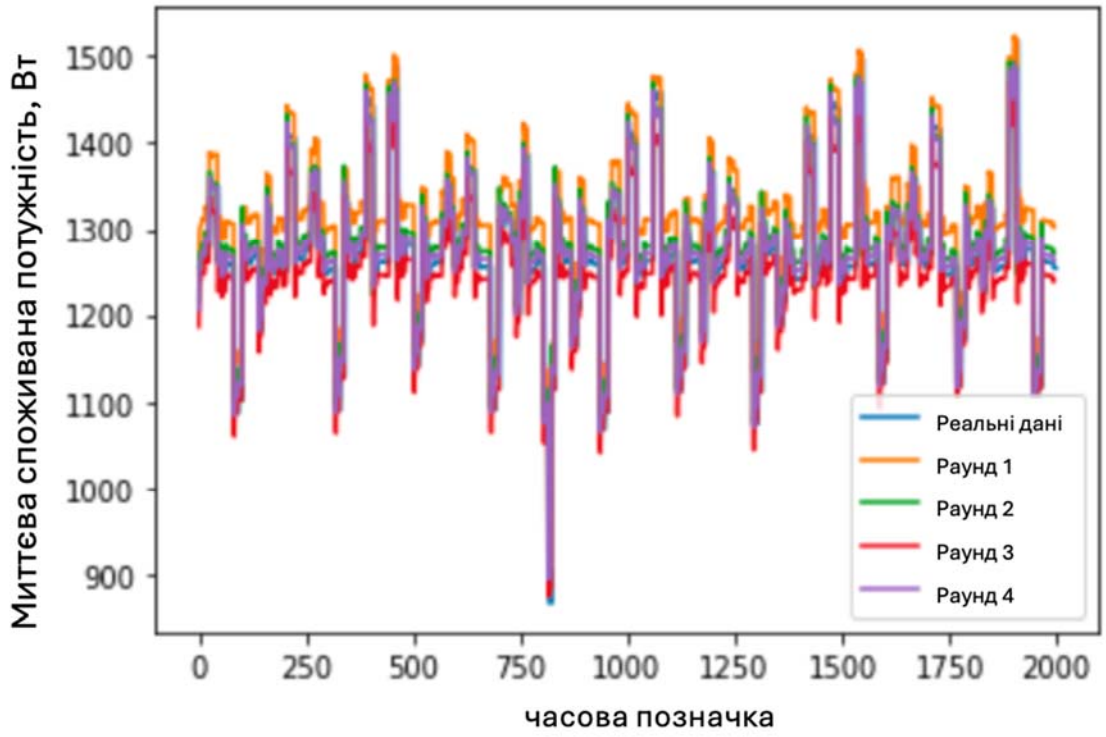


Рисунок 3.14. Порівняння точності глобальних моделей після кожного раунду при чотирираундному усередненні на основі розширеного навчального набору даних

Отримані результати близькі до тих, що були отримані в попередній частині експерименту, де значення MSE для подальшого усереднення обчислювались лише за навчальними даними конкретного раунду. Водночас, ці результати є кращими за результати моделі без усереднення або моделі, побудованої лише після двох раундів усереднення. Це також підтверджує, що з використанням федеративного навчання можна отримати глобальну модель для більш точної прогнозної оцінки сигналів.

Таблиця 3.3. Точність для кожного раунду при чотирираундному усередненні на основі розширеного навчального набору даних

№ раунду	MSE	MAPE
GM Раунд 1	2 898.24	3.89%
GM Раунд 2	1 087.32	1.74%
GM Раунд 3	1 209.24	1.79%
GM Раунд 4	875.07	1.16%

У третій частині експерименту дані клієнтів були поділені на вісім частин, після чого було проведено вісім раундів усереднення. Результати глобальних моделей після всіх восьми раундів наведено на рисунку 3.15 та в таблиці 3.4.

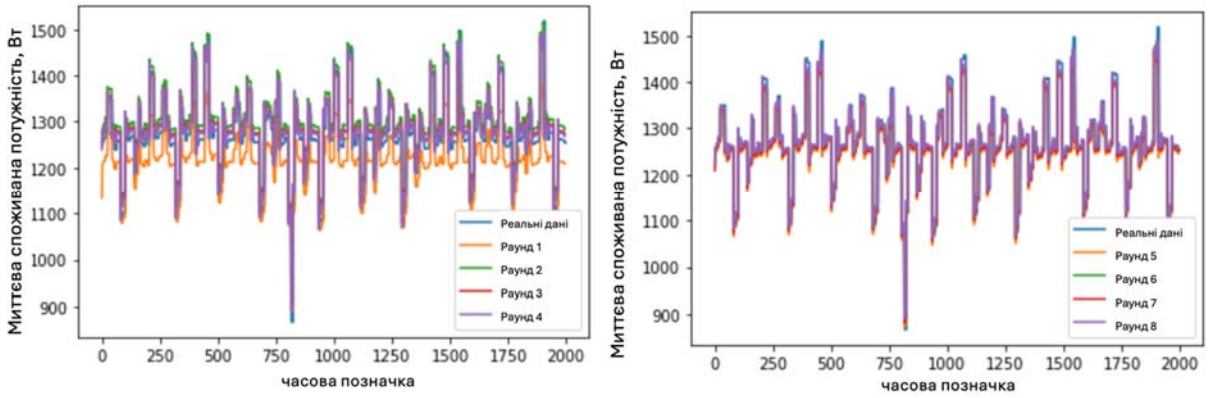


Рисунок 3.15. Порівняння точності глобальних моделей після 1-8 раундів при восьмираундному усередненні на основі розширеного навчального набору даних.

Результати, отримані в цій частині експерименту, демонструють найкращу точність прогнозування. Це підтверджує, що частіший обмін досвідом між AGV сприяє кращому прогнозуванню енергоспоживання. Також це доводить доцільність обчислення значень MSE для подальшого усереднення шляхом тренування локальних моделей на всіх наявних навчальних даних пристрою, оскільки це забезпечує точніше агрегування локальних моделей.

Коливання значень MSE та MAPE, які можна спостерігати в таблицях 3.3 та 3.4, є наслідком поділу датасетів і різних характеристик наборів даних, наданих агентам у різних раундах. Однак загальний підхід полягає у

використанні методу федеративного навчання з елементами безперервного навчання, що з часом робить поділ навчального набору даних менш релевантним, оскільки локальні та глобальна моделі постійно оновлюються.

Таблиця 3.4. Точність для кожного раунду при восьмираундному усередненні на основі розширеного навчального набору даних

№ раунду	MSE	MAPE
GM Раунд 1	3 923.97	4.24%
GM Раунд 2	1 626.64	2.59%
GM Раунд 3	1 116.07	1.81%
GM Раунд 4	999.67	1.54%
GM Раунд 5	954.54	1.28%
GM Раунд 6	841.26	0.92%
GM Раунд 7	872.01	1.04%
GM Раунд 8	833.72	0.92%

Усі виконані експериментальні серії підтвердили доцільність використання федеративного навчання для обміну досвідом між автономними транспортними роботами. Зведені показники наведено в таблиці 3.5. У першій серії випробувань встановлено, що федеративна агрегація покращує точність прогнозу контрольного сигналу, отже підвищується здатність своєчасно виявляти аномалії без потреби передавання сирих телеметричних даних за межі пристрою.

Таблиця 3.5. Порівняння результатів в усіх проведених експериментах

Експеримент	MSE
LSTM без FL	1029.67
FL, 1 раунд, на основі validation loss	908.78
FL, 1 раунд, на основі MSE	878.83
FL, 2 раунди, на основі навчального набору	1096.79
FL, 2 раунди, на основі розширеного набору	911.89
FL, 4 раунди, на основі навчального набору	868.15
FL, 4 раунди, на основі розширеного набору	875.07
FL, 8 раундів, на основі навчального набору	890.85
FL, 8 раундів, на основі розширеного набору	833.72

Друга та третя серії продемонстрували перевагу ітеративного перенавчання локальних моделей на кумулятивному наборі даних порівняно зі стратегією, де кожен раунд спирається лише на нову порцію вибірки. Найвищу точність отримано під час конфігурації з вісьмома раундами, коли узгодження параметрів здійснювалося на основі середньоквадратичної помилки, обчисленої для розширених локальних вибірок. У цьому режимі середня похибка прогнозу зменшилася на 19% відносно еталонної LSTM-моделі без федеративної синхронізації, що підтверджує ефективність запропонованого підходу для індустріальних застосувань автономних роботизованих систем.

3.3 Висновки до розділу

У розділі проведено комплексне експериментальне випробування розроблених алгоритмів федеративного навчання на телеметричних даних автономних пристроїв типу Formica-1 з різною кількістю раундів тренування. Результати підтвердили перевагу ітеративного перенавчання локальних мереж на повному накопиченому датасеті, що забезпечило стійке зменшення прогнозної похибки та поліпшення узагальнюючих властивостей агрегованої моделі. Запропонована адаптивна схема агрегації, у межах якої ваги локальних моделей оцінюються за їхньою актуальною прогностичною точністю, продемонструвала середнє зниження середньоквадратичної та середньої абсолютної відсоткової помилки на 19% порівняно з базовими підходами федеративного навчання, що підтверджує доцільність і практичну ефективність розробленого методу для індустріальних систем автоматизованого управління.

РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ ІНДУСТРІАЛЬНОЮ ІНФРАСТРУКТУРОЮ

Для експериментального впровадження розробленої системи використано програмно-апаратні засоби Jetson Nano, які встановлені безпосередньо на автономному транспортному засобі (AGV). Цей модуль забезпечує безперервний збір телеметрії та її попередню обробку у режимі реального часу. Отримані часові ряди слугували основою для тренування моделей шляхом федеративного навчання, зокрема для оцінювання миттєвого енергоспоживання. У ході дослідження оцінювались енергоспоживання та використання обчислювальних ресурсів програмно-апаратних пристроїв Jetson Nano у двох сценаріях: із використанням федеративного навчання та без нього.

AGV відрізняються за конструктивним виконанням і функціональним призначенням, проте їх об’єднує спільна мета автоматизованого переміщення вантажів на виробничих і складських ділянках. Перед детальним аналізом запропонованого підходу наведемо інформацію про структурно-функціональну модель інтелектуальної інформаційно-комунікаційної системи.

4.1 Структурно-функціональна модель інтелектуальної інформаційно-комунікаційної системи для автоматизованого управління інфраструктурою

У сучасних умовах цифровізації виробничих процесів індустріальні підприємства стикаються з проблемою координації великої кількості різнорідних кібер-фізичних підсистем, що функціонують у режимі реального часу. Відсутність єдиної інформаційно-комунікаційної платформи ускладнює наскрізне управління технічними та технологічними ресурсами, призводить до невиправданого резервування потужностей і збільшує операційні витрати [103]. Тому нагальною є потреба у формуванні цілісної структурно-функціональної моделі інтелектуальної системи, здатної автоматизовано керувати динамікою

індустріальної інфраструктури, спираючись на розроблені методи федеративного навчання та гібридні хмарно-граничні обчислення.

Запропонована структурно-функціональна модель інтелектуальної інформаційно-комунікаційної системи (ІІКС) для автоматизованого управління індустріальною інфраструктурою будується за принципом мультиплощинної організації, яка вже продемонструвала свою ефективність у різних застосуваннях (рис. 4.1). Модель включає площину сенсорних та виконавчих пристроїв, площину цифрових двійників із функціями розподіленої аналітики периферійних пристроїв та площини інтелектуального управління, де здійснюється агрегація та навчання алгоритмів. Кожна з площин виконує специфічні функції, але взаємодіє через стандартизовані інтерфейси типу «запит/відповідь» або «підписка/сповіщення», що забезпечує модульність і масштабованість системи.

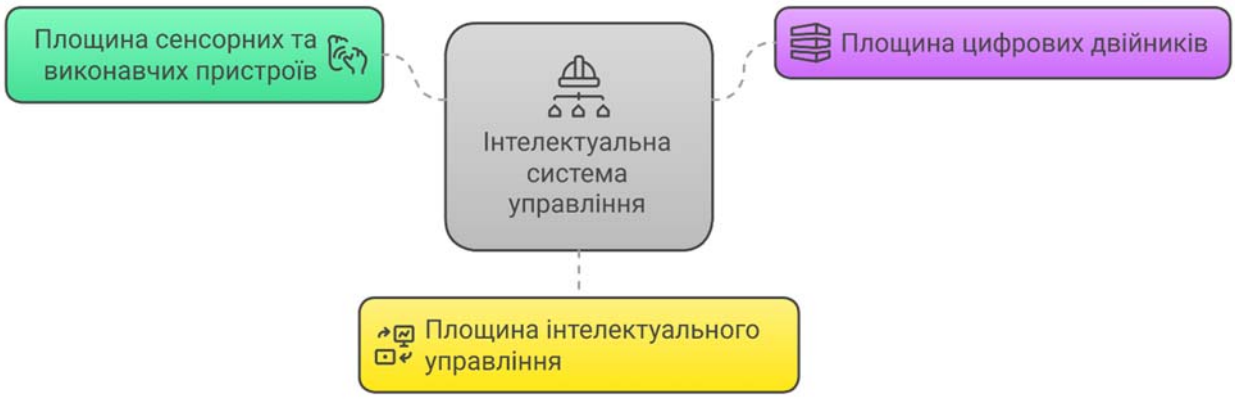


Рисунок 4.1. Загальна архітектура інтелектуальної інформаційно-комунікаційної системи.

