УДК 621.391:004.056.53 **DOI**: 10.31673/2412-9070.2026.050617

О. Є. ГОРШЕНІН, канд. техн. наук, доцент;
ORCID: 0009-0005-8946-3339
В. В. ЧУХОВ, канд. техн. наук, доцент;
ORCID: 0000-0001-7782-9077
Д. О. ВАРГАНОВА, ст. викл.;
ORCID: 0000-0002-8712-027X
Д. С. МОРОЗОВ, ст. викл.,
ORCID: 0000-0002-0807-590X
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ FEDERATED LEARNING У СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ: ОПТИМІЗАЦІЯ МЕРЕЖЕВИХ РЕСУРСІВ ТА КІБЕРБЕЗПЕКА

У статті досліджено перспективи та методологію впровадження технології федеративного навчання (Federated Learning – FL) у сучасні телекомунікаційні мережі наступних поколінь (5G/6G). Розглянуто концептуальні засади FL як інноваційного підходу до розподіленого машинного навчання, що дозволяє здійснювати навчання глобальних моделей штучного інтелекту безпосередньо на периферійних пристроях (Edge computing) без необхідності централізованої передачі сирих даних на сервери обробки. Такий підхід суттєво знижує вимоги до пропускної здатності магістральних каналів зв'язку та мінімізує ризики витоку конфіденційної інформації користувачів.

Здійснено аналіз архітектурних особливостей інтеграції FL у телекомунікаційні системи, включаючи взаємодію периферійних вузлів, базових станцій та центрального агрегатора моделей. Особливу увагу приділено алгоритмам федеративної агрегації, зокрема FedAvg та його модифікаціям, які забезпечують ефективне об'єднання локально навчених параметрів у глобальну модель. Досліджено роль FL у підвищенні рівня кібербезпеки сучасних телекомунікаційних систем. Встановлено, що використання децентралізованого навчання дозволяє значно зменшити поверхню атак, оскільки відсутня необхідність передачі персоналізованих даних у централізовані сховища. Водночас проаналізовано потенційні загрози, пов'язані з атаками на модель (model poisoning, inference attacks), що потребують додаткових механізмів захисту та валідації оновлень.

Показано, що впровадження Federated Learning у поєднанні з технологіями Mobile Edge Computing (MEC) та Software Defined Networking (SDN) створює основу для побудови інтелектуальних, адаптивних та самоорганізованих телекомунікаційних мереж нового покоління. Отримані результати свідчать про високу перспективність FL як ключової технології для реалізації концепції мереж із вбудованим штучним інтелектом (AI-native networks), здатних ефективно функціонувати в умовах високої динаміки навантаження та обмежених ресурсів.

Ключові слова: телекомунікаційні системи, Federated Learning, федеративне навчання, периферійні обчислення (Edge Computing), 5G/6G, оптимізація трафіку, кібербезпека.

Вступ

Стрімкий розвиток телекомунікаційних технологій, збільшення обсягів передавання даних та впровадження мереж п'ятого і шостого поколінь (5G/6G) формують нові вимоги до ефективності управління мережевими ресурсами, швидкості обробки інформації та рівня кібербезпеки. Сучасні телекомунікаційні системи функціонують в умовах постійного зростання кількості підключених пристроїв, зокрема IoT-систем, мобільних терміналів та периферійних обчислювальних вузлів. У таких умовах традиційні централізовані підходи до збору та

© Горшенін О. Є., Чухов В.В., Варганова Д. О., Морозов Д. С., 2026

обробки даних створюють значне навантаження на транспортні канали зв'язку (Backhaul), збільшують затримки передачі інформації та підвищують ризики витоку конфіденційних даних.

Одним із перспективних напрямів вирішення зазначених проблем є використання технології Federated Learning (FL), яка дозволяє здійснювати навчання моделей штучного інтелекту без передачі сирих даних до центрального сервера. На відміну від класичних централізованих моделей машинного навчання, FL забезпечує локальне навчання на периферійних пристроях із подальшою передачею лише вагових коефіцієнтів або параметрів моделі. Такий підхід суттєво знижує навантаження на мережеву інфраструктуру та підвищує рівень захисту інформації [2].

Особливої актуальності технологія Federated Learning набуває в телекомунікаційних системах нового покоління, де виникає потреба в оперативному аналізі великих потоків даних у режимі реального часу. Використання FL у поєднанні з технологіями Multi-access Edge Computing (MEC) та Software Defined Networking (SDN) дозволяє реалізувати інтелектуальне керування радіоресурсами, прогнозування навантаження мережі, адаптивне розподілення спектра частот та автоматичне виявлення кіберзагроз.

Водночас впровадження Federated Learning у телекомунікаційне середовище супроводжується низкою технічних викликів. До основних проблем належать нестабільність бездротових каналів зв'язку, обмеженість обчислювальних ресурсів периферійних пристроїв, неоднорідність апаратного забезпечення, затримки синхронізації моделей та вразливість до атак на процес федеративного навчання. Це потребує розробки нових алгоритмів оптимізації, методів стиснення параметрів моделей та засобів захисту від кіберзагроз [3].

