ВСТУП

Стрімкий розвиток інфокомунікаційних систем, поява сервісів з високими вимогами до швидкодії та стабільності, а також масштабування мережевої інфраструктури створюють принципово нові умови для організації процесів передачі інформації. Збільшення кількості користувацьких та машинних з'єднань, поява трафіку з різними профілями навантаження й підвищення чутливості до затримок формують середовище, у якому традиційні підходи до управління мережею поступово втрачають результативність. У таких умовах актуальною стає потреба у впровадженні інтелектуальних технологій моніторингу, здатних адаптуватися до динамічних змін стану мережі та приймати оптимальні рішення в реальному часі.

Сучасні методи оброблення даних на основі глибинного навчання й алгоритмів навчання з підкріпленням відкривають можливість побудови моделей, що забезпечують гнучку реакцію на зміну параметрів середовища. Зокрема, моделі типу Deep Q-Network дозволяють формувати політики поведінки агента на основі накопиченого досвіду, що робить їх придатними для завдань оптимізації розподілу ресурсів, маршрутизації чи вибору параметрів передавання інформації. Паралельно з цим рекурентні нейронні мережі, зокрема архітектури LSTM, демонструють високу ефективність під час аналізу показників якості користувацького досвіду, що мають часову структуру та залежать від попередніх станів мережі.

Поєднання цих двох класів моделей формує перспективний напрямок розвитку інтелектуальних систем управління телекомунікаційними процесами. Водночас на практиці залишається низка невирішених завдань: узгодження роботи моделей, визначення адекватного представлення станів мережі, дослідження стійкості алгоритмів у змінних умовах та оцінка їх впливу на якість обслуговування. Дослідження цих аспектів є важливим як для модернізації комунікаційної інфраструктури, так і для проєктування систем, здатних забезпечувати гарантовані рівні QoE за умов нерівномірних навантажень та непередбачуваних мережевих подій.

Актуальність роботи зумовлена стрімким розвитком цифрових технологій та зростанням вимог до швидкості, надійності й безпеки інформаційного обміну. Сучасні інфокомунікаційні системи стикаються з проблемами збільшення обсягів даних, ускладнення мережевих архітектур та необхідністю автоматизованого управління процесами передачі інформації. Використання алгоритмів штучного інтелекту є одним із ключових напрямів підвищення ефективності таких систем, оскільки дозволяє оптимізувати маршрутизацію, прогнозувати навантаження, забезпечувати адаптивне керування та зменшувати затримки в мережі. Інтелектуальні методи також відіграють важливу роль у забезпеченні кібербезпеки, виявленні аномалій і підвищенні стійкості мереж до зовнішніх впливів.

Таким чином, дослідження методів інтеграції ШІ у системи передачі інформації є актуальним і своєчасним, оскільки сприяє створенню більш ефективних, безпечних та масштабованих телекомунікаційних рішень, здатних відповідати сучасним та майбутнім викликам галузі.

Запропонований підхід передбачає інтеграцію моделі DQN як модуля прийняття рішень та гібридної моделі LSTM + Dense для оцінювання якості, що забезпечує одночасний аналіз поточного стану мережі, прогнозування її поведінки та адаптивну зміну параметрів функціонування. Це дозволяє сформувати інтелектуальну систему самооптимізації, яка підвищує ефективність використання ресурсів, мінімізує деградацію якості обслуговування та забезпечує стабільність у складних динамічних.

Мета роботи: дослідження методів побудови системи передачі інформації із застосуванням штучного інтелекту, спрямоване на визначення оптимальних підходів до інтеграції алгоритмів ШІ в інфокомунікаційних системах з метою підвищення їх ефективності, надійності та адаптивності.

Об’єкт дослідження: процес передачі інформації в інфокомунікаційних системах, включаючи механізми маршрутизації, розподілу ресурсів, забезпечення якості обслуговування та адаптивного управління мережевими процесами за допомогою алгоритмів штучного інтелекту.

Предмет дослідження: методи та алгоритми побудови системи передачі інформації із застосуванням штучного інтелекту.

РОЗДІЛ 1 СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

1.1 Теоретичні основи систем передачі інформації

Система передачі інформації є ключовим елементом будь-якої інфокомунікаційної інфраструктури. Її основна функція полягає у забезпеченні надійного, ефективного й точного передавання даних між джерелом повідомлення та приймачем. У сучасному інформаційному суспільстві такі системи становлять основу для функціонування глобальних мереж, мобільного зв’язку, Інтернету речей та систем керування критичною інфраструктурою.

Теоретичні засади передачі інформації були сформульовані у середині XX століття завдяки працям Клода Шеннона, який у своїй класичній роботі «A Mathematical Theory of Communication» заклав основи кількісного вимірювання інформації та визначив межі її ефективної передачі. Саме ця праця започаткувала інформаційну теорію, яка стала базовим інструментом для розробки сучасних систем зв’язку.

Згідно з моделлю Шеннона, яка зображена на рисунку 1.1, система передачі інформації складається з п’яти основних компонентів.



Рис. 1.1 Класична модель системи передачі інформації

У такій моделі головне завдання полягає в тому, щоб інформація, сформована джерелом, максимально точно відтворювалася на приймальній стороні, незважаючи на вплив шумів, завад, інтерференції та обмежень каналу.