Методологічно модель ґрунтується на принципі поетапного структурно-функціонального синтезу, який передбачає послідовне виділення базових елементів інфраструктури, визначення їх функціональних зв’язків і формалізацію потоків даних між ними. Слід наголосити, що інтеграція інтелектуальних функцій управління в ІІКС відбувається з урахуванням двох взаємодоповнювальних стратегій. По-перше, реалізується локальна адаптація на рівні периферійних обчислювальних вузлів, що мінімізує час реакції на

критичні події у виробничому середовищі. По-друге, глобальна оптимізація здійснюється у хмарному домені, де акумулюються історичні дані для тренування глибоких моделей прогнозування попиту на ресурси та раннього виявлення аномалій (рис. 4.2). Завдяки такому дворівневому механізму досягається баланс між обчислювальною складністю й вимогами до затримки, що є ключовим для критично важливих процесів індустрії 4.0/5.0.

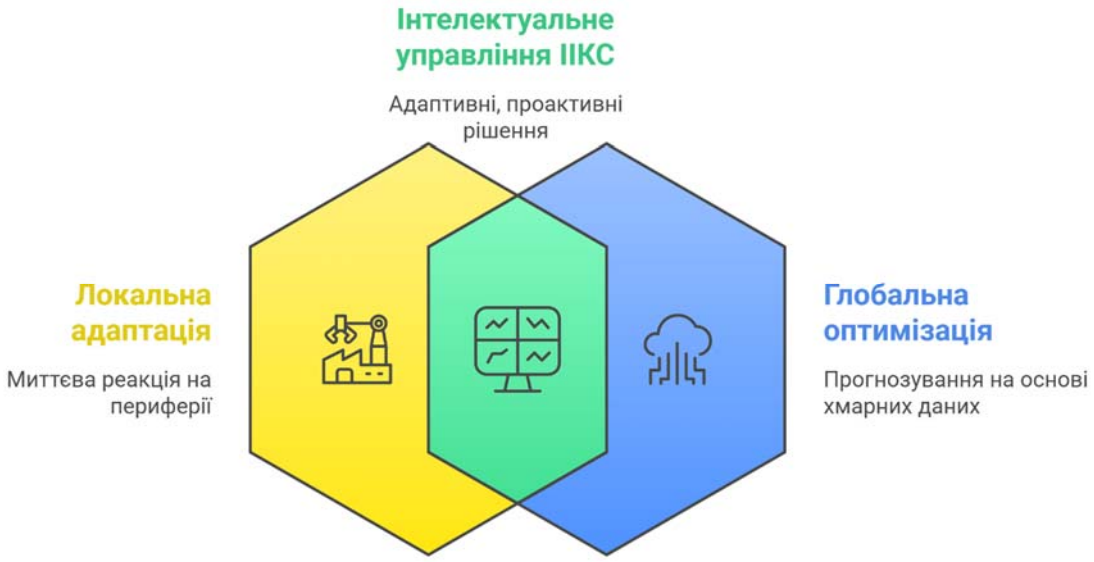


Рисунок 4.2. Ілюстрація принципу взаємодоповнення інтелектуальних функцій управління в ІІКС на локальному та глобальному рівні.

Інтеграція структурно-функціональної моделі інтелектуальної інформаційно-комунікаційної системи з хмарною платформою доцільна передусім тому, що вона формує безперервний контур передавання даних, аналітики та управління, що дає змогу системі самонавчатися на основі реальної експлуатаційної інформації та оперативно адаптувати параметри індустріальної інфраструктури, із використанням алгоритмів федеративного навчання.

Централізоване промислове сховище даних слугує базовою точкою конвергенції різнорідних потоків, що надходять із сенсорної та виконавчої площин моделі. Збереження фактичних даних у хмарному середовищі зводить до мінімуму витрати на масштабування й водночас формує історичну базу, необхідну для глибинного аналізу та ретроспективного валідування прогнозів.

На мережному рівні між периферійними вузлами і хмарою гарантія надійної доставки повідомлень, взаємна аутентифікація пристроїв та прозора маршрутизація є необхідною складовою системи. Підтримка протоколів MQTT, HTTP та CoAP забезпечує уніфікований канал для вузлів з різними обчислювальними можливостями та рівнем енергоспоживання, що особливо важливо для масових mMTC-сценаріїв.

У запропонованій архітектурі ІІКС кожен периферійний вузол тренує локальні ваги на своїх вибірках, після чого агрегований у хмарі «м'який» градієнт синтезує узагальнений алгоритм, що враховує регіональну специфіку, але не вимагає передавання конфіденційних вимірювань. Такий підхід зменшує навантаження на канал зворотного зв'язку та відповідає вимогам нормативів щодо приватності виробничих даних, водночас зберігаючи сталість процесу самовдосконалення когнітивної площини системи.

4.2 Структурно-функціональна модель інтелектуального автономного мобільного робота Formica-1

Платформу Formica-1 створено фахівцями компанії AIUT у співпраці з Сілезьким технологічним університетом у Глівіце та Національним університетом «Львівська політехніка». Метою розроблення було отримання універсального мобільного робота, здатного виконувати операції внутрішнього транспортування в умовах гнучкого виробництва та складської логістики (рис. 4.3). В основі лежить сталеве шасі з модульною посадковою рамою, що дає змогу швидко адаптувати візок під різні сценарії експлуатації. Базова конфігурація підтримує два режими роботи. Перший передбачає переміщення пасивних платформ із застосуванням телескопічних штифтів для підхоплення та утримання візка. Другий режим реалізується шляхом установлення підйомної плити на верхню кришку корпусу, що перетворює робота на самохідний підйомник для перевезення штучних вантажів.

Власна маса конструкції становить приблизно двісті п'ятдесят кілограмів, при цьому граничне корисне навантаження досягає однієї тонни. Приводна

система побудована за схемою електричного диференціального керування з двома тяговими двигунами змінного струму на передній осі та пасивними колесами заднього обертання, що забезпечує мінімальний радіус розвороту менший ніж півтора метра. Енергооснащення складається з тягового акумуляторного модуля, ідентичного за типорозміром батареям міських електробусів. Ємності достатньо для не менше ніж восьми годин безперервного циклу роботи за номінального навантаження. Вбудований блок керування акумулятором реалізує балансування комірок, температурний моніторинг та багаторівневе відсіювання при перевантаженні.

Набір сенсорів включає лідара на триста шістдесят градусів, інерціально-навігаційний модуль з гіроскопом та акселерометром, енкодери коліс, оптичні маркери позиціювання та безконтактні температурні давачі підшипників. Для аналізу електричних параметрів встановлено шунтові датчики струму та високо-швидкісні перетворювачі напруги. Основні обчислення виконує модуль Jetson Nano з чотирьохядерним процесором ARM Cortex-A57 і графічним прискорювачем Maxwell, на якому розгорнуто набір програмного забезпечення реального часу, що включає середовище ROS 2, бібліотеку керування силовою електронікою і контейнерний сервіс для задач машинного навчання. Канальні інтерфейси представлені двома адаптерами Wi-Fi 6 і резервною шиною EtherCAT, які забезпечують інтеграцію в заводську мережеву інфраструктуру та можливість участі у федеративних обчисленнях безпосередньо на борту пристрою [104]. Система безпеки реалізує багаторівневе апаратно-програмне блокування. До неї належать лазерні сканери з функцією динамічних захисних полів, інтенсивний звуковий майор, світлова індикація напрямку руху та трьохконтурний аварійний вимикач живлення.

Комплексна апаратна конфігурація Formica-1 у поєднанні з відкритою архітектурою керування робить платформу придатною для впровадження запропонованої інтелектуальної інформаційно-комунікаційної системи. Високі резерви вантажопідйомності, достатня енергоємність та розширений сенсорний пакет дають змогу виконувати повноцінний збір даних, реалізовувати локальні

алгоритми машинного навчання та брати участь у федеративному обміні параметрами без загрози дефіциту обчислювальних чи енергетичних ресурсів.

Рисунок 4.3. Зображення Formica-1, AGV, який є джерелом даних для експериментів

Прогностичну модель енергоспоживання було розгорнуто безпосередньо на обчислювальному модулі Jetson Nano, установленому на платформі Formica-1 (рис. 4.4). Уся телеметрія надходила у внутрішню пам’ять пристрою, де проходила передоброблення та використання для локального тренування рекурентної нейронної мережі типу LSTM. Завдяки такій організації дані не покидали бортові обчислювальні потужності, що забезпечувало конфіденційність і знижувало мережеві витрати. Для оцінювання потенційних переваг федеративного підходу використовували одну й ту саму вибірку телеметрії з Formica-1, проте варіювали спосіб її розподілу та кількість раундів синхронізації моделей.

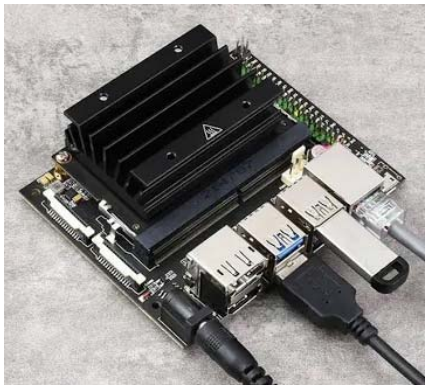


Рисунок 4.4. Периферійний пристрій NVIDIA Jetson Nano, який встановлений на Formica-1 AGV.

Для дослідженнях розроблено модель двох відокремлених виробничих майданчиків, кожен із яких експлуатує власний парк автономних транспортних засобів. Функціонування AGV у такому сценарії передбачає постійну взаємодію із системою диспетчеризації транспорту, системою керування виробництвом, підсистемою складського обліку, а також із широким спектром польових пристроїв, що безпосередньо контролюють технологічні операції. Гетерогенність інформаційних потоків і різнорідність протоколів обміну зумовили використання сервера OPC UA як універсального посередника, здатного конвертувати сигнали від програмованих логічних контролерів, датчиків наближення та виконавчих механізмів у стандартизований формат, придатний для подальшої аналітики в режимі реального часу.

З метою безпосереднього підключення AGV до цієї сервісної інфраструктури розроблено спеціалізований OPC UA-клієнт, інтегрований до периферійного модуля даних (рис. 4.5). Модуль інстальовано на окремому обчислювальному вузлі, розташованому безпосередньо на шасі транспортного засобу, що мінімізує затримку при обробці критичних телеметричних подій. Клієнт контролює життєвий цикл підписки на вузли інформаційної моделі OPC UA, виконує попередню фільтрацію та нормалізацію вибірок, агрегує їх у часові вікна фіксованої довжини й зберігає у локальній базі даних, забезпечуючи таким чином повноцінний буфер для сценаріїв відкладеного навчання.

На верхньому рівні ієрархії результати попередньої обробки передаються через IoT Hub до хмарного Data Lake, де формуються цільові набори для глобальної аналітики. Вибір моделі федеративного навчання обґрунтовується необхідністю враховувати технологічну специфіку кожного майданчика без розкриття чутливих операційних даних. Кожен периферійний модуль тренує локальні ваги прогнозних мереж на основі власних телеметричних послідовностей, після чого агреговані у хмарі градієнти формують узагальнений параметричний простір, релевантний одразу для обох підприємств. Отримана глобальна модель повертається на периферію тим

самим каналом IoT Hub і коригує алгоритми маршрутного планування, контроль енергоспоживання та політику профілактичного обслуговування.

Таким чином, OPC UA-клієнт слугує ключовою ланкою, що замикає сенсорну площину структурно-функціональної моделі із когнітивною, забезпечуючи безперервний потік даних для федеративного навчання. Синергетична взаємодія периферійного модуля, IoT Hub, Data Lake та Cloud Federated Learning створює адаптивний контур управління, у якому кожна нова телеметрична подія підвищує точність прогнозних алгоритмів, а відтак сприяє зменшенню часу простою, оптимізації використання ресурсів і підвищенню економічної ефективності інтегрованої індустріальної інфраструктури [105, 106].