Метою даної статті є дослідження особливостей застосування технології Federated Learning у сучасних телекомунікаційних системах, аналіз її впливу на оптимізацію мережевих ресурсів та підвищення рівня кібербезпеки. У роботі розглянуто архітектурні особливості FL у телекомунікаційному середовищі, основні переваги та недоліки технології, а також перспективи її використання в мережах нового покоління.

Постановка проблеми

Розвиток мобільних мереж п'ятого (5G) та шостого (6G) поколінь супроводжується лавиноподібним зростанням кількості підключених пристроїв Інтернету речей (IoT) та обсягів трафіку. Сучасні телекомунікаційні платформи стикаються із серйозним технологічним викликом – критичною потребою в оптимізації обчислювальних алгоритмів для безперебійного аналізу масивних цифрових потоків з мінімальною затримкою у режимі реального часу.

Традиційні підходи на основі централізованого машинного навчання (Centralized ML) вимагають збору та передачі гігабайтів сирих даних (наприклад, логів базових станцій, телеметрії смартфонів) у єдине хмарне сховище. Це породжує дві фундаментальні проблеми:

1. Перевантаження транспортної мережі: передавання вихідних даних споживає дефіцитну пропускну здатність каналів зв'язку.

2. Конфіденційність: передача персональних даних користувачів суперечить сучасним стандартам безпеки (GDPR тощо).

Концепція Federated Learning (FL) вирішує цю суперечність, пропонуючи парадигму «навчання на місцях», де дані залишаються на пристроях, а мережею передаються лише оновлені вагові коефіцієнти математичних моделей [1].

Аналіз останніх досліджень і публікацій (Literature Review)

Основи федеративного навчання (Federated Learning, FL) були сформовані у 2017 році дослідницькою групою компанії Google як відповідь на зростаючі вимоги до конфіденційності даних та необхідності навчання моделей машинного навчання без централізованої передачі сирих даних. Початкові дослідження були зосереджені на задачах оптимізації для мобільних пристроїв, де запропонований підхід дозволяв виконувати локальне навчання моделей безпосередньо на користувацьких пристроях із подальшою агрегацією оновлень на сервері.

Подальший розвиток концепції FL у період 2018-2022 років був пов'язаний із вдосконаленням алгоритмів агрегації, серед яких найбільш відомим став алгоритм FedAvg (Federated Averaging). Даний підхід забезпечив базову модель для синхронізації локальних оновлень шляхом усереднення вагових коефіцієнтів, що дозволило значно зменшити обсяг переданих даних у порівнянні з класичними централізованими схемами навчання. Окрім FedAvg, у науковій літературі були запропоновані модифікації, спрямовані на підвищення стійкості до неоднорідності даних (non-IID data), оптимізацію швидкості збіжності та зменшення впливу затримок у мережі.

У 2023-2026 роках концепція Federated Learning почала активно інтегруватися у телекомунікаційні системи нового покоління, зокрема в архітектури 5G та перспективні 6G-мережі. Особливу увагу дослідники приділяють використанню FL у поєднанні з технологіями Mobile Edge Computing (MEC), Multi-access Edge Computing та Software Defined Networking (SDN). У таких системах обчислення та навчання моделей переносяться ближче до джерел даних – на периферійні вузли, що дозволяє зменшити затримки та підвищити ефективність керування мережевими ресурсами [4].

Окремий напрям досліджень стосується застосування FL для оптимізації Radio Resource Management (RRM), зокрема для динамічного розподілу спектра частот, балансування навантаження між базовими станціями та прогнозування трафіку в реальному часі. Результати сучасних робіт демонструють, що використання федеративних підходів дозволяє підвищити ефективність використання радіоресурсів, зменшити перевантаження мережі та покращити якість обслуговування (QoS) у гетерогенних телекомунікаційних середовищах.

Водночас у наукових публікаціях наголошується на значних обмеженнях та відкритих проблемах впровадження FL у реальні телекомунікаційні системи. Однією з ключових проблем є нестабільність бездротових каналів зв'язку, яка призводить до втрати або пошкодження вагових оновлень моделей під час їх передачі від периферійних вузлів до агрегуючого сервера. У таких умовах виникають проблеми десинхронізації навчального процесу, уповільнення збіжності моделей та зниження загальної точності прогнозування.

Іншим критичним викликом є гетерогенність телекомунікаційних пристроїв, відома як проблема stragglers, коли частина вузлів має обмежені обчислювальні ресурси або нестабільне підключення до мережі. Це призводить до асинхронності оновлень та ускладнює реалізацію класичних алгоритмів агрегації. У сучасних дослідженнях пропонуються підходи до часткової участі клієнтів, адаптивного вибору вузлів та використання ймовірнісних схем синхронізації для мінімізації впливу цієї проблеми [5].

Значна увага приділяється також питанням кібербезпеки у FL-системах. Незважаючи на відсутність прямої передачі сирих даних, існує ризик атак типу model poisoning та data poisoning, при яких зловмисні вузли можуть навмисно змінювати вагові коефіцієнти моделі з метою спотворення результатів навчання. Крім того, досліджуються атаки на основі відновлення даних із градієнтів (gradient inversion attacks), які потенційно дозволяють відтворити вихідні дані користувачів навіть без їх прямої передачі [6].