Розвиток інформаційних технологій у XXI столітті значно розширив розуміння цих принципів. Сучасні системи передачі даних поєднують цифрову обробку сигналів, оптичні технології, безпроводові протоколи та адаптивні алгоритми управління якістю сервісу. У багатьох з них уже впроваджено елементи штучного інтелекту, які дозволяють прогнозувати стан каналу, виявляти аномалії та автоматично налаштовувати параметри передачі для досягнення оптимальної ефективності.

Таким чином, вивчення теоретичних основ систем передачі інформації залишається актуальним, оскільки ці знання є фундаментом для розроблення інтелектуальних систем зв'язку нового покоління, у яких класичні принципи теорії інформації поєднуються з алгоритмами машинного навчання.

Основні поняття та структура системи передачі інформації [1]

Система передачі інформації — це комплекс технічних, програмних та організаційних засобів, призначених для кодування, передачі, приймання і відновлення повідомлень між віддаленими об'єктами. В узагальненому вигляді її можна подати схемою зображеною на рисунку 1.1.

У цій структурі кожен елемент виконує свою функцію:

- джерело створює інформаційне повідомлення;
- передавач формує сигнал і кодує дані;
- канал передає інформацію;
- приймач декодує сигнал, усуває спотворення;
- одержувач сприймає результат і використовує отриману інформацію.

Математично процес передачі сигналу можна описати рівнянням:

$$y(t) = x(t) + n(t) \tag{1.1}$$

де: *x(t)* — переданий сигнал *y(t)* — прийнятий сигнал, *n(t)* — шум або завада, що додається під час передачі. Завдання системи — відновити x(t) із максимально можливою точністю, зважаючи на вплив n(t).

Інформація, ентропія та кількість даних [2]

Однією з основних категорій інформаційної теорії є поняття ентропії, яке характеризує міру невизначеності джерела повідомлень. Шеннон визначив кількість інформації, що міститься у повідомленні, за формулою:

$$I(x) = -log_2 p(x) \tag{1.2}$$

p(x) — імовірність появи конкретного повідомлення x.

Середня кількість інформації, або ентропія джерела, розраховується як:

$$H(X) = -\sum_{i=1}^{n} p(x_i) log_2 p(x_i) \tag{1.3}$$

Ця величина визначає середню кількість бітів, необхідних для подання одного повідомлення. Ентропія є мірою ефективності кодування: чим вона більша, тим більше інформації несе повідомлення і тим складніше здійснити стиснення без втрат.

З позицій теорії зв'язку, метою проектування систем передачі інформації є досягнення рівноваги між пропускною здатністю каналу, надійністю передачі та енергоспоживанням. На практиці це досягається за допомогою оптимального вибору методів модуляції, кодування та управління потоком даних.

Канал зв'язку та його параметри [3]

Канал зв'язку є фізичним або логічним середовищем, через яке здійснюється передача сигналу. Він може бути проводовим, безпроводовим, або комбінованим. Кожен канал має свої характеристики — смугу пропускання, затримку, коефіцієнт завадостійкості та ймовірність помилки передачі.

Одним із базових показників каналу є пропускна здатність — максимальна швидкість передавання інформації без помилок при даному співвідношенні сигнал/шум. Вона визначається за формулою Шеннона для каналу з адитивним білим гаусовим шумом:

$$C = Blog_2(1 + \frac{S}{N}) \tag{1.4}$$

де: *C* — пропускна здатність, біт/с;

B — смуга пропускання каналу, Гц;

$\frac{S}{N}$ — відношення потужності сигналу до потужності шуму.

Ця залежність показує, що збільшення потужності сигналу або розширення смуги пропускання підвищує потенційну швидкість передачі. Проте у реальних системах ці параметри обмежуються фізичними властивостями середовища, енергетичними витратами та вимогами до стабільності зв’язку.

Типи каналів зв’язку

Канали зв’язку поділяють за кількома критеріями, які впливають на їх експлуатаційні властивості та технології передачі сигналів. Одним із головних поділів є класифікація за типом сигналу — аналогу чи цифровому.

Аналогові канали передають безперервні сигнали, що безперервно змінюються у часі та амплітуді, наприклад, традиційні телефонні мережі або радіочастотні канали. Вони піддаються впливу шумів і спотворень, що ускладнює збереження цілісності інформації.

Цифрові канали, натомість, оперують дискретними, бінарними послідовностями, що дозволяє застосовувати методи кодування і корекції помилок для підвищення надійності передачі. [4]

Методи кодування та корекції помилок [5]

Кодування є одним із ключових етапів у системах передачі інформації, оскільки визначає ефективність, швидкість та надійність комунікаційного процесу. Його основне призначення полягає у перетворенні даних у форму, зручну для передавання або зберігання з урахуванням характеристик каналу зв’язку.

У інфокомунікаційних системах виділяють два основних типи кодування:

Кодування джерела — спрямоване на усунення надлишковості інформації без втрати її змісту. Це дозволяє зменшити обсяг передаваних даних і підвищити ефективність використання каналу. До найпоширеніших методів належать коди Хаффмана та арифметичне кодування, що широко використовуються при стисненні текстових, аудіо- та відеоданих.

Кодування каналу — забезпечує підвищення завадостійкості передавання за рахунок додавання контрольних або надлишкових бітів, які дозволяють виявляти та виправляти помилки. Типовими прикладами є коди Хеммінга, турбо-коди та

LDPC-коди, які використовуються у цифрових стандартах Wi-Fi, 4G/5G та супутникових системах зв’язку.