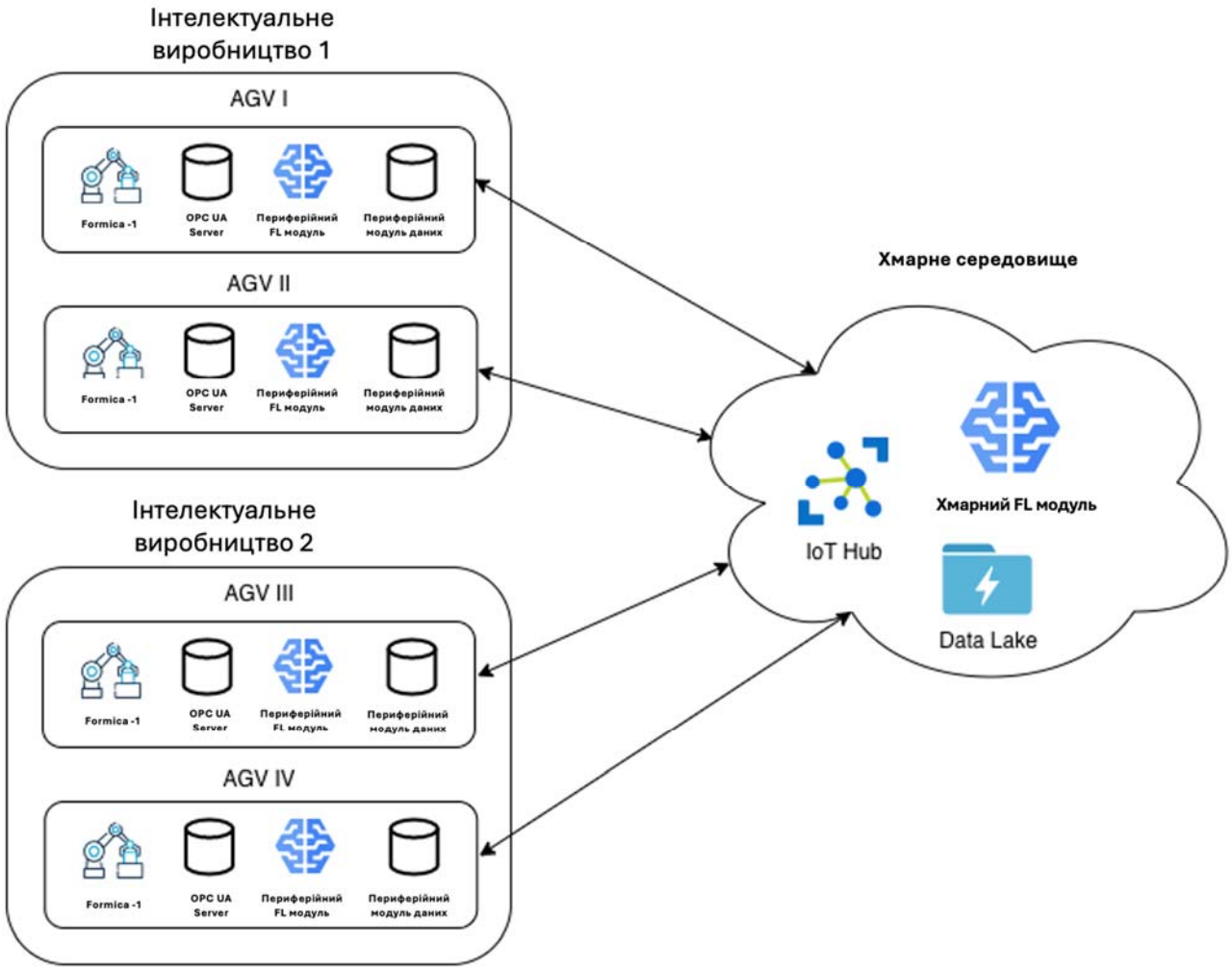


Рисунок 4.5. Концептуальна діаграма розробленої моделі обміну даними в інтелектуальній інформаційно-комунікаційній системі автоматизованого управління [107].

Надалі необхідна інформація, включно з параметрами локальних моделей прогнозування, сформованих на основі даних з AGV, передається до хмарного середовища для довготривалого зберігання та подальшої обробки (наприклад, побудови глобальної моделі). Локально накопичені дані також використовуються для навчання моделей безпосередньо на периферійному пристрої, закріпленому на AGV.

4.3 Реалізація процесу збору даних з автономно керованих пристроїв розумного виробництва.

У межах експериментальної частини дослідження було сформовано репрезентативний масив телеметричної інформації, що надходила від автономних транспортних засобів під час їх роботи у виробничому середовищі [108, 109, 110]. З метою полегшення подальшого аналізу ця інформація була систематизована за змістом і функціональним призначенням окремих повідомлень. До першої групи віднесено сигнали вимірювання енергії, які фіксують миттєве споживання (MEC) у ватах і напругу акумуляторної батареї в мілівольтах; при цьому вимірювання виконуються без поділу на складники, пов’язані із силовими двигунами та бортовою електронікою. Друга група характеризує стан приводів: для лівого та правого двигунів знімаються логічні ознаки їхньої активності та способу активації. Третю групу становить одометрія—числові значення імпульсних частот енкодерів і накопичені пройдені відстані для кожного колеса. Четверту групу утворюють сигнали гальмування, які відображають поточний стан гальмівної системи та метод її ініціювання. П’ята група описує механізми роботи з корисним вантажем, зокрема логічні стани штифтів або підйомної плити залежно від конструкції навантажувального модуля. До шостої групи увійшли сигнали, що фіксують активність окремих світлодіодних стрічок індикації. Сьому групу сформовано навігаційними та шляховими параметрами: координатами, напрямком руху, швидкістю, показником достовірності позиціювання й ідентифікатором сегмента траєкторії. Восьму і дев’яту групи становлять, відповідно, тривожні

повідомлення про збої та попередження щодо потенційно небезпечних ситуацій, а також сигнали безпеки, що реєструють втручання у зони охорони.

Для перевірки придатності підходу федеративного навчання до прогнозування споживання енергії AGV було виконано дев’ять тестових заїздів, середня довжина кожного з яких становила приблизно 1600 дискретних значень за частоти вибірки 1 Гц; загалом сформовано близько 14 тис. часових позначок. Траєкторії описували повторювані кругові рухи діаметром два метри з орієнтацією «за» та «проти» годинникової стрілки при швидкості 0,25 м·с$^{-1}$, а також прямолінійні проходи «туди-назад» зі швидкістю 0,2 м·с$^{-1}$, переривчасті цикли екстреного гальмування й швидкого розгону в обох напрямках. Кожен сценарій реалізовувався як на порожньому транспортному засобі, так і при напівзавантаженому відсіку корисного вантажу (425 кг), оскільки сумарна маса AGV позитивно корелює зі споживанням енергії і має бути врахована під час побудови прогнозної моделі. Послідовності не розділялися на окремі цикли, що забезпечило навчання моделі на даних, отриманих за різних експлуатаційних умов і рівнів завантаження. Кожна вибірка містила понад сорок ознак, проте дослідження зосереджене на прогнозуванні миттєвого споживання енергії МЕС; ілюстративний фрагмент відповідного часового ряду представлено на рисунку 4.6.

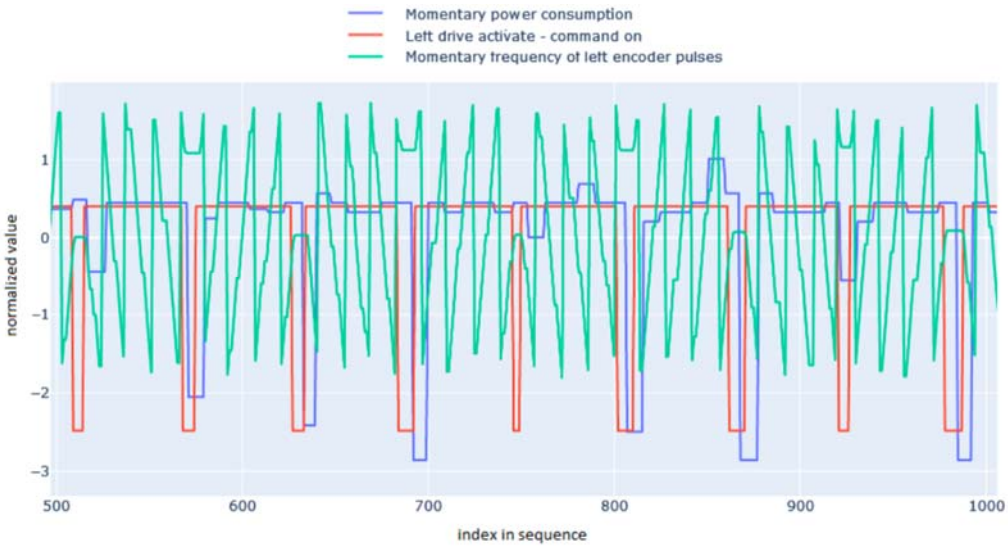


Рисунок 4.6. Фрагмент часового ряду з набору даних, що відображає миттєве споживання/потужності (МЕС), команду активації лівого приводу та миттєву частоту імпульсів лівого енкодера.

З урахуванням зазначеної різноманітності даних і динамічних характеристик руху, сформований датасет є достатньо багатим для оцінювання ефективності федеративного підходу та подальшого вдосконалення енергетичних стратегій AGV у межах запропонованої структурно-функціональної моделі [111].

4.4. Експериментальні дослідження енергоспоживання на периферійному пристрої AGV при різних сценаріях федеративного навчання

Порівняння трьох сценаріїв дає змогу кількісно оцінити додаткові витрати ресурсів, пов’язані з пакуванням і передаванням градієнтних оновлень, а також виявити компроміс між кількістю раундів, обсягом даних у кожному з них і питомим енергоспоживанням під час тренування моделі прогнозування миттєвого енергоспоживання автономного робота.

1. Використання моделі прогнозування миттєвого споживання енергії, навченої у рамках 1-раундного федеративного навчання (1-R FL) на трьох пристроях Jetson Nano. Кожен пристрій зібрав 4000 вибірок (п. 4.4.1).
2. Застосування моделі LSTM, навченої у рамках 4-раундного федеративного навчання (4-R FL) на трьох пристроях Jetson Nano. Кожен пристрій зібрав 4 000 вибірок, розподілених на 4 раунди навчання, по 1000 вибірок у кожному раунді (п. 4.4.2).
3. Застосування моделі LSTM, навченої у рамках 8-раундного федеративного навчання (8-R FL) на трьох пристроях Jetson Nano. Кожен пристрій зібрав 4 000 вибірок, розподілених на 8 раундів навчання, по 500 вибірок у кожному раунді (п. 4.4.3).

Таким чином, було проаналізовано, яку необхідну кількість ресурсів Jetson Nano потрібно для навчання моделі прогнозування без федеративного навчання, а також під час одного раунду 4-R FL та одного раунду 8-R FL. Для визначення споживання ресурсів при навчанні рекурентної нейронної мережі

використовувалася бібліотека Python jetson stats. В усіх розглянутих експериментах Jetson Nano працював у режимі максимальної продуктивності.

4.4.1 Оцінка енергоспоживання при використанні LSTM у межах 1-раундового федеративного навчання

У першій серії експериментів було проведено оцінку обсягів ресурсів, які споживає edge-пристрій за відсутності використання багатораундового федеративного навчання. Середнє споживання ресурсів під час навчання на цьому наборі даних зображено на рисунку 4.7.

Навчання тривало 532 секунди. Всі чотири процесори пристрою Jetson Nano були завантажені на 45%. Крім того, було використано 1,0 ГБ оперативної пам’яті, а миттєве енергоспоживання під час експерименту становило 5 053 мВт, що еквівалентно загальному енергоспоживанню в 8034 Дж під час навчання.

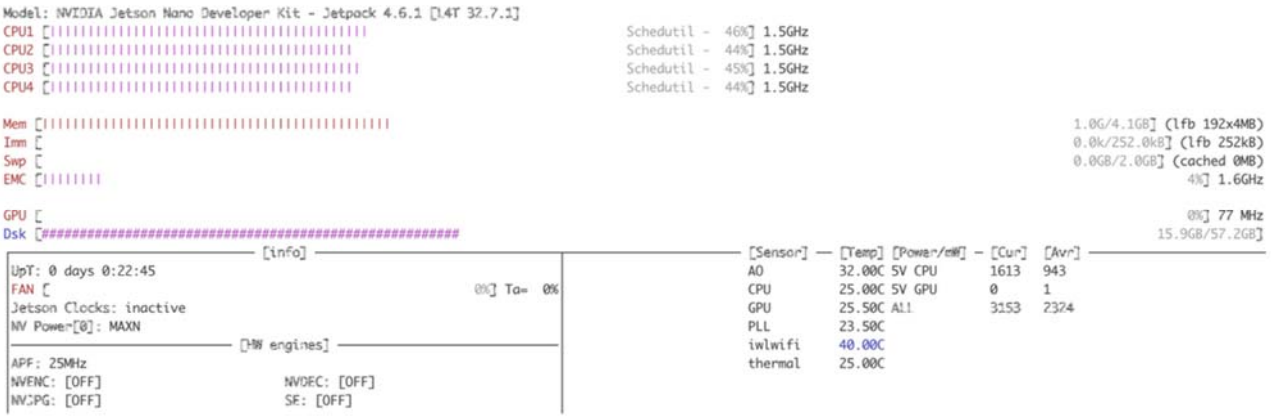


Рисунок 4.7. Споживання ресурсів периферійного пристрою під час навчання моделі прогнозування миттєвого споживання енергії при одноетапному навчанні.

4.4.2 Оцінка енергоспоживання при використанні LSTM у межах 4-раундового федеративного навчання

У цій серії експериментів було розгорнуто федеративне навчання на трьох edge-пристроях. Кожен пристрій виконував чотири раунди навчання у форматі 4-R FL з метою побудови глобальної моделі прогнозування миттєвого енергоспоживання (MEC) та обміну ваговими коефіцієнтами між пристроями.

Це означає, що кожен пристрій збирав 1 000 зразків за раунд (загалом 12 000 зразків для чотирьох раундів навчання). У цьому випадку було зафіксовано, скільки ресурсів споживав edge-пристрій під час навчання моделі прогнозування МЕС на 1 000 зразках (в межах одного раунду). Середнє споживання ресурсів під час такого навчання зображено на рисунку 4.8.