Окремим напрямом є дослідження енергоефективності FL у мобільних та IoT-мережах. Встановлено, що локальне навчання моделей суттєво збільшує навантаження на обчислювальні ресурси кінцевих пристроїв, що може призводити до підвищеного енергоспоживання та скорочення часу автономної роботи. У зв'язку з цим активно розробляються методи оптимізації частоти оновлень, квантування моделей та стиснення градієнтів.

Таким чином, сучасний стан досліджень FL у телекомунікаційних системах демонструє значний прогрес у напрямі підвищення ефективності мережевих ресурсів та забезпечення конфіденційності даних. Водночас залишаються відкритими питання надійності функціонування FL у реальних умовах нестабільних каналів зв'язку, масштабованості рішень у великих гетерогенних мережах та стійкості до сучасних кіберзагроз, що визначає актуальність подальших досліджень у цій області.

Основна частина

Архітектура Federated Learning у телекомунікаційному середовищі базується на децентралізованому принципі навчання моделей штучного інтелекту, за якого обробка даних виконується безпосередньо на периферійних вузлах мережі. На відміну від класичного ШІ, де сервер зчитує всю базу даних, процес FL у телекомунікаціях побудований за ітераційним принципом. Виконаємо візуалізацію архітектури FL у телекомунікаційному середовищі (рис.1).

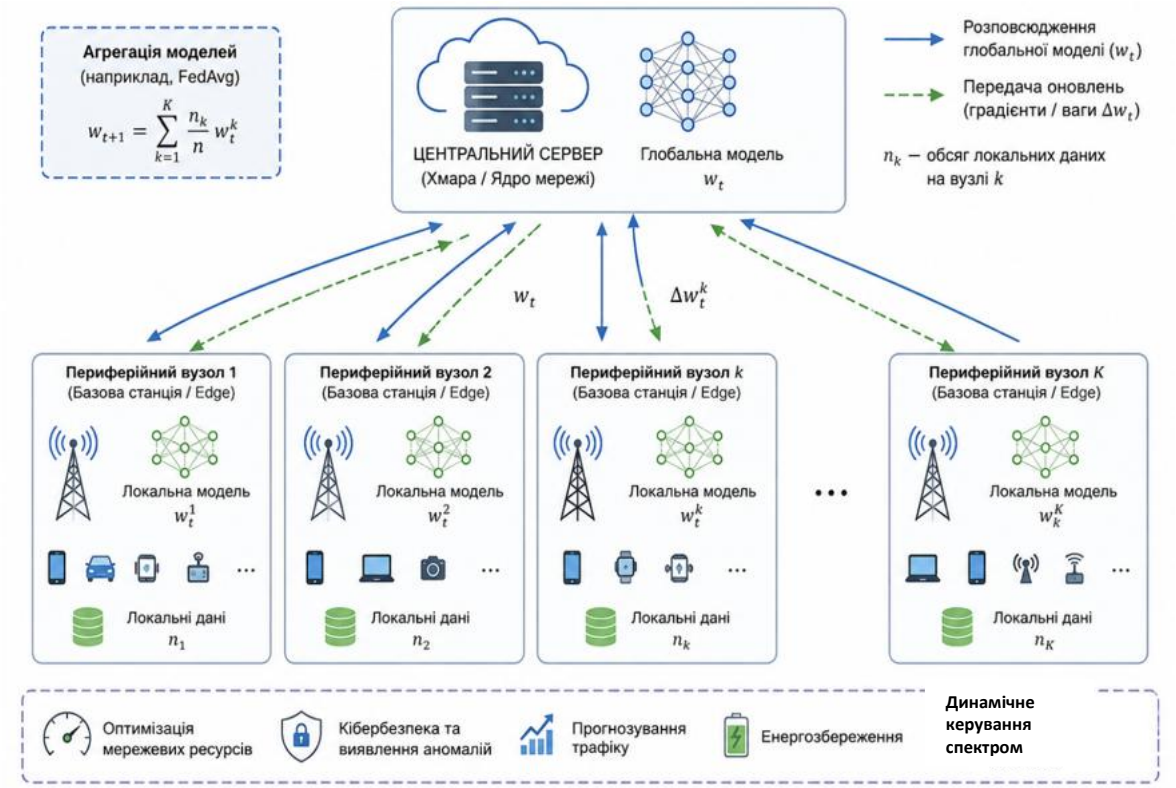


Рис. 1. Візуалізація архітектури FL у телекомунікаційному середовищі

Розглянемо структуру ітераційного принципу:

1. Центральний сервер (наприклад, ядро мережі оператора або хмара) ініціалізує глобальну модель штучного інтелекту (наприклад, нейромережу для прогнозування мобільного трафіку).
2. Копія цієї моделі надсилається на периферійні вузли (Edge вузли: базові станції gNodeB або кінцеві пристрої користувачів).
3. Кожен вузол проводить навчання моделі локально, використовуючи лише власні дані (метрики завантаження локальних стільників, рівень сигналу RSSI).
4. Замість відправки даних вузли відправляють назад на сервер лише градієнти або матриці вагових коефіцієнтів (ΔW) [7].
5. Сервер агрегує отримані оновлення (найчастіше за алгоритмом FedAvg):

$$W_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} W_t^k , \quad (1)$$

де W_{t+1} – оновлена глобальна вага моделі, n_k – обсяг локальних даних на k-му пристрої, W_t^k – локальні ваги пристрою.