Під час передавання сигналів через реальні канали зв’язку виникають шуми, інтерференції та інші спотворення, що призводять до появи помилок у прийнятих даних. Для мінімізації цих втрат застосовуються методи виявлення та корекції помилок.

До методів виявлення помилок належать:

контрольні суми;

циклічний надлишковий код, який забезпечує високий рівень достовірності контролю при низьких обчислювальних витратах.

Методи корекції помилок дозволяють відновити вихідну інформацію без повторної передачі даних. Найбільш відомими є:

коди Ріда–Соломона — ефективні для виправлення блокових помилок, застосовуються в оптичних і супутникових мережах;

коди Хеммінга — дозволяють виправляти одиночні помилки та виявляти подвійні;

турбо-коди — наближаються до межі пропускної здатності за Шенноном і використовуються у високошвидкісних цифрових каналах;

LDPC-коди — забезпечують високу ефективність і використовуються у сучасних стандартах мобільного та безпроводового зв’язку.

Застосування комплексного підходу до кодування та корекції помилок дозволяє забезпечити високу надійність і стабільність функціонування систем передачі інформації навіть у складних умовах, характерних для сучасних комунікаційних мереж.

Мультиплексування: поняття і основні методи

Мультиплексування — це технологічний процес, який забезпечує передачу декількох незалежних інформаційних потоків через один фізичний канал зв’язку. Такий підхід дозволяє максимально ефективно використовувати пропускну здатність каналу та ресурси мережі.

Існує кілька основних типів мультиплексування, що відрізняються способом розподілу канального ресурсу між потоками даних:

Частотне мультиплексування — передбачає поділ загального спектра частот на окремі піднесучі, кожна з яких закріплюється за конкретним сигналом. Метод широко використовується в аналогових системах зв’язку, зокрема в радіомовленні та кабельному телебаченні.

Часове мультиплексування — полягає у послідовній передачі сигналів у часових інтервалах. Кожен потік отримує свій часовий слот, у межах якого здійснюється передача даних. Такий підхід типовий для цифрових систем, наприклад, у телефонії або транспортних мережах SDH.

Кодове мультиплексування — використовує принцип накладання сигналів за допомогою унікальних кодових послідовностей. Кожен абонент отримує свій код, що дозволяє одночасно передавати кілька сигналів на одній частоті без взаємних перешкод.

Ортогональне частотне мультиплексування — сучасна технологія, що базується на використанні великої кількості піднесучих, які є ортогональними між собою. Кожна піднесуча модулюється окремо, що забезпечує високу стійкість до міжсимвольних інтерференцій. OFDM застосовується в системах Wi-Fi, LTE, 5G та інших стандартах високошвидкісного зв’язку.

Завдяки мультиплексуванню стає можливим одночасне обслуговування багатьох користувачів або сервісів у межах одного фізичного середовища передачі, що істотно підвищує ефективність використання частотного спектра та дозволяє масштабувати комунікаційні системи.

Модуляція та демодуляція [6]

Модуляція являє собою процес перетворення інформаційного сигналу, який зазвичай має низьку частоту або дискретний характер, у форму, що підходить для передачі по конкретному каналу зв’язку. Застосування модуляції дозволяє адаптувати сигнал до особливостей середовища передачі і покращити якість зв’язку.

Основні типи модуляції зображені на рисунку 1.2 та включають:

Амплітудна модуляція, при якій амплітуда несучої хвилі змінюється відповідно до інформаційного сигналу;

Частотна модуляція, що полягає у варіюванні частоти несучого сигналу залежно від інформації;

Фазова модуляція, де інформація кодується зміною фази несучої хвилі.