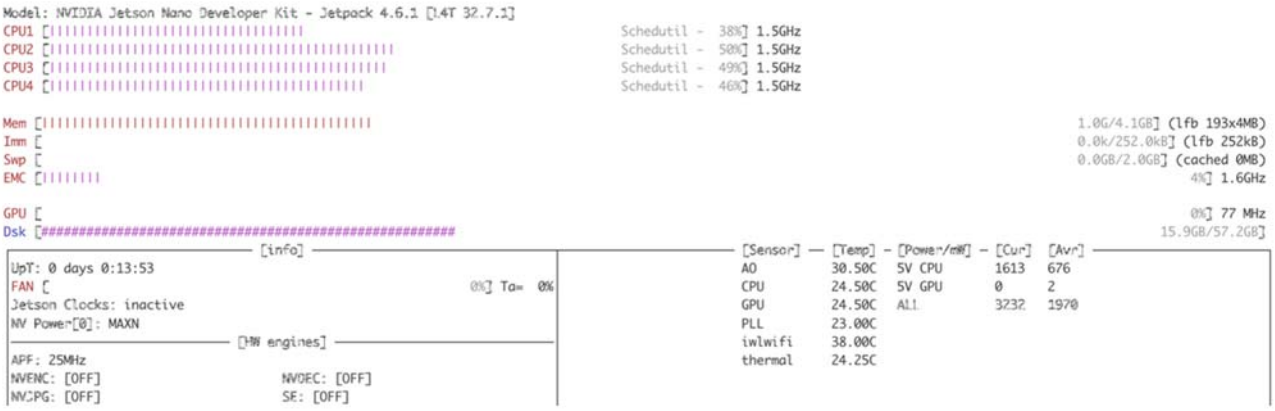


Рисунок 4.8 Споживання ресурсів периферійного пристрою під час навчання моделі прогнозування миттєвого споживання енергії у 4-раундному федеративному навчанні.

Навчання в межах одного раунду тривало 133 секунди. Всі чотири процесори Jetson Nano були завантажені на 46%. Було використано 1 ГБ оперативної пам’яті, а миттєве енергоспоживання під час експерименту становило 3 232 мВт, що еквівалентно загальному енергоспоживанню 5 158 Дж за час навчання. Загалом споживання ресурсів майже не відрізнялось від навчання без використання федеративного підходу, однак у цьому випадку ці ресурси було розподілено між трьома пристроями.

4.4.3 Оцінка енергоспоживання при використанні LSTM у межах 8-раундового федеративного навчання

У цій серії експериментів три граничні пристрої збирали по 500 зразків за кожен раунд (усього 12 000 зразків для 8 раундів навчання). Середні витрати ресурсів під час одного раунду навчання на цьому наборі даних показано на рисунку 4.9.

Час навчання склав 66 секунд, усі чотири процесори Jetson Nano у середньому були завантажені на 44%. Крім того, використовувалося 1 ГБ оперативної пам’яті, а миттєве споживання потужності під час експерименту становило 2 570 мВт, що еквівалентно 4 070 Дж загального споживання енергії під час навчання.

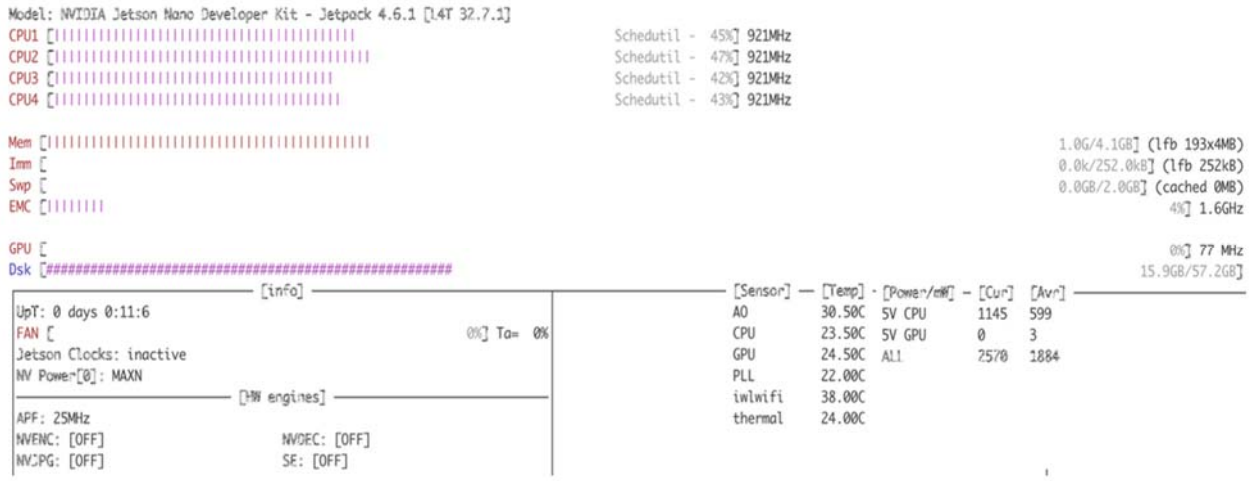


Рисунок 4.9. Споживання ресурсів периферійного пристрою під час навчання моделі прогнозування миттєвого споживання енергії у межах 8 раундів федеративного навчання.

У цьому сценарії ми зафіксували нижче енергоспоживання та помітили, що процесори працюють на нижчих частотах, що, на нашу думку, пов’язано зі зниженим енергоспоживанням. Отримані результати зображені в Таблиці 4.1 свідчать про те, що варіант з 8 раундами федеративного навчання споживав найменше ресурсів граничного пристрою. Крім того, саме цей підхід дозволив досягти найкращої точності прогнозування, що відповідає результатам, наведеними в [112]

Час навчання, завантаження процесора, використання оперативної пам’яті та споживання енергії IoT-пристроями - це критично важливі показники ефективності при побудові моделей прогнозування, що функціонують безпосередньо на бортових системах автономних мобільних роботів. Ці показники безпосередньо впливають на споживання енергії з батарей AGV, а отже, і на їхню здатність ефективно функціонувати. Саме тому в цьому

підрозділі проведено аналіз, як ці ресурси споживаються під час локального навчання нейронної мережі.

Таблиця 4.1. Споживання ресурсів для кожного з протестованих сценаріїв навчання моделі прогнозування

Підхід	**Час за раунд**	**CPU**	**Миттєве сумарне енергоспоживання**	**Загальне сумарне енергоспоживання**
1-раунд FL	532 сек	45%	5,053 мВт	8,034 Дж
4-раунди FL	133 сек	46%	3,232 мВт	5,158 Дж
8-раундів FL	66 сек	44%	2,570 мВт	4,070 Дж

Результати експерименту свідчать, що найбільш ефективним та енергоощадним способом навчання нейронних мереж безпосередньо на AGV є використання більшої кількості раундів федеративного навчання. Як показано в Таблиці 4.1, використання 8-раундового навчання дозволяє суттєво заощадити ресурси, зменшити загальне навантаження на пристрій та покращити точність прогнозування сигналу MEC, що є критично важливим для виявлення аномалій в роботі AGV.

Аналіз експериментальних вимірювань демонструє, що варіювання кількості раундів федеративного навчання впливає переважно на миттєву потужність споживання обчислювальних вузлів, тоді як сумарна тривалість тренування лишається майже сталою. Для одноraундового сценарію 1-R FL на одному Jetson Nano зафіксовано миттєву потужність 5,053 мВт, що у випадку трьох пристроїв відповідає 15,16 мВт на кластер. Загальна інтегральна енергія, витрачена на повний цикл обробки 12 000 вибірок (4 000 × 3), становить 8,034 Дж, тобто приблизно 0,67 мДж на одну вибірку для окремого вузла.

Коли партію даних було поділено на чотири раунди, тривалість локального епізоду скоротилася до 133 с, а миттєва потужність знизилася до 3,232 мВт на пристрій, що дає 9,70 мВт на увесь кластер. Внаслідок меншої активності GPU та кеш-оптимізованої обробки параметрів сумарне

енергоспоживання трьох вузлів зменшилося до 5,158 Дж, тобто майже на 36 % порівняно з одноraундовим навчанням. Відносна економія на рівні однієї вибірки зросла до 0,43 мДж.

Подальше дроблення вибірки до восьми раундів дало найнижчу миттєву потужність - 2,570 мВт на вузол (7,71 мВт для кластера). Сукупна енергія, необхідна для навчання тієї ж самої моделі, становить 4,070 Дж, що відповідає додатковому скороченню ще майже на 13 % проти чотирираундового сценарію й на 49 % проти 1-R FL. Споживання енергії на одну вибірку зменшилася до 0,34 мДж, тобто удвічі нижче еталону.

Показник завантаження CPU тримався у межах 44–46 %, тому головною причиною різниці у потужності є скорочення активної фази GPU та пам’яті при обробці менших партій, а також відносно низький внесок мережевого інтерфейсу, що, за даними попередніх експериментів, додає менш ніж один відсоток до енергобалансу. Тривалість одного раунду зменшується пропорційно розміру партії (532, 133 і 66 с), але добуток «час × кількість раундів» залишається практично незмінним (≈ 530 с), тому поліпшення енергоефективності досягається не завдяки скороченню загального часу роботи, а за рахунок нижчої миттєвої потужності.

Отримані результати свідчать, що з погляду питомих енергетичних витрат найвигіднішою є конфігурація з вісьмома раундами: вона майже вдвічі економніша за одноraундовий підхід і на третину випереджає чотирираундовий. Водночас потрібно враховувати збільшення мережевого трафіку для агрегації градієнтів, яке у разі малосмугових бездротових каналів може стати обмежувальним фактором. За наявності достатньої пропускної здатності й зацікавленості в мінімізації теплового навантаження 8-R FL є оптимальним; якщо ж канал є вузьким або потрібна висока швидкість адаптації моделі, виправданим компромісом може стати чотирираундовий режим, що забезпечує помітну економію енергії й не створює надмірного трафіку.

Подальше збільшення кількості раундів, теоретично може дати ще більший виграш з точки зору енергоспоживання. Однак, при надто малому

розмірі навчальної вибірки в одному раунді, точність моделей починає знижуватись.

4.5 Моделі та архітектури розгортання федеративного навчання в індустріальних інформаційно-комунікаційних системах

Федеративне навчання (FL) створює технологічну основу для впровадження алгоритмів штучного інтелекту у виробниче середовище без передавання первинних даних за межі їхнього фізичного джерела. Така властивість особливо цінна в умовах «розумного» виробництва, де одночасно діють вимоги до неухильного дотримання конфіденційності, гарантованої пропускної здатності каналів та мінімальної затримки циклу «вимірювання-прогноз-керування». У запропонованій структурно-функціональній моделі інтелектуальної інформаційно-комунікаційної системи (ІІКС) FL інтегрується на рівні когнітивної площини, замикаючи контур даних між сенсорними вузлами AGV, edge-обчисленнями та хмарним доменом. З огляду на топологію промислової мережі, кількість вузлів і характер технологічних процесів, виокремлено дві базові архітектури, релевантні для різних сценаріїв експлуатації.

4.5.1 Локалізоване федеративне навчання на виробничих серверах

У першій архітектурі кожна виробнича лінія оснащується власним серверним сегментом, до якого надходить сировинна телеметрія від усіх AGV і сенсорів, що обслуговують відповідний технологічний контур (рис. 4.10). Локальний сервер виконує повний цикл обробки: фільтрацію потоків OPC UA, нормалізацію вибірок, формування навчальних вибірок і тренування спеціалізованої нейронної мережі прогнозування енергоспоживання та технічного стану. Після завершення чергової епохи на верхній рівень передається лише вектор ваг, ущільнений до формату 32-бітних коефіцієнтів. У хмарному центрі ці ваги агрегуються алгоритмом усереднення утворюючи глобальну модель, що акумулює інформацію всіх виробничих ліній. Оновлений

набір параметрів повертається на локальні сервери, де він негайно використовується для прогнозу та наступного раунду локального донавчання.

Такий підхід мінімізує капітальні витрати: відсутня потреба встановлювати на кожен AGV окремий edge-комп'ютер із GPU для машинного навчання, а масштабування розв'язується додаванням стандартних серверів у машинних залах. Крім економічної привабливості, архітектура забезпечує високу точність прогнозу для відносно статичних виробничих ліній, оскільки локальна модель навчається на конгруентних даних з однорідними режимами навантаження. Ризики втрати конфіденційності залишаються контрольованими: сирі дані ніколи не залишають меж цеху, а з хмарою циркулюють лише параметри моделі з математично нівельованими слідами вихідних вибірок. Негативним чинником є додаткова латентність, спричинена транспортуванням потоків від AGV до локального сервера, що може обмежити застосування у сценаріях з жорсткими вимогами до затримки менше 1 мілісекунди.