Результати дослідження

У ході дослідження сценаріїв застосування FL у комунікація виділено три найбільш перспективні сфери інтеграції FL у мережеву інфраструктуру:

– Динамічний розподіл спектра (Slicing): Моделі FL на базових станціях прогнозують сплески трафіку окремо для різних типів сервісів (eMBB, URLLC, mMTC) та миттєво перерозподіляють частотні канали без запитів до центрального ядра.

– Енергозбереження базових станцій: Локальні моделі аналізують поведінку абонентів у зоні покриття і вимикають невикористовувані антени MIMO в години найменшого навантаження.

– Периферійне виявлення аномалій (IoT Security): FL дозволяє виявляти DDoS-атаки на рівні IoT-шлюзів до того як шкідливий трафік заблокує магістральний канал.

Для визначення практичної доцільності впровадження FL у телекомунікаційних системах виконано порівняльне дослідження централізованого та федеративного підходів до машинного навчання [6]. Моделювання проводилося для мережі, що містить 100 базових станцій, а результати оцінювання наведено у табл. 1.

Таблиця 1

Порівняльна характеристика централізованого (ML) та федеративного навчання (FL)

Критерій порівняння	Централізоване навчання (ML)	Федеративне навчання (FL)
Обсяг Backhaul-трафіку	Високий (передача всіх сирих логів)	Низький (лише W-коефіцієнти, економія до 85%)
Затримка прийняття рішень	Обумовлена часом передачі в хмару	Мінімальна (рішення приймається на Edge-вузлі)
Рівень приватності даних	Низький	Абсолютний (дані не залишають пристрій)
Вимоги до обчислень на Edge	Відсутні	Середні/Високі (потрібні процесори з підтримкою ШІ)

У мережах п'ятого та шостого поколінь технологія Federated Learning відіграє важливу роль у реалізації концепції інтелектуального керування мережею. На відміну від традиційних телекомунікаційних систем мережі 5G/6G повинні підтримувати мільйони одночасно підключених пристроїв із різними вимогами до швидкості передачі даних, затримок та енергоспоживання.

Одним із ключових напрямів використання FL у мережах 5G є Network Slicing – технологія логічного розділення фізичної мережі на окремі віртуальні сегменти для різних сервісів:

– eMBB (enhanced Mobile Broadband);
– URLLC (Ultra-Reliable Low Latency Communications);
– mMTC (massive Machine Type Communications).

Алгоритми FL дозволяють локальним вузлам прогнозувати навантаження кожного сегмента мережі та динамічно перерозподіляти радіоресурси без необхідності постійної взаємодії з центральним сервером. Це дозволяє знизити затримки та підвищити ефективність використання спектра [6].

У перспективних мережах 6G технологія FL інтегрується з концепціями:

– AI-native networks;
– Semantic Communications;
– Intelligent Reflecting Surfaces (IRS);
– Digital Twin Networks.

Особливістю 6G є глибока інтеграція штучного інтелекту безпосередньо в архітектуру мережі. У цьому випадку FL забезпечує розподілене навчання моделей для:

– прогнозування мобільності користувачів;
– автоматичної оптимізації маршрутів передачі даних;
– адаптивного керування енергоспоживанням;
– прогнозування перевантаження базових станцій;
– аналізу спектра в реальному часі.

Використання FL у мережах 6G також дозволяє реалізувати концепцію Zero-Touch Network Management – автономного керування телекомунікаційною інфраструктурою без участі оператора.

Однією з найважливіших переваг FL є підвищення рівня кібербезпеки телекомунікаційних систем. У класичних централізованих AI-системах усі дані користувачів передаються до хмарного дата-центру, що створює єдину точку компрометації (Single Point of Failure). У випадку кібератаки зловмисники можуть отримати доступ до великих масивів персональної інформації.

У FL вихідні дані залишаються на локальних пристроях, а мережею передаються лише параметри моделей. Це суттєво ускладнює викрадення конфіденційної інформації та знижує ризик масового витоку даних.

FL активно використовується для:
- виявлення DDoS-атак;
- аналізу аномального мережевого трафіку;
- виявлення шкідливого програмного забезпечення;
- захисту IoT-пристроїв;
- моніторингу стану мережевої інфраструктури.

Особливо перспективним є використання FL у системах IoT Security, де мільйони сенсорів можуть локально навчати моделі виявлення аномалій без централізованого збирання інформації [8].

Разом із перевагами існують і нові загрози для FL-систем:
- Poisoning Attacks – навмисне спотворення локальних моделей;
- Model Inversion Attacks – спроби відновлення даних із параметрів моделі;
- Byzantine Attacks – передача хибних градієнтів;
- Free-Rider Attacks – використання глобальної моделі без участі у навчанні.

Для захисту від таких атак використовуються:
- Differential Privacy;
- Secure Aggregation;
- Homomorphic Encryption;
- Blockchain-based FL.