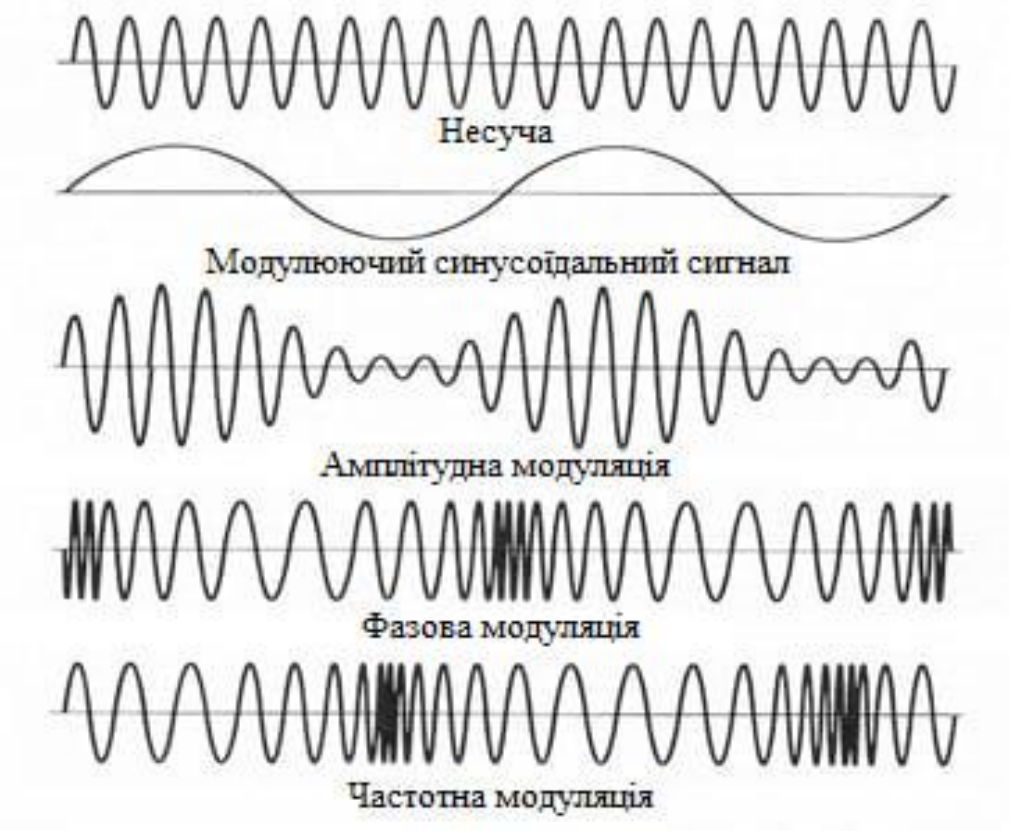
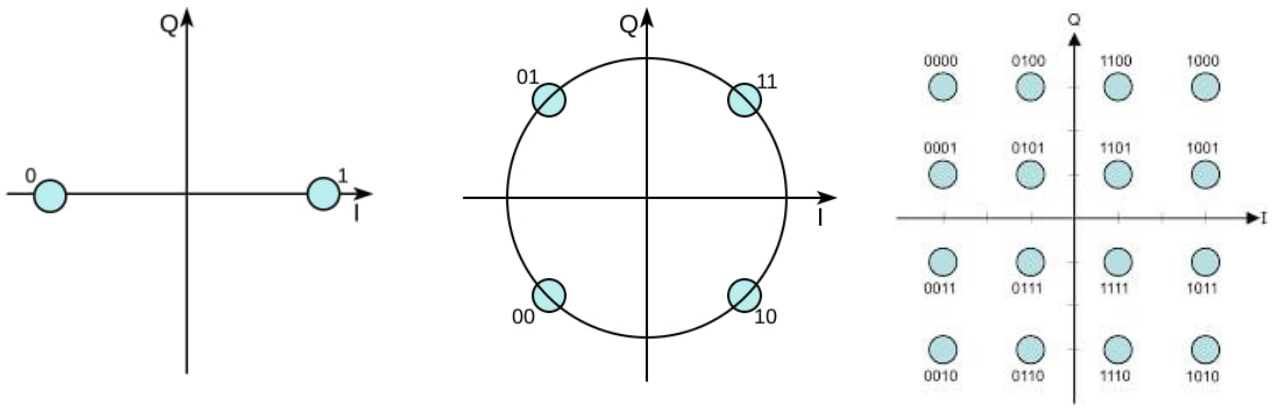


Рис. 1.2 Основні типи модуляції

У цифрових системах передачі інформації використовуються складніші методи модуляції, такі як QPSK, QAM, PSK, які є стандартом у сучасних радіозв’язках і мобільних мережах, принципи їх роботи зображено на рисунку 1.3. [7]

Демодуляція — це процес відновлення вихідного інформаційного сигналу на приймачі шляхом обробки прийнятого модульованого сигналу. Від правильного вибору способу модуляції залежить ефективність передачі, рівень стійкості до шумів та пропускна здатність системи зв’язку.



(а) (б) (в)

Рис. 1.3 Типи цифрової модуляції (а) — BPSK; (б) — QPSK; (в) — 16-QAM.

Практичні аспекти побудови систем передачі [8]

Проєктування систем передачі даних потребує комплексного підходу, який поєднує технічні, організаційні та експлуатаційні рішення. Головною метою є забезпечення стабільної, безперервної та ефективної взаємодії між елементами інфокомунікаційної мережі.

Одним із ключових завдань на етапі проєктування є оптимальне формування структури мережі з урахуванням типу трафіку, необхідної пропускної здатності, затримок передачі та якості обслуговування. Вибір каналів і технічних засобів визначається їхньою стійкістю до завад, швидкістю передачі, топологічною побудовою та економічною ефективністю. Сучасні мережі проєктуються за принципом модульності, що забезпечує масштабованість і спрощує подальшу модернізацію системи без значних структурних змін.

Надійність системи є критичним показником її ефективності. Для її забезпечення застосовуються методи резервування каналів і вузлів, дублювання ключових елементів, балансування навантаження, а також автоматичне перемикання на альтернативні траєкторії передачі під час відмов або збоїв. Додатково впроваджується постійний моніторинг стану каналів і адаптивне керування потоками даних, що мінімізує ризик перевантажень.

Захист інформації займає особливе місце в системах передачі. Для запобігання несанкціонованому доступу застосовуються методи шифрування, автентифікації користувачів, контроль політик доступу та інструменти виявлення вторгнень. Особливу увагу приділяють безпеці службових каналів і протоколів керування мережею, адже їх компрометація може призвести до системних збоїв.

Важливою характеристикою ефективної системи є здатність адаптуватися до змін умов середовища. Для цього використовуються алгоритми динамічного налаштування параметрів передачі — потужності сигналу, типу модуляції, ширини смуги частот тощо. Такий підхід дозволяє підтримувати оптимальну продуктивність при мінімальному енергоспоживанні.

У сучасних системах дедалі активніше впроваджуються технології інтелектуального керування на основі машинного навчання. Вони забезпечують прогнозування перевантажень, оптимізацію маршрутів трафіку, своєчасне виявлення аномалій та підвищення загальної надійності мережі.