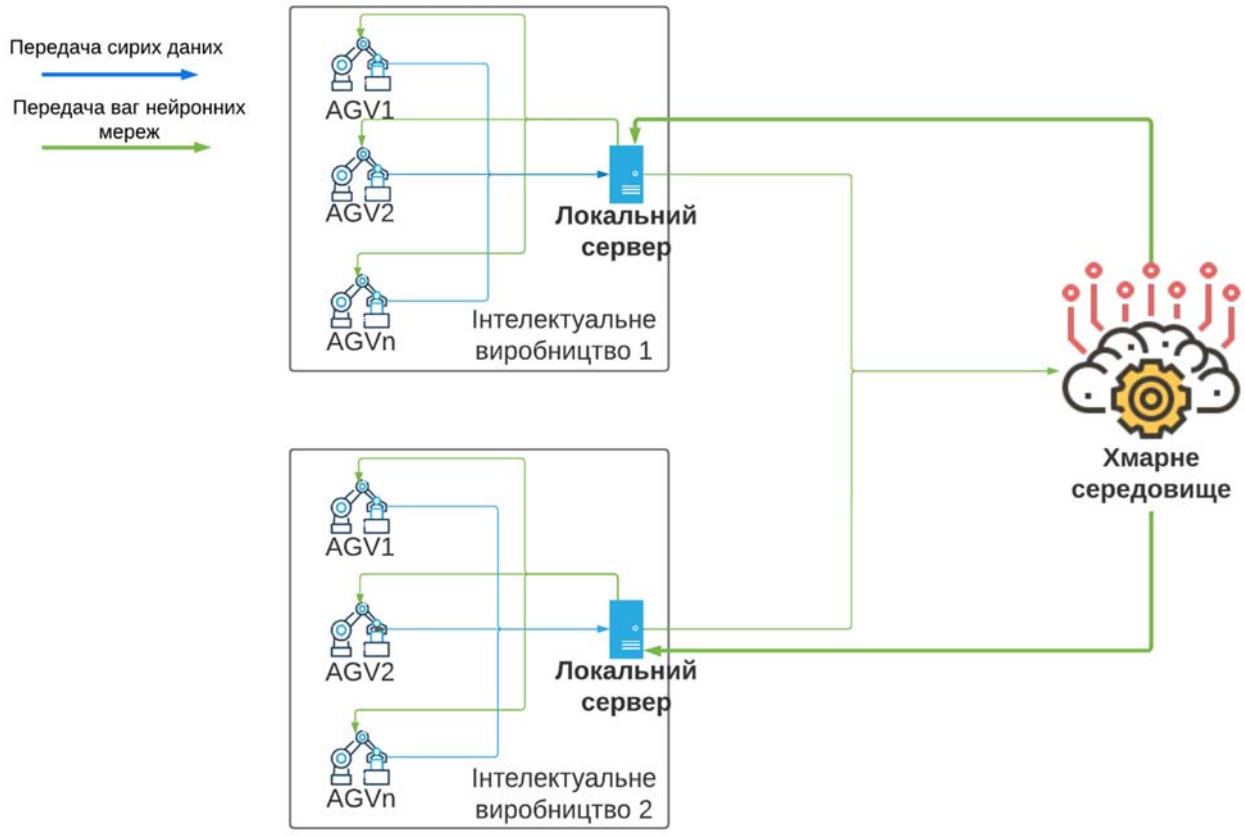


Рисунок 4.10. Архітектура федеративного навчання на локальних серверах.

4.5.2 Граничне федеративне навчання безпосередньо на AGV-пристроях

Друга архітектура переносить усі обчислення першої фази FL безпосередньо на рухомих платформах AGV (рис. 4.11). Кожен транспортний засіб оснащено компактним вузлом типу Jetson Nano, на якому працює OPC UA-клієнт, модуль попередньої обробки та локальна LSTM-мережа. Після накопичення заданої партії даних відбувається градієнтне оновлення ваг, а самі ваги через IoT Hub передаються до хмари. На рівні глобального агрегатора формується інтегрована модель, що відображає досвід експлуатації усіх AGV незалежно від їхніх маршрутових і вантажних профілів. Через той самий канал IoT Hub нові параметри розповсюджуються назад на пристрої і одразу залучаються до реального-часового оцінювання аномалій та корекції навігаційних траєкторій.

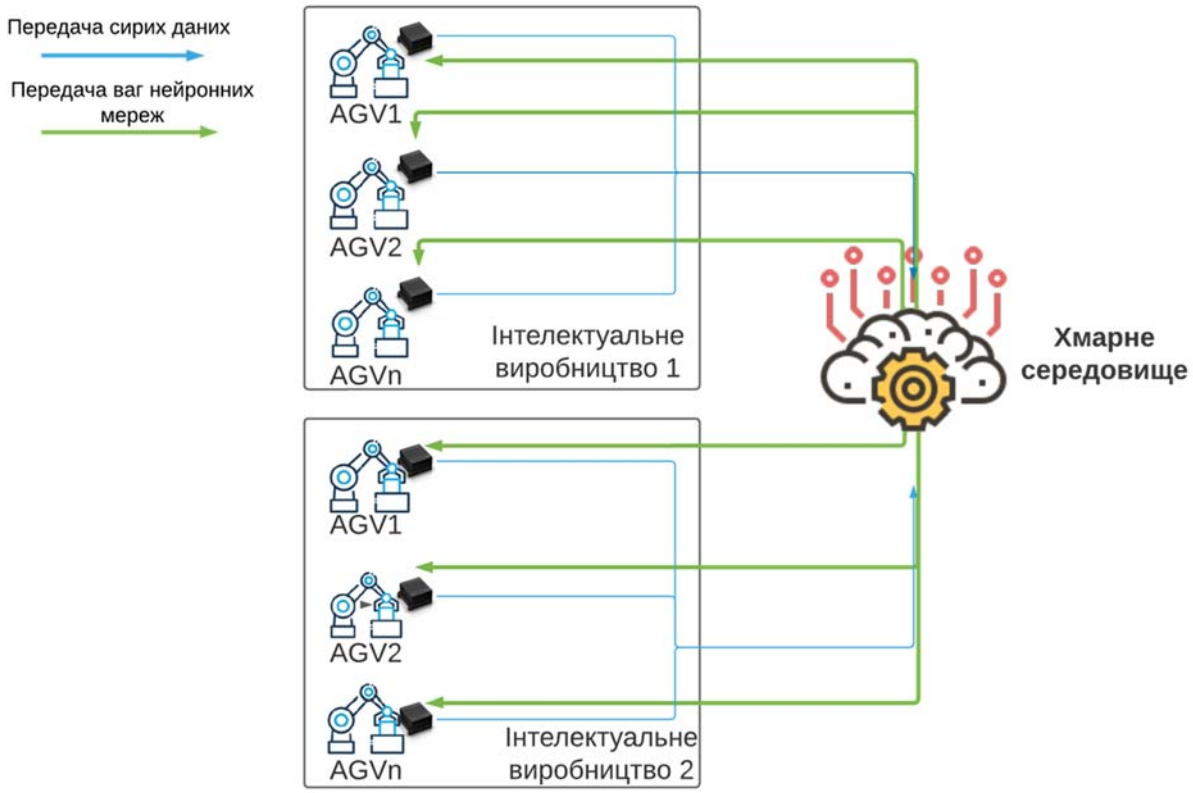


Рисунок 4.11. Архітектура федеративного навчання безпосередньо на граничних вузлах.

Ключова перевага граничної схеми полягає у максимальному ступені приватності: сирі телеметричні ряди ніколи не полишають бортовий комп’ютер, а тому ризик витоку даних про процеси й топологію підприємства прямує до нуля. Додатково скорочується сумарний обсяг трафіку, оскільки передаються тільки стиснені тензори ваг замість мегабайтів сенсорних вимірювань. Розміщення алгоритму прогнозування «біля сенсора» зменшує затримку виявлення відмов, що критично для систем безпеки й узгоджується з принципами граничних обчислень MEC, інтегрованих у транспортну площину ІІКС. Водночас такий підхід вимагає більших інвестицій у кожне AGV, а обмеження енергоспоживання та дисипації тепла на мобільному обчислювачі накладають суворі обмеження на складність нейронної моделі.

4.5.3 Порівняльний аналіз та критерії вибору архітектур федеративного навчання

Поглиблений аналіз чинників вибору архітектури федеративного навчання ґрунтується на взаємодії технологічних вимог виробничого процесу та економічних обмежень життєвого циклу ІІКС. Передусім слід ураховувати часові характеристики керування: для стаціонарних технологічних ліній із повторюваними режимами обробки матеріалів характерні предиктивні цикли з допуском затримки в десятки або навіть сотні мілісекунд. У таких умовах обчислювальну фазу FL доцільно зосередити на локальному сервері, розташованому всередині виробничого сегмента мережі. Сервер консолідує телеметрію від великої кількості однорідних сенсорів, ефективно використовує багатоядерні CPU та дискретні GPU й мінімізує витрати канального ресурсу, оскільки між периферією та сервером циркулюють необроблені дані лише в межах одного комутаційного домену. При цьому капітальні та операційні витрати залишаються прийнятними: сервісний персонал обслуговує єдину точку обчислень, а подальше масштабування вирішується вертикальним нарощуванням ресурсів серверної платформи.

У мобільних кібер-фізичних системах, до яких належать автономні транспортні роботи, домінують інші пріоритети. Висока варіативність траєкторій, нестаціонарні умови навантаження та вимога негайної реакції на непередбачені події (наприклад, раптову появу перешкоди або деградацію тягових батарей) формують інтервал допустимої затримки в одиниці мілісекунд. Передавання повних потоків телеметрії на віддалений сервер у таких умовах призводить до неприпустимої затримки навіть у провідних мережах Gigabit Ethernet, не кажучи вже про безпровідні канали Wi-Fi 6 або 5G. Тому обчислювальну фазу FL доцільно переносити безпосередньо на бортові вузли AGV, оснащені енергоефективним GPU типу Jetson. Виграш у часі реакції компенсує зростання вартості апаратури, а ризик витоку технологічно чутливих даних істотно знижується, оскільки оригінальні вимірювання ніколи не полишають корпус робота, а в мережі циркулюють лише зашифровані тензори ваг.

У межах запропонованої ІІКС периферійне федеративне навчання прийнято як базовий механізм для автономних транспортних роботів, тоді як локалізоване FL доцільно застосовувати для стаціонарних виробничих ліній із великою кількістю сенсорів, від яких не вимагається миттєве само-налаштування. Комбіноване використання обох архітектур на різних рівнях ієрархії формує гнучку, масштабовану та безпечну екосистему «розумного» виробництва, де кожен інформаційний потік обробляється там, де це найбільш ефективно з погляду часу відгуку, пропускної здатності та енергетичних витрат.

4.6. Висновки до розділу

У розділі реалізовано нову структурно-функціональну модель інтелектуальної інформаційно-комунікаційної системи, що поєднує сенсорну, транспортну, когнітивну та децентралізовану площини й забезпечує наскрізний контур «дані-аналітика-управління» для автономних транспортних роботів та стаціонарних технологічних ліній. На базі цієї моделі впроваджено граничне

федеративне навчання, яке дало змогу здійснювати локальне тренування нейронних мереж без передавання оригінальних даних, зберігаючи конфіденційність і мінімізуючи мережеві витрати.

Експериментальні дослідження з порівняння одноraундної, чотири-раундної та восьми-раундної конфігурацій FL засвідчили чітку залежність енергоефективності від кількості раундів агрегування. Перехід до 4-раундного режиму дав змогу зменшити сукупне споживання енергії на 35,8 %, а 8-раундний режим дав змогу зменшити енергоспоживання на 49,3% порівняно з 1-раундним еталоном, із збереженням точності прогнозування.

Запропонована структурно-функціональна модель у поєднанні з 8-раундним федеративним навчанням забезпечує максимальний виграш в енергоефективності, повну ізоляцію конфіденційних даних та збереження швидкодії, що підтверджує її практичну ефективність для застосування в системах «розумного» виробництва з обмеженими ресурсами периферійних пристроїв та жорсткими вимогами до роботи в реальному часі.

ВИСНОВКИ

На основі проведених теоретичних та експериментальних досліджень у дисертаційній роботі розроблено нові та вдосконалено існуючі методи та моделі федеративного машинного навчання для інформаційно-комунікаційних систем автоматизованого управління, з метою підвищення точності прийняття рішень в умовах неповноти й нестаціонарності даних та обмежених обчислювальних ресурсів кінцевих пристроїв.

1. Проведено аналіз сучасних методів та моделей побудови інформаційно-комунікаційних систем автоматизованого управління індустріальною інфраструктурою з використанням методів штучного інтелекту. Визначено, що перехід від Індустрії 4.0 до Індустрії 5.0 формує нові вимоги до кіберфізичних виробничих та невиробничих комплексів. Це своєю чергою стимулює еволюцію архітектури інформаційно-комунікаційної системи від централізованих хмарних до децентралізованих граничних обчислень. В такому контексті, інтеграція методів федеративного навчання дозволяє зберегти конфіденційність даних і значно знизити обсяг передаваних через мережу даних. Проведено порівняння централізованої, децентралізованої та напівцентралізованої архітектур федеративного навчання та визначено оптимальні варіанти їх розгортання у різних індустріальних середовищах. Як базовий об'єкт дослідження в дисертаційній роботі для інформаційно-комунікаційних систем автоматизованого управління індустріальною інфраструктурою обрано процес горизонтального федеративного навчання. Окреслено основні виклики та обмеження стосовно інтеграції федеративного навчання в індустріальних системах, такі як необхідність залучення великих масивів даних при збереженні конфіденційності, статистична неоднорідність вибірок, обмежені обчислювальні та енергетичні ресурси кінцевих пристроїв.

2. Розроблено структурно-функціональну модель інтелектуальної інформаційно-комунікаційної системи для автоматизованого управління інфраструктурою, яка базується на відокремленні площини пристроїв, площини передавання даних, площини автоматизованої інфраструктури та площини

інтелектуальної обробки даних, які взаємодіють на основі спільного онтологічного ядра. Це дало змогу забезпечити інтероперабельність та обмін знаннями локальних моделей між різними виробничими та невиробничими інфраструктурами в процесі федеративного навчання, завдяки децентралізації ресурсів та стандартизованим інтерфейсам обміну знань між окремими галузями.

3. Удосконалено метод обчислення параметрів агрегованої моделі, шляхом введення додаткового середньозваженого критерію оцінювання ефективності локальних моделей кінцевих пристроїв. Такий підхід дав змогу підвищити ефективність процесу федеративного навчання за рахунок зниження вагомості статистичних викидів та помилок локальних моделей під час обчислення агрегованої моделі.