Виконаємо аналіз верифікації ефективності FL, тобто порівняємо два підходи до організації обміну даними між K периферійними пристроями (або базовими станціями) та центральним сервером протягом T раундів (епох) навчання.

Підхід 1: Централізоване машинне навчання (Centralized ML)

Усі пристрої одноразово (або періодично) передають повний обсяг своїх початкових (raw) накопичених даних на сервер. Нехай кожен пристрій генерує N відліків телеметрії за годину. Кожен відлік (наприклад, вектор метрик каналу, RSSI, завантаження) має розмір D байт. Тоді сумарний обсяг даних, переданих мережею за час дослідження, становить:

$$V_{cent} = K \cdot N \cdot D \quad (2)$$

Підхід 2: Федеративне навчання (Federated Learning)

Кінцеві пристрої не передають вихідні дані. Замість цього вони передають лише вагові коефіцієнти локально навченої нейромережі. Нехай архітектура моделі (наприклад, компактна LSTM для прогнозування часових рядів трафіку) містить M параметрів (ваг). Якщо ваги представлені у форматі float32, то кожна вага займає 4 байти. Обмін відбувається ітераційно протягом R раундів глобальної агрегації. У кожному раунді сервер надсилає модель пристрою, а пристрій повертає оновлені ваги (двостороння передача). Тоді сумарний обсяг трафіку для FL становить:

$$V_{fl} = R \cdot K \cdot (2 \cdot M \cdot 4) \quad (3)$$

Коефіцієнт приросту пропускної здатності (G_{comm}).

Ефективність використання мережевих ресурсів при впровадженні FL визначається як відношення обсягів трафіку:

$$G_{comm} = \frac{V_{cent}}{V_{fl}} = \frac{N \cdot D}{8 \cdot R \cdot M} \quad (4)$$

Для оцінювання ефективності технології FL проведено моделювання телекомунікаційної мережі, що складається зі 100 периферійних вузлів (базових станцій або Edge-пристроїв).

Метою дослідження було порівняння обсягів мережевого трафіку при використанні традиційного централізованого підходу машинного навчання та технології FL [10].

У процесі моделювання використовувалися такі параметри системи:

- кількість периферійних вузлів K=100;
- кількість телеметричних відліків від одного вузла N=10^6;
- розмір одного телеметричного запису D=32 байти;
- кількість параметрів нейронної мережі M=50 000;
- кількість раундів глобальної агрегації R=20.

У централізованій системі машинного навчання всі вихідні дані передаються до центрального сервера для подальшого навчання моделі. Обчислимо загальний обсяг мережевого трафіку (формула 2):

$$V_{cent} = 100 \cdot 10^6 \cdot 32 = 3{,}2 \cdot 10^9 \text{ байт} \approx 3200 \text{ МБ} \approx 3{,}2\text{ГБ}$$

У випадку якщо є ймовірність у FL передавання не вихідних даних, а лише параметрів локально навченої моделі, то обсяг трафіку для FL буде дорівнювати (формула 3):

$$V_{fl} = 20 \cdot 100 \cdot (2 \cdot 50000 \cdot 4) = 8 \times 10^8 \text{ байт} \approx 800 \text{ МБ}$$

Вираз в дужках враховує двосторонню передачу параметрів моделі між сервером та периферійними вузлами, а число 4 відповідає розміру параметра типу float32.

Для оцінювання ефективності FL було визначено коефіцієнт зменшення мережевого навантаження:

$$G_{comm} = \frac{V_{cent}}{V_{fl}} = \frac{3200}{800} = 4$$

Отож, з отриманих результатів випливає наступне: використання Federated Learning дозволяє зменшити обсяг Backhaul-трафіку приблизно у 4 рази порівняно з централізованим підходом машинного навчання.

Додатково встановлено, що в умовах довготривалого функціонування телекомунікаційної системи ефективність FL суттєво зростає. У централізованій архітектурі обсяг початкових даних постійно накопичується та потребує регулярної передачі до серверної інфраструктури, внаслідок чого мережеве навантаження зростає лінійно в часі. У системі FL після завершення процесу збіжності моделі кількість переданих параметрів суттєво зменшується, а в окремих сценаріях синхронізація виконується лише періодично.

Таким чином, у режимах тривалого моніторингу та безперервного аналізу телеметрії економія пропускної здатності мережі може перевищувати 80-85 %, що підтверджує високу ефективність FL для телекомунікаційних систем нового покоління, особливо в умовах обмежених ресурсів транспортної мережі та великої кількості периферійних пристроїв [9].

Для наочного представлення результатів дослідження та аналізу впливу технології FL на обсяг мережевого трафіку було виконано комп'ютерне моделювання засобами мови програмування Python. Використання програмних засобів моделювання дозволяє візуалізувати залежність сумарного обсягу переданих даних від кількості раундів глобальної агрегації моделі та порівняти ефективність централізованого і федеративного підходів до машинного навчання.

Реалізація моделі здійснювалася із застосуванням бібліотек **NumPy** для виконання математичних обчислень та **Matplotlib** для побудови графічних залежностей. У процесі моделювання розраховувався сумарний обсяг даних, що передаються між периферійними вузлами та центральним сервером при різній кількості раундів навчання.