1.2 Сучасні технології та тенденції розвитку систем передачі інформації

Сучасні системи передачі інформації зазнають глибокої трансформації, викликаної стрімким зростанням обсягів даних, появою нових сервісів і дедалі вищими вимогами до продуктивності та надійності. Мережі вже не просто забезпечують канал для передавання даних — вони перетворюються на надскладні, багаторівневі системи, здатні оперативно адаптуватися до змін навантаження та специфіки підключень. Ці трансформації диктують необхідність інтелектуального підходу до управління, який виходить за межі класичних моделей.

Оптоволоконні системи становлять основу магістральної інфраструктури завдяки їхній високій пропускній здатності і низьким втратам. Сучасні мережі активно використовують DWDM, що дозволяє мультиплексувати десятки або сотні каналів на різних довжинах хвиль. Завдяки цьому на одному волоконі можна передавати дуже великі обсяги даних паралельно.

Однією з ключових переваг є висока гнучкість системи: завдяки реконфігурованим мультиплексорам оператори можуть додавати нові канали або перенаправляти існуючі без необхідності зупинки мережі, що забезпечує більш адаптивну і масштабовану інфраструктуру.

Дослідницькі результати демонструють, що можливості DWDM-систем зростають: наприклад, є експериментальні результати передачі 56,5 Тб/с через 96,5 км стандартного одномодової оптики за допомогою WDM та високоефективної модуляції.

Однак, з ростом кількості каналів та швидкостей управління такими мережами ускладнюється. Для підтримки ефективної роботи DWDM-мереж важливо здійснювати прогнозування навантажень, контролювати якість оптичного сигналу та автоматично коригувати параметри системи.

Мобільні комунікаційні мережі зазнають суттєвих змін, які відповідають загальним тенденціям розвитку сучасних систем передачі даних. Впровадження технології п’ятого покоління не лише забезпечує підвищену швидкість передачі інформації, але й встановлює новий підхід до організації послуг — концепцію «сервісу на вимогу». В рамках цієї концепції розрізняють три основні типи сервісів, які орієнтовані на різні потреби та сценарії застосування: [9]

eMBB — цей тип послуг забезпечує надвисоку пропускну здатність, необхідну для роботи сучасних мультимедійних додатків, зокрема потокового відео у високій роздільній здатності, а також технологій віртуальної та доповненої реальності;

mMTC — спрямований на масове підключення великої кількості пристроїв Інтернету речей, що потребують ефективної та енергоощадної передачі малих обсягів даних;

URLLC — гарантує надзвичайно надійний зв’язок з дуже низькою затримкою, що є критичним для застосувань, таких як автономні транспортні засоби, промислова автоматизація та медичні дистанційні операції.

Досягнення високої ефективності в кожному з цих напрямків стало можливим завдяки впровадженню низки передових технологій.

Massive MIMO, структура якого зображена на рисунку 1.4, використовує велику кількість антен на базових станціях, що дає змогу одночасно обслуговувати велику кількість користувачів і значно підвищувати спектральну ефективність мережі. [10]

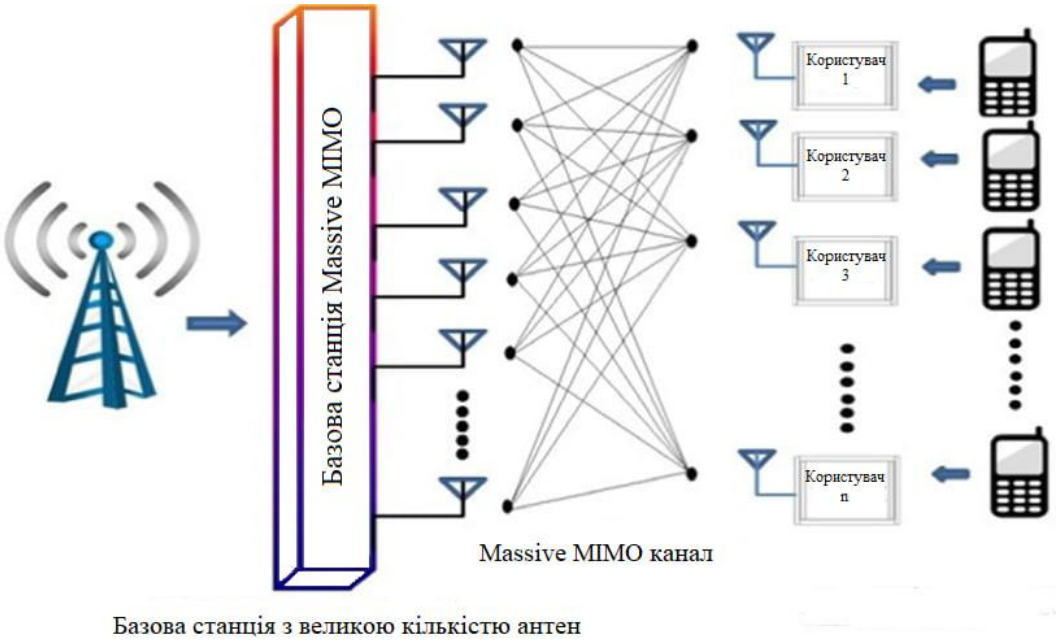


Рис. 1.4 Структура технології Massive MIMO

Технологія beamforming, схематичне зображення роботи якої зображене на рисунку 1.5, забезпечує спрямування радіосигналу безпосередньо до конкретного пристрою, що дозволяє зменшити рівень перешкод і поліпшити якість зв’язку. [11]