4. Розроблено метод багатораундного федеративного навчання, який на відміну від відомих, використовує хронологічну стратифікацію навчальної вибірки, з поетапним усередненням агрегованих моделей кожного раунду. Хронологічна стратифікація забезпечує цілісність процесу навчання з точки зору часової динаміки, а також зменшення розміру вибірки для кожного раунду навчання. У сукупності це дало змогу знизити складність обчислень для мобільних кінцевих пристроїв федеративного навчання при збереженні точності результуючої агрегованої моделі, а також забезпечити швидшу адаптацію моделей до динаміки індустріальної системи. Розроблений алгоритм багатораундного федеративного навчання дає змогу знизити похибку прогнозування агрегованих моделей до 10% залежно від від умов функціонування та кількості раундів для навчання.

5. Розроблено алгоритмічно-програмне забезпечення інтелектуальної інформаційно-комунікаційної системи для практичної реалізації розроблених методів федеративного навчання. Зокрема, реалізовано програмно-апаратну модель інтелектуальної інформаційно-комунікаційної системи, яка забезпечує наскрізний контур «дані-аналітика-управління» для автономних транспортних роботів та стаціонарних технологічних ліній. На базі цієї моделі впроваджено

граничне федеративне навчання з використанням розроблених алгоритмів, яке дало змогу здійснювати локальне тренування нейронних мереж без передавання оригінальних даних, зберігаючи конфіденційність і мінімізуючи мережеві витрати.

6. Проведено експериментальні дослідження розроблених методів та моделей для автоматизованого управління інтелектуальними роботизованими системами в реальному індустріальному середовищі. Експериментальні результати показали, що розроблений алгоритм обчислення агрегованих моделей федеративного навчання забезпечує підвищення достовірності прогнозування у задачах регресії, з відповідним зниженням похибки при прогнозуванні енергоспоживання автономних транспортних засобів на 19% при їх функціонуванні у реальному виробничому середовищі. Розроблений алгоритм багатораундного федеративного навчання підвищує енергетичну ефективність процесу федеративного навчання на кінцевих пристроях на 37% при використанні 4 раундів навчання та на 50%, при використанні 8 раундів навчання за умови збереження аналогічної точності прогнозування часових характеристик індустріальної системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. X. Fu, H. Wang, and P. Shi, “A survey of blockchain consensus algorithms: Mechanism, design and applications,” Sci. China Inf. Sci., vol. 64, pp. 1–15, 2021.
2. H. Chen, S. Asif, J. Park, C. Shen, and M. Bennis, “Robust blockchained federated learning with model validation and proof-of-stake inspired consensus.” arXiv preprint arXiv:2101.03300, 2021.
3. K. Toyoda, J. Zhao, A. Zhang, and P. Mathiopoulos, “Blockchain-enabled federated learning with mechanism design,” in IEEE Access, vol. 8, pp. 219744–219756, 2020.
4. S. Pokhrel and J. Choi, “Federated learning with blockchain for autonomous vehicles: Analysis and design challenges,” IEEE Trans. Commun., vol. 68, no. 8, pp. 4734–4746, 2020.
5. R. Kumar, A. Khan, J. Kumar, Zakria, N. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, “Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging,” IEEE Sens. J., vol. 21, no. 14, pp. 16301–16314, 2021.
6. T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” Proceedings of Machine Learning Research, vol. 119, pp. 4292–4304, 2020.
7. M. Hankel and B. Rexroth, “The reference architectural model Industrie 4.0 (RAMI 4.0),” ZVEI, vol. 2, no. 2, pp. 4–9, 2015.
8. K. T. Park, J. Lee, H. J. Kim, and S. D. Noh, “Digital twin-based cyber-physical production system architectural framework for personalized production,” The International Journal of Advanced Manufacturing Technology, vol. 106, pp. 1787–1810, 2020.
9. J. Lee, B. Bagheri, and H.-A. Kao, “A cyber-physical systems architecture for Industry 4.0-based manufacturing systems,” Manufacturing Letters, vol. 3, pp. 18–23, 2015.

10. Z. Du, C. Wu, T. Yoshinaga, K.-L. A. Yau, Y. Ji, and J. Li, “Federated learning for vehicular internet of things: Recent advances and open issues,” IEEE Open Journal of the Computer Society, vol. 1, pp. 45–61, 2020.
11. X. Ouyang, Z. Xie, J. Zhou, G. Xing, and J. Huang, “Clusterfl: a clustering-based federated learning system for human activity recognition,” ACM Transactions on Sensor Networks, vol. 19, no. 1, p. 17, 2023.
12. M. S. H. Abad, E. Ozfatura, D. Gündüz, and O. Ercetin, “Hierarchical federated learning across heterogeneous cellular networks,” in Proceedings of 2020 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 8866–8870, 2020.
13. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, pp. 1273–1282, 2017.
14. S. Truex, L. Liu, K. H. Chow, M. E. Gursoy, and W. Wei, “Ldp-fed: federated learning with local differential privacy,” in Proceedings of the 3rd ACM International Workshop on Edge Systems, Analytics and Networking, pp. 61–66, 2020.
15. Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, “Federated learning,” Synthesis Lectures on Artificial Intelligence and Machine Learning, vol. 13, no. 3, pp. 1–207, 2019.
16. D. Gao, C. Ju, X. Wei, Y. Liu, T. Chen, and Q. Yang, “Hhhfl: Hierarchical heterogeneous horizontal federated learning for electroencephalography,” arXiv preprint arXiv:1909.05784, 2019.
17. T. Wei, Y. Wang, and W. Li, “The deep flow inspection framework based on horizontal federated learning,” in 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1–4, IEEE, 2022.
18. F. Zheng, K. Li, J. Tian, X. Xiang, et al., “A vertical federated learning method for interpretable scorecard and its application in credit scoring,” arXiv preprint arXiv:2009.06218, 2020.

19. Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, “Fedhealth: A federated transfer learning framework for wearable healthcare,” IEEE Intelligent Systems, vol. 35, no. 4, pp. 83–93, 2020.
20. J. Guo, I. W.-H. Ho, Y. Hou, and Z. Li, “Fedpos: A federated transfer learning framework for csi-based wi-fi indoor positioning,” IEEE Systems Journal, 2023.
21. S. Feng and H. Yu, “Multi-participant multi-class vertical federated learning,” arXiv preprint arXiv:2001.11154, 2020.
22. T.-D. Cao, T. Truong-Huu, H. Tran, and K. Tran, “A federated learning framework for privacy-preserving and parallel training,” arXiv preprint arXiv:2001.09782, 2020.
23. S. Rahmadika and K. Rhee, “Blockchain technology for providing an architecture model of decentralized personal health information,” Int. J. Eng. Bus. Manag., vol. 10, pp. 1–9, 2018. Article 1847979018790589.
24. J. Wei, Q. Zhu, Q. Li, L. Nie, Z. Shen, K. Choo, and K. Yu, “A redactable blockchain framework for secure federated learning in industrial internet of things,” IEEE Internet Things J., vol. 9, no. 22, pp. 17901–17911, 2022.
25. P. Zhang, G. Liu, Z. Chen, J. Guo, and P. Liu, “A study of a federated learning framework based on the interstellar file system and blockchain: Private blockchain federated learning,” in 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), (Changchun, China), pp. 267–273, IEEE, 2022.
26. H. Kim, J. Park, M. Bennis, and S. Kim, “Blockchained on-device federated learning,” IEEE Commun. Lett., vol. 24, no. 6, pp. 1279–1283, 2020.
27. M. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, “Towards blockchain-based reputation-aware federated learning,” in IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), (Toronto, ON, Canada), pp. 183–188, IEEE, 2020.

28. P. Corcoran and S. K. Datta, “Mobile-edge computing and the internet of things for consumers: Extending cloud computing and services to the edge of the network,” IEEE Consumer Electronics Magazine, vol. 5, no. 4, pp. 73–74, 2016.
29. M. Chiang and T. Zhang, “Fog and IoT: An overview of research opportunities,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016.
30. N. Agarwal, P. Kairouz, and Z. Liu, “The Skellam mechanism for differentially private federated learning,” pp. 5052–5064, 2021.
31. N. Agarwal, A. T. Suresh, F. Yu, S. Kumar, and H. B. McMahan, “CPSGD: Communication-efficient and differentially-private distributed SGD,” pp. 7575–7586, 2024.
32. A. Triastcyn and B. Faltings, “Federated learning with Bayesian differential privacy,” in Proceedings of 2019 IEEE International Conference on Big Data, pp. 2587–2596, 2019.
33. K. Wei, J. Li, M. Ding, C. Ma, H. Su, B. Zhang, and H. V. Poor, “User-level privacy-preserving federated learning: Analysis and performance optimization,” IEEE Transactions on Mobile Computing, vol. 21, no. 9, pp. 3388–3401, 2022.
34. Erlingsson, V. Pihur, and A. Korolova, “RAPPOR: Randomized aggregatable privacy-preserving ordinal response,” in Proceedings of 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 1054–1067, 2014.
35. A. M. Girgis, D. Data, and S. N. Diggavi, “Renyi differential privacy of the subsampled shuffle model in distributed learning,” in Proceedings of the 35th International Conference on Neural Information Processing Systems, pp. 29181–29192, 2021.
36. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Aguera y Arcas, “Communication-efficient learning of deep networks from decentralized data,” Artificial Intelligence and Statistics, pp. 1273–1282, 2017.
37. Y. Mansour, M. Mohri, J. Ro, and A. T. Suresh, “Three approaches for personalization with applications to federated learning,” arXiv preprint arXiv:2002.10619, 2020.

38. Z. Chai, A. Ali, S. Zawad, S. Truex, A. Anwar, N. Baracaldo, Y. Zhou, H. Ludwig, F. Yan, and Y. Cheng, “TiFL: A tier-based federated learning system,” in Proceedings of the 29th International Symposium on High-Performance Parallel and Distributed Computing, pp. 125–136, 2020.
39. S. Warnat-Herresthal, H. Schultze, K. L. Shastry, S. Manamohan, S. Mukherjee, V. Garg, R. Sarveswara, K. Händler, P. Pickkers, N. A. Aziz, et al., “Swarm learning for decentralized and confidential clinical machine learning,” Nature, vol. 594, no. 7862, pp. 265–270, 2021.
40. H. Kim, J. Park, M. Bennis, and S. L. Kim, “Blockchained on-device federated learning,” IEEE Communications Letters, vol. 24, no. 6, pp. 1279–1283, 2020.
41. P. Mohassel and Y. Zhang, “ SecureML: A system for scalable privacy-preserving machine learning,” in Proceedings of 2017 IEEE Symposium on Security and Privacy, pp. 19–38, 2017.
42. K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, “ Practical secure aggregation for privacy-preserving machine learning,” in Proceedings of 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175–1191, 2017.
43. Y. Liu, Z. Ma, Z. Yan, Z. Wang, X. Liu, and J. Ma, “ Privacy-preserving federated k-means for proactive caching in next generation cellular networks,” Information Sciences, vol. 521, pp. 14–31, 2020.
44. V. Chen, V. Pastro, and M. Raykova, “ Secure computation for machine learning with SPDZ,” arXiv preprint arXiv:1901.00329, 2019.
45. A. Ziller, A. Trask, A. Lopardo, B. Szymkow, B. Wagner, E. Bluemke, J. M. Nounahon, J. Passerat-Palmbach, K. Prakash, N. Rose, T. Ryffel, Z. N. Reza, and G. Kaissis, “ PySyft: A library for easy federated learning,” in Federated Learning Systems: Towards Next-Generation AI, pp. 111–139, Springer, 2021.
46. I. Damgård, V. Pastro, N. Smart, and S. Zakarias, “ Multiparty computation from somewhat homomorphic encryption,” in Proceedings of the 32nd Annual Cryptology Conference, pp. 643–662, 2012.

47. B. Jeon, S. M. Ferdous, M. R. Rahman, and A. Walid, “ Privacy-preserving decentralized aggregation for federated learning,” in Proceedings of 2021 IEEE Conference on Computer Communications Workshops, pp. 1–6, 2021.
48. T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “ Federated optimization in heterogeneous networks,” in Proceedings of Machine Learning and Systems 2020, 2020.
49. S. P. Karimireddy, S. Kale, M. Mohri, S. J. Reddi, S. U. Stich, and A. T. Suresh, “ SCAFFOLD: Stochastic controlled averaging for federated learning,” in Proceedings of the 37th International Conference on Machine Learning, p. 476, 2020.
50. J. Hamer, M. Mohri, and A. T. Suresh, “ FedBoost: Communication-efficient algorithms for federated learning,” in Proceedings of the 37th International Conference on Machine Learning, p. 372, 2020.
51. D. Rothchild, A. Panda, E. Ullah, N. Ivkin, I. Stoica, V. Braverman, J. Gonzalez, and R. Arora, “ FetchSGD: Communication-efficient federated learning with sketching,” in Proceedings of the 37th International Conference on Machine Learning, p. 764, 2020.
52. A. T. Suresh, F. X. Yu, S. Kumar, and H. B. McMahan, “Distributed mean estimation with limited communication,” in Proceedings of the 34th International Conference on Machine Learning, pp. 3329–3337, 2017.
53. S. Caldas, J. Konečný, B. McMahan, and A. Talwalkar, “Expanding the reach of federated learning by reducing client resource requirements.” ICLR Workshop, 2019.
54. J. Xu, W. Du, Y. Jin, W. He, and R. Cheng, “Ternary compression for communication-efficient federated learning,” IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 3, pp. 1162–1176, 2022.
55. F. Haddadpour, M. M. Kamani, A. Mokhtari, and M. Mahdavi, “Federated learning with compression: unified analysis and sharp guarantees,” in Proceedings of the 24th International Conference on Artificial Intelligence and Statistics, pp. 2350–2358, 2021.