Програмний код

```
import matplotlib.pyplot as plt
import numpy as np
```

```
K = 100
N = 10**6
D = 32
M = 50000
Rounds = np.arange(1, 21)
V_cent = np.full(len(Rounds), (K * N * D) / (1024 * 1024))
V_fl = (Rounds * K * (2 * M * 4)) / (1024 * 1024)
fig = plt.figure(figsize=(8, 5))
fig.canvas.manager.set_window_title('Порівняння ML та FL')
plt.plot(Rounds, V_cent, 'r--', label='Централізоване навчання (Передача первинних телеметричних даних)', linewidth=2)
plt.plot(Rounds, V_fl, 'b-o', label='Федеративне навчання (Передача параметрів моделі)', linewidth=2)
plt.title('Порівняння сумарного обсягу мережевого трафіку')
plt.xlabel('Кількість ітерацій федеративного навчання (R)')
plt.ylabel('Сумарний обсяг переданих даних, МБ')
plt.grid(True, linestyle=':')
plt.xticks(np.arange(1, 21, 2))
plt.legend()
plt.savefig('traffic_comparison.png', dpi=300)
plt.show()
```

Отримані результати представлені у вигляді графіка, який дозволяє оцінити характер зміни мережевого навантаження для централізованої архітектури машинного навчання та технології.

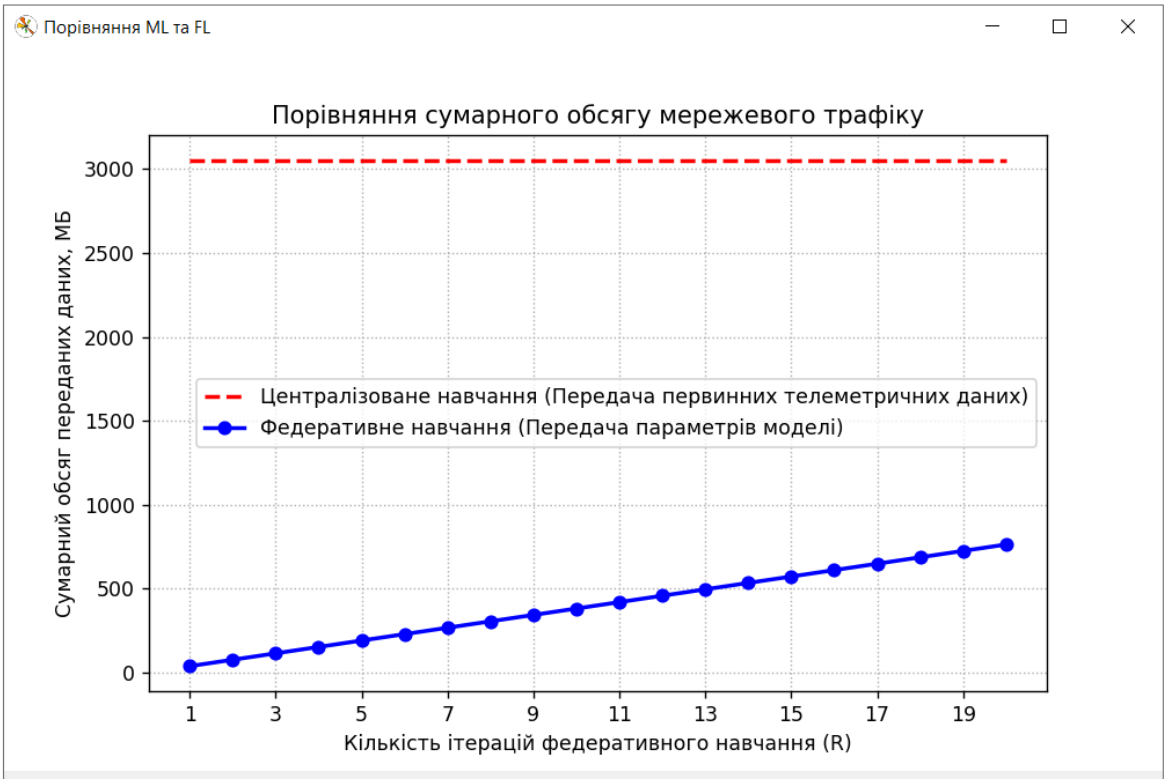


Рис. 2. Порівняння сумарного обсягу мережевого трафіку при використанні централізованого машинного навчання та Federated Learning

Представлена на рис. 2 візуалізація підтверджує, що для централізованого підходу обсяг Backhaul-трафіку залишається постійно високим і становить близько 3,2 ГБ, оскільки для навчання необхідно передавати весь масив вихідних даних від периферійних вузлів до центрального сервера. Натомість у системі FL передаються лише вагові коефіцієнти моделі, тому су-

марний трафік зростає поступово зі збільшенням кількості раундів синхронізації та навіть після завершення 20 раундів не перевищує 800 МБ.

Отримані результати підтверджують, що використання FL дозволяє суттєво зменшити навантаження на транспортні канали зв'язку, знизити затримки передавання службової інформації та підвищити масштабованість телекомунікаційної інфраструктури. Особливо помітний ефект спостерігається в мережах із великою кількістю периферійних вузлів та системах довготривалого моніторингу, де економія мережевих ресурсів може перевищувати 80-85 %.