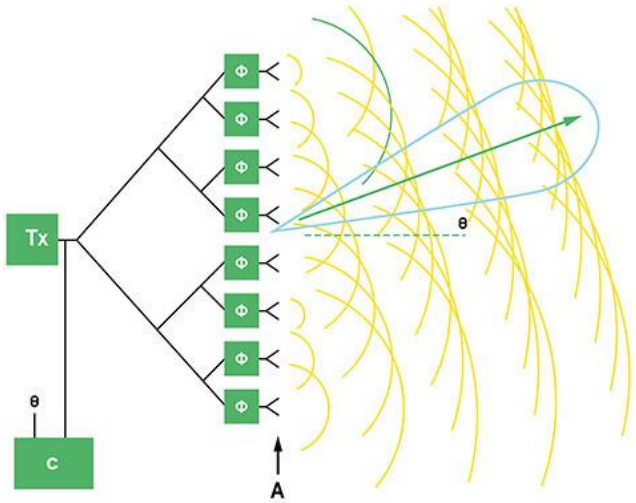


Рис. 1.5 Схематичне зображення роботи технології beamforming

Крім того, адаптивна модуляція і кодування дають можливість динамічно змінювати параметри передачі залежно від поточних умов каналу, що сприяє оптимальному співвідношенню між швидкістю передачі та стабільністю сигналу.

Network slicing є однією з ключових технологічних парадигм, що визначають еволюцію мобільних мереж п’ятого та наступних поколінь. Її концепція зображена на рисунку 1.6 ґрунтується на можливості створення множини ізольованих логічних підмереж, побудованих поверх спільної фізичної інфраструктури оператора зв’язку. Кожен такий мережевий «зріз» має власні характеристики продуктивності, безпеки, пріоритетності та граничних параметрів обслуговування, що дозволяє забезпечувати диференційований доступ до ресурсів залежно від задачі або сервісної моделі. На відміну від класичної мережі, яка пропонує однакові функціональні можливості всім користувачам, network slicing формує динамічне багатошарове середовище, у якому інфокомунікаційні ресурси розподіляються з високою точністю і з урахуванням конкретних вимог застосувань. [12]

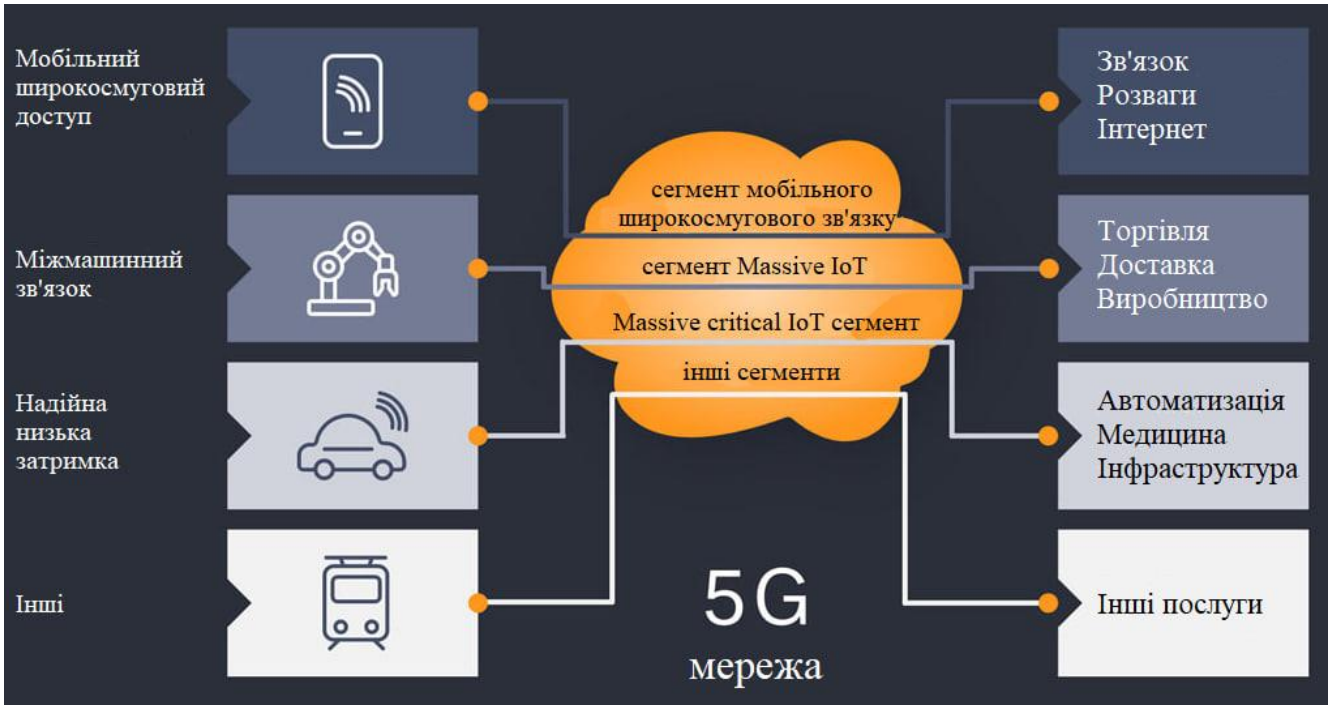


Рис. 1.6 Структура Network slicing

Технологічні передумови реалізації network slicing виникли у зв’язку з істотним зростанням гетерогенності трафіку, появою критично важливих сервісів, швидким розширенням екосистеми Інтернету речей і підвищенням вимог до

гнучкості мережевої інфраструктури. Традиційні механізми управління трафіком, засновані на статичному плануванні, вже не здатні забезпечувати оптимальне функціонування такої складної системи. Відтак виникла необхідність у переході до програмно-керованих архітектур, які допускають оперативне перепрофілювання ресурсів та адаптацію до змінного навантаження. Саме тому network slicing тісно інтегрований з двома фундаментальними технологіями: SDN та NFV, які забезпечують необхідну гнучкість, масштабованість і керованість.