56. L. Cui, X. Su, Z. Ming, Z. Chen, S. Yang, Y. Zhou, and W. Xiao, “Creat: blockchain-assisted compression algorithm of federated learning for content caching in edge computing,” IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14151–14161, 2022.
57. Q. Wu, K. He, and X. Chen, “Personalized federated learning for intelligent iot applications: A cloud-edge based framework,” IEEE Open Journal of the Computer Society, vol. 1, pp. 35–44, 2020.
58. A. Huang, Y. Liu, T. Chen, Y. Zhou, Q. Sun, H. Chai, and Q. Yang, “Starfl: Hybrid federated learning architecture for smart urban computing,” ACM Transactions on Intelligent Systems and Technology (TIST), vol. 12, no. 4, pp. 1–23, 2021.
59. A. M. Elbir, S. Coleri, and K. V. Mishra, “Hybrid federated and centralized learning,” arXiv preprint arXiv:2011.06892, 2020.
60. M. Chen, H. V. Poor, W. Saad, and S. Cui, “Wireless communications for collaborative federated learning,” IEEE Communications Magazine, vol. 58, no. 12, pp. 48–54, 2020.
61. S. Pandya, G. Srivastava, R. Jhaveri, M. R. Babu, S. Bhattacharya, P. K. R. Maddikunta *et al.*, “Federated learning for smart cities: A comprehensive survey,” *Sustainable Energy Technologies and Assessments*, vol. 55, Art. no. 102987, 2023, doi: 10.1016/j.seta.2022.102987.
62. B. Johnson and M. Geller, “Meta-federated learning: A novel approach for real-time traffic flow management,” *arXiv* preprint arXiv:2501.16758, 2025, doi: 10.48550/arXiv.2501.16758.
63. Z. Zhang, S. Rath, J. Xu, and T. Xiao, “Federated learning for smart grid: A survey on applications and potential vulnerabilities,” *arXiv* preprint arXiv:2409.10764, 2024, doi: 10.48550/arXiv.2409.10764.
64. T. E. T. Djaidja, B. Brik, A. Boualouache, S. M. Senouci, and Y. Ghamri-Doudane, “Federated learning for 5G and beyond, a blessing and a curse: An experimental study on intrusion detection systems,” *Computers & Security*, vol. 139, Art. no. 103707, 2024, doi: 10.1016/j.cose.2024.103707.

65. B. Shubyn, P. Grzesik, T. Maksymyuk, D. Kostrzewa, P. Benecki, J.-H. Syu, J. C.-W. Lin, V. Sunderam, and D. Mrozek, “Resource consumption of federated learning approach applied on edge IoT devices in the AGV environment,” in Computational Science – ICCS 2023, pp. 492–504, Springer Nature Switzerland, 2023.
66. Y. Zhang, X. Li, and P. Zhang, “Real-time automatic configuration tuning for smart manufacturing with federated deep learning,” in Service-Oriented Computing - 18th International Conference, ICSOC 2020, Dubai, United Arab Emirates, December 14-17, 2020, Proceedings (E. Kafeza, B. Benatallah, F. Martinelli, H. Hacid, A. Bouguettaya, and H. Motahari, eds.), vol. 12571 of Lecture Notes in Computer Science, pp. 304–318, Springer, 2020.
67. T. Maksymyuk, J. Gazda, M. Liyanage, L. Han, B. Shubyn, B. Strykhaliuk, O. Yaremko, M. Jo, and M. Dohler, “AI-enabled blockchain framework for dynamic spectrum management in multi-operator 6G networks,” *Lecture Notes in Electrical Engineering*, vol. 831, 2022, pp. 322–338.
68. T. Maksymyuk, J. Gazda, B. Shubyn *et al.*, “Metaverse of Things in 6G era: An emerging fusion of IoT, XR, edge AI and blockchain technologies,” *Lecture Notes in Electrical Engineering*, vol. 965, 2023, pp. 546–564.
69. A. Volovyk, Y. Pyrih, O. Urikova, A. Masiuk, B. Shubyn, and T. Maksymyuk, “Dynamic system state estimation with resilience to observation data anomalies,” *Contemporary Mathematics* (Singapore), vol. 5, no. 1, 2024.
70. A. Luntovskyy, B. Shubyn, T. Maksymyuk, and M. Klymash, “5G slicing and handover scenarios: compulsoriness and machine learning,” *Lecture Notes in Networks and Systems*, vol. 212, 2021, pp. 223–255.
71. T. A. Maksymyuk, B. P. Shubyn, D. O. Mysakovyets, V. S. Andrushchak, and S. S. Dumych, “Adaptive logical network slicing method for 5G based on deep learning,” Scientific Notes of Tavria National V. I. Vernadsky University. Series: Technical Sciences, vol. 31 (70), no. 5, pp. 36–42, 2020 (in Ukrainian).

72. A. Luntovskyy, L. Globa, and B. Shubyn, “From big data to smart data: The most effective approaches for data analytics,” *Lecture Notes in Networks and Systems*, vol. 152, 2021, pp. 23–40.
73. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, pp. 1273–1282, PMLR, 2017.
74. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” Proceedings of Machine Learning Research, vol. 119, pp. 4292–4304, 2020.
75. S. Ek, F. Portet, P. Lalanda, and G. Vega, “A federated learning aggregation algorithm for pervasive computing: Evaluation and comparison,” In 19th IEEE International Conference on Pervasive Computing and Communications PerCom 2021, 2021.
76. F. Chen, Z. Dong, Z. Li, and X. He, “Federated meta-learning for recommendation,” CoRR, vol. abs/1802.07876, 2018.
77. C. Finn, P. Abbeel, and S. Levine, “Model-agnostic meta-learning for fast adaptation of deep networks,” In International conference on machine learning, pp. 1126–1135, 2017.
78. H. Wang, M. Yurochkin, Y. Sun, D. S. Papailiopoulos, and Y. Khazaeni, “Federated learning with matched averaging,” in 8th International Conference on Learning Representations (ICLR), OpenReview.net, 2020.
79. S. Ek, F. Portet, P. Lalanda, and G. Vega, “A federated learning aggregation algorithm for pervasive computing: Evaluation and comparison,” in 2021 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 1–10, IEEE, 2021.
80. J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, “Federated learning: Strategies for improving communication efficiency,” CoRR, vol. abs/1610.05492, 2016.

81. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (A. Singh and J. Zhu, eds.), vol. 54 of Proceedings of Machine Learning Research, pp. 1273–1282, PMLR, 20–22 Apr 2017.
82. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Fedprox: Federated optimization in heterogeneous networks," Proceedings of Machine learning and systems, pp. 429–450, 2020.
83. M. G. Arivazhagan, V. Aggarwal, A. K. Singh, and S. Choudhary, "Federated learning with personalization layers," arXiv preprint arXiv:1912.00818, 2019.
84. C. Briggs, Z. Fan, and P. Andras, "Federated learning with hierarchical clustering of local updates to improve training on non-iid data," 2020.
85. T. Berghout, T. Bentrcia, M. A. Ferrag, and M. Benbouzid, "A heterogeneous federated transfer learning approach with extreme aggregation and speed," Mathematics, vol. 10, no. 19, 2022.
86. R. Ye, Z. Ni, C. Xu, J. Wang, S. Chen, and Y. C. Eldar, "Fedfm: Anchor-based feature matching for federated learning," arXiv preprint arXiv:2210.07615, 2022.
87. C. Palihawadana, N. Wiratunga, A. Wijekoon, and H. Kalutarage, "Fedsim: Similarity guided model aggregation for federated learning," Neurocomputing , vol. 483, pp. 432–445, 2022.
88. D. Li and J. Wang, "Fedmd: Heterogenous federated learning via model distillation," arXiv preprint arXiv:1910.03581, 2019.
89. L. Hu, H. Yan, L. Li, Z. Pan, X. Liu, and Z. Zhang, "Mhat: An efficient model-heterogenous aggregation training scheme for federated learning," Information Sciences, vol. 560, pp. 493–503, 2021.
90. C. Xie, S. Koyejo, and I. Gupta, "Asynchronous federated optimization," arXiv preprint arXiv:1903.03934, 2019.
91. J. Yao and N. Ansari, "Enhancing federated learning in fog-aided iot by cpu frequency and wireless power control," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3438–3445, 2020.

92. Z. Xu, Z. Yang, J. Xiong, J. Yang, and X. Chen, “Elfish: Resource-aware federated learning on heterogeneous edge devices,” arXiv preprint arXiv:1908.04373, 2019.
93. R. Saha, S. Misra, and P. K. Deb, “Fogfl: Fog-assisted federated learning for resource-constrained iot devices,” IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8456–8463, 2020.
94. L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. Nguyen, and C. S. Hong, “Federated learning for edge networks: Resource optimization and incentive mechanism,” IEEE Communications Magazine, vol. 58, no. 10, pp. 88–93, 2020.
95. Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, “A blockchained federated learning framework for cognitive computing in industry 4.0 networks,” IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2964–2973, 2020.
96. H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, “Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing,” IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 6073–6084, 2021.
97. S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, “Unsupervised real-time anomaly detection for streaming data,” Neurocomputing, vol. 262, pp. 134–147, 2017.
98. A. Luntovskyy and B. Shubyn, “Energy efficiency for IoT,” *Studies in Computational Intelligence*, vol. 976, 2021, pp. 199–215.
99. B. Shubyn, D. Mrozek, T. Maksymyuk, V. Sunderam, D. Kostrzewa, P. Grzesik, and P. Benecki, “Federated learning for anomaly detection in industrial IoT-enabled production environment supported by autonomous guided vehicles,” *Lecture Notes in Computer Science*, vol. 13353, 2022, pp. 409–421.
100. T. Maksymyuk, N. Lutsiv, B. Shubyn, J. Gazda, and O. Ivakhiv, “Feature engineering for deep learning-based anomaly detection in 5G and beyond,” in Proc. IEEE Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2023, pp. 1110–1113.

101. P. Benecki, D. Kostrzewa et al., “Towards detection of anomalies in automated guided vehicles based on telemetry data,” Lecture Notes in Computer Science, vol. 14838, 2024, pp. 192–207.

102. P. Benecki, D. Kostrzewa, B. Shubyn et al., “Enhancing anomaly detection in automated guided vehicles through feature weight optimization,” in Companion Proc. 2024 Genetic and Evolutionary Computation Conf. (GECCO), 2024, pp. 79–80.

103. A. Luntovskyy, T. Zobjack, B. Shubyn, and M. Klymash, “Energy efficiency and security for IoT scenarios via WSN, RFID and NFC,” in Proc. IEEE Ukrainian Microwave Conf. (UkrMiCo), 2021, pp. 1–6.

104. B. Shubyn, D. Mrozek, L. Fabry, T. Maksymyuk, E. M. Amhoud, and J. Gazda, “Federated learning techniques for 5G mobile networks,” in Proc. 16th Int. Conf. Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2022, pp. 653–657.

105. A. Luntovskyy and B. Shubyn, “Advanced architectures for IoT scenarios,” in Proc. Int. Conf. Smart and Sustainable Technologies (SpliTech), 2020.

106. A. Luntovskyy, B. Shubyn, T. Maksymyuk, and M. Klymash, “Highly-distributed systems: What is inside?” in Proc. IEEE Conf. Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 207–211.

107. P. Grzesik, P. Benecki, D. Kostrzewa, B. Shubyn, and D. Mrozek, “On-edge aggregation strategies over industrial data produced by autonomous guided vehicles,” Lecture *Notes in Computer Science*, vol. 13353, 2022, pp. 458–471.

108. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, and D. Mrozek, “Forecasting of energy consumption for anomaly detection in automated guided vehicles: Models and feature selection,” in *Proc. IEEE Int. Conf. Systems, Man and Cybernetics (SMC)*, 2022, pp. 2073–2079.

109. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, and D. Mrozek, “Optimizing telemetry signal influence for power consumption prediction,” in *Companion Proc. 2023 Genetic and Evolutionary Computation Conf. (GECCO)*, 2023, pp. 51–52.

110. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, J.-H. Syu, J. C.-W. Lin, V. Sunderam, and D. Mrozek, “Effective prediction of energy consumption in automated guided vehicles with recurrent and convolutional neural networks,” in *Proc. IEEE Int. Conf. Big Data (BigData)*, 2023, pp. 5024–5030.

111. B. Shubyn, T. Maksymyuk, J. Gazda, B. Rusyn, and D. Mrozek, “Federated learning: A solution for improving anomaly detection accuracy of autonomous guided vehicles in smart manufacturing,” *Lecture Notes in Electrical Engineering*, vol. 1198, 2024, pp. 746–761.

112. B. Shubyn, D. Kostrzewa, P. Grzesik, P. Benecki, T. Maksymyuk, V. Sunderam, J.-H. Syu, J. C.-W. Lin, and D. Mrozek, “Federated learning for improved prediction of failures in autonomous guided vehicles,” Journal of Computational Science, p. 101956, 2023.

ДОДАТОК А. АКТИ ВИКОРИСТАННЯ ТА ВПРОВАДЖЕННЯ

«ЗАТВЕРДЖУЮ»
Директор
ТзОВ «МАКСІТЕХ»
Сергій ЗАБЛОЦЬКИЙ.
“__” квітня 2025 р.