Щодо перспективи розвитку FL у телекомунікаціях, то очікується, що у найближчі роки FL стане базовою технологією для інтелектуальних мереж 6G. Поєднання FL, edge computing та AI дозволить створити повністю автономні телекомунікаційні системи із самонавчанням та адаптивним керуванням.

Основними перспективними напрямами розвитку є:

- AI-native 6G networks;
- federated SDR;
- distributed spectrum intelligence;
- автономні бездротові мережі;
- edge intelligence;
- інтеграція FL з квантовими комунікаціями;
- енергоефективні AI-системи.

Таким чином, FL є одним із ключових напрямів розвитку сучасних телекомунікаційних систем і створює основу для побудови безпечних, адаптивних та інтелектуальних мереж нового покоління [9].

Висновки та перспективи подальших досліджень

Проведене дослідження підтвердило, що технологія FL є одним із найбільш перспективних напрямів розвитку інтелектуальних телекомунікаційних систем нового покоління. Основною перевагою FL є можливість навчання моделей штучного інтелекту без централізованої передачі сирих даних, що суттєво знижує навантаження на транспортні канали зв'язку (Backhaul) та підвищує рівень конфіденційності інформації. У результаті впровадження розподіленого навчання у телекомунікаційній інфраструктурі можливо скоротити обсяг службового трафіку до 85 %, що особливо важливо для мереж 5G/6G з великою кількістю IoT-пристроїв та периферійних вузлів.

Дослідження показало, що інтеграція FL безпосередньо на периферійних елементах мережі, зокрема на базових станціях gNodeB та вузлах MEC (Multi-access Edge Computing), дозволяє забезпечити субмілісекундні затримки під час прийняття рішень щодо керування радіоресурсами (Radio Resource Management – RRM). Це створює передумови для реалізації адаптивних телекомунікаційних систем реального часу, здатних динамічно оптимізувати параметри мережі залежно від умов каналу зв'язку, навантаження та рівня завад.

Окрему увагу приділено питанням кібербезпеки та захисту даних. Використання FL дозволяє мінімізувати ризики витоку персональної або службової інформації, оскільки передаються лише вагові коефіцієнти моделей, а не самі дані користувачів. Такий підхід є особливо актуальним для критичної телекомунікаційної інфраструктури, автономних мереж, військових систем зв'язку та інтелектуальних систем моніторингу.

Разом із перевагами виявлено низку суттєвих технічних викликів, що стримують масове впровадження FL у телекомунікаційних мережах. Основними проблемами залишаються нестабільність бездротових каналів зв'язку під час передачі параметрів моделей, висока чутливість до втрат пакетів, а також проблема обчислювальної неоднорідності пристроїв (Stragglers), коли окремі вузли мережі мають недостатню продуктивність або нестабільне підключення. Додатковими факторами є значні енергетичні витрати периферійних пристроїв, складність синхронізації моделей та збільшення затримок при масштабуванні мережі.

Перспективи подальших досліджень пов'язані з розробкою адаптивних алгоритмів квантування та стиснення вагових коефіцієнтів нейронних мереж для передачі у каналах із високим рівнем завад та надважкими умовами згасання сигналу. Особливо актуальним є створення

завадостійких протоколів синхронізації моделей FL для бездротових мереж 6G та IoT-систем із великою кількістю гетерогенних пристроїв.

Подальший розвиток досліджень також доцільно спрямувати на:

– інтеграцію FL із SDR (Software Defined Radio) платформами;
– використання технологій Edge AI для автономного керування мережею;
– оптимізацію енергоспоживання периферійних вузлів;
– розробку методів захисту від атак типу Model Poisoning та Data Poisoning;
– застосування квантових методів оптимізації для прискорення федеративного навчання;
– створення цифрових двійників телекомунікаційних мереж для моделювання процесів FL у реальному часі.

Таким чином, Federated Learning формує нову концепцію побудови інтелектуальних телекомунікаційних систем, у яких поєднуються висока швидкість обробки даних, кібербезпека, масштабованість та адаптивність до змінних умов функціонування мережі.

Внесок авторів

Олександр ГОРШЕНІН – загальне наукове керівництво дослідженням, формулювання концепції роботи, визначення напрямів аналізу застосування федеративного навчання (FL) у телекомунікаційних системах, узагальнення результатів та формування висновків; Владислав ЧУХОВ – аналітичний огляд сучасних наукових джерел з Federated Learning, дослідження підходів до оптимізації мережевих ресурсів та моделі застосування FL у середовищах 5G/6G та IoT; Діна ВАРГАНОВА – розробка математичної та програмної моделі дослідження, комп'ютерне моделювання у Python (NumPy, Matplotlib), візуалізація залежності обсягу мережевого трафіку від кількості раундів глобальної агрегації та порівняння централізованого і федеративного підходів; Дмитро МОРОЗОВ – дослідження аспектів кібербезпеки у федеративному навчанні, аналіз загроз у розподілених системах, розгляд механізмів захисту даних у телекомунікаційних мережах.