SDN — програмно-конфігуровані мережі. У рамках архітектури SDN управління мережею здійснюється централізованим контролером, що відокремлює рівень управління від рівня пересилання даних. Це дозволяє не лише спростити процес планування ресурсів, але й у режимі реального часу змінювати параметри маршрутизації, балансування навантаження та політики доступу. Завдяки SDN кожен зріз мережі отримує можливість формувати власну логіку взаємодії з фізичною інфраструктурою, не впливаючи на роботу інших сегментів. Контролер, у свою чергу, координує розподіл ресурсів між зрізами, враховуючи їхні поточні потреби та пріоритетність. Основні переваги використання SDN наведені на рисунку 1.7.



Рис. 1.7 Переваги SDN

NFV — віртуалізація мережевих функцій, доповнює цю архітектуру, переводячи традиційні мережеві функції — маршрутизатори, комутатори, шлюзи, міжмережеві екрани, системи керування доступом — із апаратного середовища у програмне. Завдяки цьому функції можуть розгортатися на стандартних серверних платформах у формі віртуальних машин або контейнерів, масштабуватися відповідно до навантаження та швидко мігрувати між обчислювальними вузлами, що надає низку переваг зображену на рисунку 1.8.



Рис. 1.8 Переваги NFV

Поєднання SDN і NFV дає змогу забезпечити повну ізоляцію зрізів, налаштовувати їх на різних рівнях мережевої моделі та оперативно змінювати конфігурацію без фізичного втручання у топологію.

Стратегічна цінність технологій полягає у здатності поєднати довгострокове планування ресурсів із динамічним масштабуванням, створюючи основу для моделей на кшталт «мережа як послуга» та приватних віртуальних інфраструктур для критичних галузей. У перспективі розвитку 5G-Advanced та майбутніх мереж 6G, network slicing має стати фундаментом інтелектуально керованих архітектур, у яких розподіл ресурсів, оптимізація трафіку й мережеві конфігурації формуватимуться в режимі реального часу на основі аналізу великих обсягів

телеметричних даних. Таким чином, network slicing трансформується з інструменту сегментації мережі у концептуальну платформу, що забезпечує гнучкість, масштабованість і готовність до впровадження інтелектуальних алгоритмів.

Інтернет речей також висуває унікальні вимоги до сучасних систем передачі інформації, що суттєво відрізняються від традиційних комунікаційних мереж. Основна особливість полягає у великій кількості сенсорних пристроїв, що зазвичай передають невеликі обсяги даних, але мають забезпечувати тривалу роботу без частої заміни джерел живлення. Ці особливості зумовлюють суворі обмеження щодо енергоспоживання та продуктивності протоколів передачі даних.

Для задоволення цих специфічних потреб розроблені спеціалізовані технології зв’язку, такі як NB-IoT, LoRaWAN та LTE-M. Вони оптимізовані для низького енергоспоживання, розширеного радіусу дії та здатності працювати в умовах високої густини пристроїв. Порівняння параметрів технологій зв’язку наведено в таблиці 1.1.

Масштабування таких мереж до рівня мільйонів одночасно підключених пристроїв ставить серйозні виклики щодо управління мережею. Важливим є питання вибору архітектури управління — централізованої або децентралізованої. Централізовані системи полегшують координацію та моніторинг, але можуть стикатися з проблемами навантаження та затримок. Децентралізовані рішення, навпаки, забезпечують більшу гнучкість і стійкість до відмов, але потребують складніших алгоритмів взаємодії та узгодження.

Для ефективного функціонування IoT-інфраструктури необхідно впроваджувати інтелектуальні механізми управління, які дозволять адаптувати ресурси мережі під динамічні умови експлуатації, прогнозувати навантаження та автоматично оптимізувати роботу пристроїв із врахуванням обмежень енергоспоживання. Це відкриває перспективи для застосування методів штучного інтелекту і машинного навчання, що є важливим напрямком подальших досліджень і розробок.

Таблиця 1.1

Порівняння технологій зв’язку для IoT

	NB-IoT	LoRaWAN	LTE-M
Тип мережі	Ліцензована, мобільна мережа LTE	Неліцензована, LPWAN	Ліцензована, мобільна мережа LTE
Радіочастотний діапазон	700–900 МГц LTE-діапазони	868 МГц в Європі, 915 МГц в США	700–900 МГц LTE-діапазони
Максимальний радіус дії	10 км у міській зоні 35–40 км у сільській місцевості	2–5 км у міській зоні 15 км у сільській місцевості	11 км
Пропускна здатність	до 250 кбіт/с	до 50 кбіт/с	до 1 Мбіт/с
Час затримки	1,6–10 с	1–10 с	менше 100 мс
Енергоспоживання	до кількох років роботи	більше 10 років роботи	до кількох років роботи
Тип переданих даних	невеликі пакети даних до 1600 байтів	невеликі пакети до 242 байтів	короткі повідомлення, або тривалі сесій з обсягом даних до кількох мегабайт
Кількість пристроїв на базову станцію	до 50000	до 10000	до 60000
Стандарт безпеки	LTE Security	AES-128 шифрування	LTE Security