АКТ
про використання результатів дисертаційної роботи
Шубина Богдана Петровича
«Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою»

Даний акт складений про те, що у ТзОВ «МАКСІТЕХ» для підвищення ефективності управління інфраструктурою телекомунікаційної мережі використано результати дисертаційної роботи Шубина Б.П. «Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою», представленої на здобуття наукового ступеня доктора філософії, а саме:

- Використання алгоритму обчислення агрегованих моделей федеративного навчання з введенням додаткового середньозваженого критерію оцінювання ефективності локальних моделей кінцевих пристроїв дало змогу підвищити точність прогнозування трафіку в телекомунікаційній мережі.

Результати експериментальних досліджень, виконаних на виробничих потужностях ТзОВ «МАКСІТЕХ», відповідають результатам досліджень, що представлені у дисертаційній роботі, похибка не перевищує 3%.

Інженер з телекомунікацій та електроніки
ТзОВ “МаксіТех” Матіїшин Л.З.

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
Національного університету
"Львівська політехніка"
_____ доц. Олег ДАВИДЧАК
"___" травня 2025 р.

АКТ

про впровадження в навчальний процес результатів
дисертаційної роботи на здобуття наукового ступеня доктора філософії
Шубина Богдана Петровича

Цей акт складений комісією у складі завідувача кафедри ІКТ, д.т.н., проф. Михайла КЛИМАША, к.т.н., доцента кафедри ІКТ Ольги ШПУР, д.т.н., проф., професора кафедри ІКТ Мар'яна КИРИКА, д.т.н., доц., професора кафедри ІКТ Миколи БЕШЛЕЯ, про те, що результати дисертаційної роботи Шубина Богдана Петровича на тему «Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою», представленої на здобуття наукового ступеня доктора філософії, використовуються у навчальному процесі кафедри «Інформаційно-комунікаційних технологій» Національного університету «Львівська політехніка».

Матеріали дисертаційного дослідження використовуються під час викладання дисциплін «Інтернет речей та 5G технології» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 126 «Інформаційні системи та технології». Зокрема, впроваджено методи федеративного машинного навчання для модернізації лабораторної роботи «Дослідження методів прогнозування трафіку в мережах мобільного зв'язку 5G».

Також матеріали дисертаційного дослідження впроваджено в освітній процес під час викладання навчальної дисципліни «Технології машинного навчання та штучного інтелекту» для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 126 «Інформаційні системи та технології» освітньо-наукової програми «Інформаційно-комунікаційні системи». Зокрема в лекційний матеріал було впроваджено приклади застосування запропонованих методів федеративного навчання, як перспективних сучасних підходів до побудови інтелектуальних розподілених систем.

Голова комісії:
завідувач кафедри ІКТ, д.т.н., проф. _____ Михайло КЛИМАШ

Члени комісії:
доцент кафедри ІКТ, к.т.н., _____ Ольга ШПУР

професор кафедри ІКТ, д.т.н., проф. _____ Мар'ян КИРИК

професор кафедри ІКТ, д.т.н., доц. _____ Микола БЕШЛЕЙ

«Затверджую»
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
д.т.н., проф. Івану ДЕМИДОВУ
«__» травня 2025 р.

АКТ

про використання результатів дисертаційної роботи Шубина Богдана Петровича на тему «Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою».

Комісія у складі начальника науково-дослідної частини, д.т.н., Небесного Р.В., В.О. начальника планово-фінансового відділу Фаст І.І., завідувача кафедри інформаційно-комунікаційних технологій, д.т.н., проф. Климаша М.М., склала цей акт у тому, що у держбюджетних науково-дослідних роботах:

- «Розроблення інноваційних методів та моделей побудови індустріально-орієнтованих інформаційно-комунікаційних систем для модернізації цифрових інфраструктур промисловості» (№ держреєстрації 0122U000817) (2022-2024 рр.) – основний виконавець;
- «Розроблення новітньої децентралізованої мережі мобільного зв'язку на основі блокчейн-архітектури та штучного інтелекту для впровадження технологій 5G/6G в Україні» (ДБ/Блокчейн), (2020–2022 рр.) – учасник; № держреєстрації 0120U100674;
- «Розроблення інноваційних методів та засобів розгортання інтелектуальної інформаційної інфраструктури для подвійного використання в умовах цифрової трансформації України (2023–2025 рр.) – учасник; № держреєстрації 0123U100232.

Використано наступні результати дисертаційної роботи Шубина Богдана Петровича на тему «Методи та моделі побудови інтелектуальних інформаційно-комунікаційних систем автоматизованого управління інфраструктурою»:

- метод багатораундного федеративного навчання, що забезпечує зниження складності обчислень для мобільних кінцевих пристроїв федеративного навчання;
- метод обчислення параметрів агрегованої моделі, що забезпечує підвищення ефективності процесу федеративного навчання за рахунок зниження вагомості помилок локальних моделей при обчисленні агрегованої моделі;
- структурно-функціональну модель інтелектуальної інформаційно-комунікаційної системи, яка забезпечує інтероперабельність та обмін досвідом між різними виробничими та невиробничими інфраструктурами в процесі федеративного навчання.

Члени комісії:

Роман НЕБЕСНИЙ

Ірина ФАСТ

Михайло КЛИМАШ

Norway grants

Rzeczpospolita Polska

Narodowe Centrum Badań i Rozwoju

ZAŁĄCZNIK DO UMOWY O DZIEŁO NR UMC/0802/2023 Z DNIA 13.03.2023 R..

zawartej między:

Politechniką Śląska, ul. Akademicka 2A, 44-100 Gliwice
a
Panem **mgr inż. Bohdanem Shubyn**

w ramach projektu pn.: *„Automated Guided Vehicles integrated with Collaborative Robots for Smart Industry Perspective"*, akronim: CoBotAGV, nr umowy o dofinansowanie: NOR/POLNOR/CoBotAGV/0027/2019-00, nr wewnętrzny: 02/110/ZZB/006

W związku z zawarciem wyżej wymienionej umowy o dzieło, Strony ustalają, że zakres przedmiotowej umowy obejmuje:

1. Przygotowanie raportu pt. *„Resource consumption on AGVs while using Machine Learning based on the Federated Learning approach" (Zużycie zasobów w AGV podczas korzystania z uczenia maszynowego w oparciu o podejście Federated Learning)*
2. Przekazanie praw autorskich do przygotowanego raportu.

podpis Wykonawcy

podpis Zamawiającego

Projekt realizowany w ramach Polsko-Norweskiej Współpracy Badawczej,
Norweski Mechanizm Finansowy EOG na lata 2014-2021

ДОДАТОК Б. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Статті у наукових періодичних виданнях інших держав, які включені до наукометричних баз Scopus/Web of Science:

1. B. Shubyn, D. Kostrzewa, P. Grzesik, P. Benecki, T. Maksymyuk, V. Sunderam, J.-H. Syu, J. C.-W. Lin, and D. Mrozek, “Federated learning for improved prediction of failures in autonomous guided vehicles,” Journal of Computational Science, p. 101956, 2023.
2. B. Shubyn, D. Mrozek, T. Maksymyuk, V. Sunderam, D. Kostrzewa, P. Grzesik, and P. Benecki, “Federated learning for anomaly detection in industrial IoT-enabled production environment supported by autonomous guided vehicles,” *Lecture Notes in Computer Science*, vol. 13353, 2022, pp. 409–421.
3. T. Maksymyuk, J. Gazda, M. Liyanage, L. Han, B. Shubyn, B. Strykhaliuk, O. Yaremko, M. Jo, and M. Dohler, “AI-enabled blockchain framework for dynamic spectrum management in multi-operator 6G networks,” *Lecture Notes in Electrical Engineering*, vol. 831, 2022, pp. 322–338.
4. A. Luntovskyy, B. Shubyn, T. Maksymyuk, and M. Klymash, “5G slicing and handover scenarios: compulsoriness and machine learning,” *Lecture Notes in Networks and Systems*, vol. 212, 2021, pp. 223–255.
5. A. Luntovskyy and B. Shubyn, “Energy efficiency for IoT,” Studies in Computational Intelligence, vol. 976, 2021, pp. 199–215
6. B. Shubyn, T. Maksymyuk, J. Gazda, B. Rusyn, and D. Mrozek, “Federated learning: A solution for improving anomaly detection accuracy of autonomous guided vehicles in smart manufacturing,” *Lecture Notes in Electrical Engineering*, vol. 1198, 2024, pp. 746–761.
7. A. Luntovskyy, L. Globa, and B. Shubyn, “From big data to smart data: The most effective approaches for data analytics,” Lecture Notes in Networks and Systems, vol. 152, 2021, pp. 23–40.

8. P. Grzesik, P. Benecki, D. Kostrzewa, B. Shubyn, and D. Mrozek, “On-edge aggregation strategies over industrial data produced by autonomous guided vehicles,” Lecture Notes in Computer Science, vol. 13353, 2022, pp. 458–471.
9. A. Volovyk, Y. Pyrih, O. Urikova, A. Masiuk, B. Shubyn, and T. Maksymyuk, “Dynamic system state estimation with resilience to observation data anomalies,” *Contemporary Mathematics* (Singapore), vol. 5, no. 1, 2024.
10. T. Maksymyuk, J. Gazda, B. Shubyn *et al.*, “Metaverse of Things in 6G era: An emerging fusion of IoT, XR, edge AI and blockchain technologies,” *Lecture Notes in Electrical Engineering*, vol. 965, 2023, pp. 546–564.
11. B. Shubyn, P. Grzesik, T. Maksymyuk, D. Kostrzewa, P. Benecki, J.-H. Syu, J. C.-W. Lin, V. Sunderam, and D. Mrozek, “Resource consumption of federated learning approach applied on edge IoT devices in the AGV environment,” in Computational Science – ICCS 2023, pp. 492–504, Springer Nature Switzerland, 2023.
12. P. Benecki, D. Kostrzewa *et al.*, “Towards detection of anomalies in automated guided vehicles based on telemetry data,” *Lecture Notes in Computer Science*, vol. 14838, 2024, pp. 192–207.

Статті у наукових періодичних фахових виданнях України:

13. Модель інтеграції федеративного навчання в мережі мобільного зв’язку п’ятого покоління. Шубин Б.П., Максимюк Т.А., Яремко О.М., Фабрі Л.П., Мрозек Д. Інфокомунікаційні технології та електронна інженерія. – 2022. – Т. 2, № 1. – С. 26–35.
14. Метод адаптивного логічного розділення мережі 5G на основі глибокого навчання. Максимюк Т.А., Шубин Б.П., Мисаковець Д.О., Андрущак В.С., Думич С.С. Вчені записки Таврійського національного університету ім. В. І. Вернадського. Серія «Технічні науки». – 2020. – Т. 31(70), № 5. – С. 36–42.

Статті у інших наукових періодичних виданнях:

15. Управління мережами мобільного зв’язку 5G за допомогою використання технологій штучного інтелекту. Шубин Б.П., Климаш М.М., Масюк А.Р.,

Осташевський А.І. Інфокомунікаційні технології та електронна інженерія. – 2021. – Т. 1, № 1. – С. 1–10.

Матеріали Всеукраїнських та міжнародних конференцій:

16. B. Shubyn, D. Mrozek, L. Fabry, T. Maksymyuk, E. M. Amhoud, and J. Gazda, “Federated learning techniques for 5G mobile networks,” in *Proc. 16th Int. Conf. Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 653–657.
17. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, and D. Mrozek, “Forecasting of energy consumption for anomaly detection in automated guided vehicles: Models and feature selection,” in *Proc. IEEE Int. Conf. Systems, Man and Cybernetics (SMC)*, 2022, pp. 2073–2079.
18. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, and D. Mrozek, “Optimizing telemetry signal influence for power consumption prediction,” in *Companion Proc. 2023 Genetic and Evolutionary Computation Conf.*, 2023, pp. 51–52.
19. P. Benecki, D. Kostrzewa, P. Grzesik, B. Shubyn, J.-H. Syu, J. C.-W. Lin, V. Sunderam, and D. Mrozek, “Effective prediction of energy consumption in automated guided vehicles with recurrent and convolutional neural networks,” in *Proc. IEEE Int. Conf. Big Data (BigData)*, 2023, pp. 5024–5030.
20. T. Maksymyuk, N. Lutsiv, B. Shubyn, J. Gazda, and O. Ivakhiv, “Feature engineering for deep learning-based anomaly detection in 5G and beyond,” in *Proc. IEEE Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, 2023, pp. 1110–1113.
21. P. Benecki, D. Kostrzewa, B. Shubyn *et al.*, “Enhancing anomaly detection in automated guided vehicles through feature weight optimization,” in *Companion Proc. 2024 Genetic and Evolutionary Computation Conf. (GECCO)*, 2024, pp. 79–80.
22. A. Luntovskyy and B. Shubyn, “Advanced architectures for IoT scenarios,” in Proc. Int. Conf. Smart and Sustainable Technologies (SpliTech), 2020.

23. A. Luntovskyy, B. Shubyn, T. Maksymyuk, and M. Klymash, “Highly-distributed systems: What is inside?” in *Proc. IEEE Conf. Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 207–211.
24. A. Luntovskyy, T. Zobjack, B. Shubyn, and M. Klymash, “Energy efficiency and security for IoT scenarios via WSN, RFID and NFC,” in *Proc. IEEE Ukrainian Microwave Conf. (UkrMiCo)*, 2021, pp. 1–6.
25. M. Buchyn, A. Helesh, and B. Shubyn, “Information security during electronic voting: Threats and mechanisms for ensuring,” in *Proc. IEEE 4th Int. Conf. Advanced Information and Communication Technologies (AICT)*, 2021, pp. 266–269, doi: 10.1109/AICT52120.2021.9628971.