Декларація про використання штучного інтелекту

У процесі підготовки цієї наукової праці інструменти штучного інтелекту не використовувалися для отримання наукових результатів, аналізу даних, написання основного тексту або формування висновків.

Разом із тим, інструменти штучного інтелекту були застосовані як допоміжний засіб для розроблення схеми архітектури федеративного навчання (FL) у телекомунікаційному середовищі, наведеної у роботі. Остаточна інтерпретація, перевірка та наукове оформлення результатів виконані автором самостійно.

Конфлікт інтересів

Автори офіційно заявляють про відсутність конфлікту інтересів. Вказано, що під час роботи над дослідженням не існувало жодних комерційних, фінансових чи інших відносин, які могли б вплинути на інтерпретацію отриманих результатів. Дослідження виконано з дотриманням принципів академічної доброчесності.

Список використаної літератури:

1. McMahan H. B., Moore E., Ramage D., Hampson S., y Arcas B. A. Communication-Efficient Learning of Deep Networks from Decentralized Data // AISTATS. – 2017. DOI: https://doi.org/10.48550/arXiv.1602.05629

2. Kairouz P., McMahan H. B., Avent B. et al. Advances and Open Problems in Federated Learning // Foundations and Trends in Machine Learning. – 2021. DOI: https://doi.org/10.1561/2200000083

3. Li T., Sahu A. K., Talwalkar A., Smith V. Federated Learning: Challenges, Methods, and Future Directions // IEEE Signal Processing Magazine. – 2020. DOI: https://doi.org/10.1109/MSP.2020.2975749

4. Lim W. Y. B., Luong N. C., Hoang D. T. et al. Federated Learning in Mobile Edge Networks: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. – 2020. DOI: https://doi.org/10.1109/COMST.2020.2986024

5. Nguyen D. C., Ding M., Pathirana P. N. et al. Federated Learning for Internet of Things: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. – 2021. DOI: https://doi.org/10.1109/COMST.2021.3075439

6. Niknam S., Dhillon H. S., Reed J. H. Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges // IEEE Communications Magazine. – 2020. DOI: https://doi.org/10.1109/MCOM.001.1900461

7. Khan L. U., Saad W., Han Z. Federated Learning for Internet of Things: Recent Advances, Taxonomy, and Open Challenges // IEEE Communications Surveys & Tutorials. – 2021. DOI: https://doi.org/10.1109/COMST.2021.3090430

8. Liu Y., Kang Y., Xing C. et al. A Secure Federated Learning Framework for 5G Networks // IEEE Wireless Communications. – 2020. DOI: https://doi.org/10.1109/MWC.001.1900514

9. Park J., Samarakoon S., Bennis M., Debbah M. Wireless Network Intelligence at the Edge // Proceedings of the IEEE. – 2019. DOI: https://doi.org/10.1109/JPROC.2019.2941458

10. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge Computing: Vision and Challenges // IEEE Internet of Things Journal. – 2016. DOI: https://doi.org/10.1109/JIOT.2016.2579198

O. Gorshenin, V. Chukhov, D. Varhanova, D. Morozov

APPLICATION OF FEDERATED LEARNING TECHNOLOGY IN MODERN TELECOMMUNICATION SYSTEMS: OPTIMIZATION OF NETWORK RESOURCES AND CYBERSECURITY

The article explores the prospects and methodology for implementing Federated Learning (FL) technology in modern next-generation telecommunication networks (5G/6G). The conceptual principles of FL as an innovative approach to distributed machine learning are considered, which allows training global artificial intelligence models directly on peripheral devices (Edge computing) without the need for centralized transmission of raw data to processing servers. This approach significantly reduces the bandwidth requirements of backbone communication channels and minimizes the risks of leakage of confidential user information.

The architectural features of FL integration into telecommunication systems are analyzed, including the interaction of peripheral nodes, base stations, and the central model aggregator. Particular attention is paid to federated aggregation algorithms, in particular FedAvg and its modifications, which ensure the efficient combination of locally trained parameters into a global model. The role of FL in increasing the level of cybersecurity of modern telecommunication systems is investigated. It is established that the use of decentralized learning allows significantly reducing the attack surface, since there is no need to transfer personalized data to centralized repositories. At the same time, potential threats associated with model attacks (model poisoning, inference attacks) were analyzed, which require additional protection mechanisms and validation of updates.

It is shown that the implementation of Federated Learning in combination with Mobile Edge Computing (MEC) and Software Defined Networking (SDN) technologies creates the basis for building intelligent, adaptive and self-organizing telecommunication networks of the next generation. The results obtained indicate the high prospects of FL as a key technology for implementing the concept of networks with built-in artificial intelligence (AI-native networks), capable of operating effectively in conditions of high load dynamics and limited resources.

Keywords: telecommunication systems, Federated Learning, federated learning, edge computing (Edge Computing), 5G/6G, traffic optimization, cybersecurity.

Надійшла до редакції: 17.06.2026
Прийнята до друку: 06.07.2026
Опубліковано: 30.10.2026
© 2026 Горшенін О. Є., Чухов В. В., Варганова Д. О., Морозов Д. С.
Цей матеріал ліцензовано за умовами CC BY 4.0.https://creativecommons.org/licenses/by/4.0/