Open RAN або O-RAN — це підхід до побудови радіомережі, заснований на відкритих інтерфейсах, розподіленій архітектурі та широкому використанні програмно-визначених механізмів, загальна структура Open RAN зображена на рисунку 1.9. Основою Open RAN є розподіл радіопідсистеми на функціональні вузли —RU, DU та CU, між якими встановлюються стандартизовані інтерфейси. Такий підхід дозволяє незалежно обирати апаратні та програмні компоненти, здійснювати їх поетапну модернізацію та оптимізувати конфігурації відповідно до вимог конкретних сервісів або топологій розгортання. Віртуалізація DU та CU, у

свою чергу, забезпечує можливість їхнього розміщення у датацентрах або edge-вузлах, що істотно підвищує гнучкість і ефективність використання ресурсів.

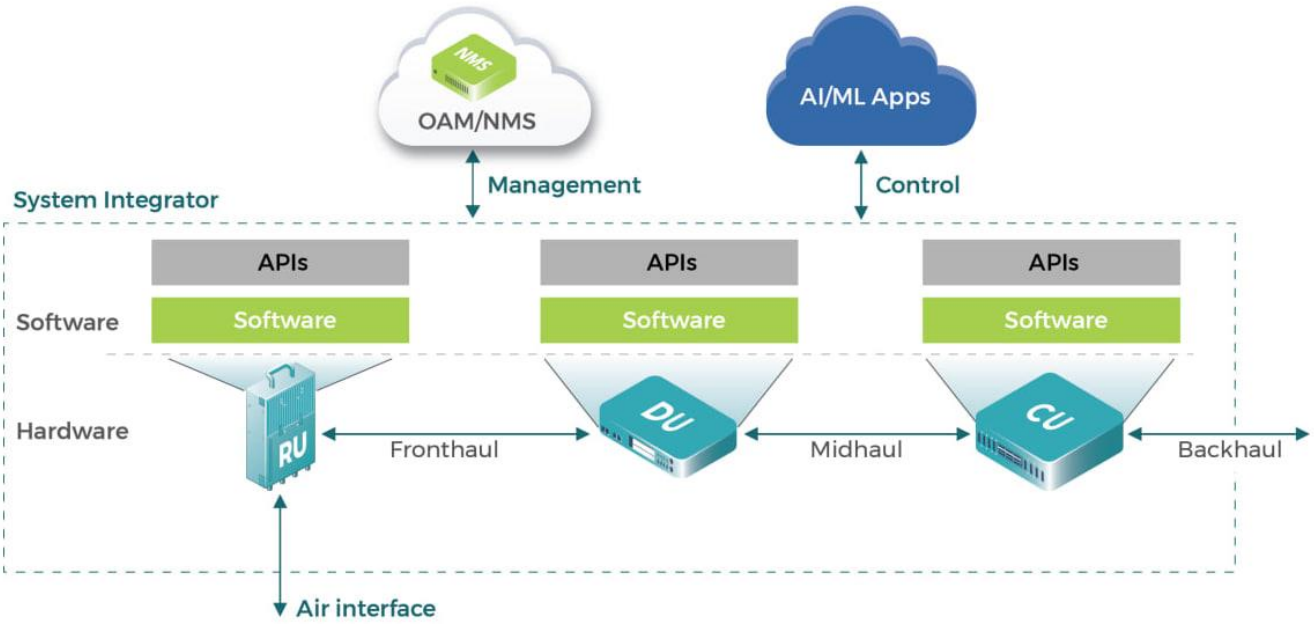


Рис. 1.9 Структура O-RAN

Важливою складовою архітектури Open RAN є впровадження інтелектуальних систем керування, зокрема RIC, який включає модулі xApps та rApps для реального часу та нефункціональних задач відповідно. Використання алгоритмів машинного навчання у RIC дозволяє автоматизувати розподіл радіоресурсів, прогнозувати навантаження, оптимізувати енергоспоживання, виявляти аномалії та адаптивно налаштовувати параметри мережі. Таким чином, Open RAN не лише розширює функціональні можливості операторів, але й слугує платформою для інтеграції інтелектуальних систем керування.

Використання концепції Open RAN визначає новий вектор розвитку сучасних систем передачі інформації, у якому ключовими стають відкриті інтерфейси, модульність та програмна керованість мережевих функцій. Відкрита архітектура створює умови для швидкої появи та інтеграції програмних компонентів, систем аналітики та засобів автоматизації, що суттєво розширює можливості конфігурування та оптимізації. Завдяки цьому оператори отримують гнучкий інструмент побудови та модернізації інфраструктури, який дозволяє впроваджувати нові технологічні рішення без складних реконструкцій апаратного

сегменту. У підсумку Open RAN слугує підґрунтям для переходу інфокомунікаційних систем до більш автономних, адаптивних і когнітивно керованих моделей функціонування.

1.3 Аналіз можливостей застосування штучного інтелекту у системах зв’язку

Стрімка еволюція інфокомунікаційних технологій, зумовлена вибуховим зростанням кількості підключених пристроїв, ускладненням архітектур мереж та збільшенням обсягу передаваних даних, формує нові вимоги до принципів керування інфраструктурою та забезпечення її стабільності. Традиційні підходи, засновані на статичних конфігураціях і ручному адмініструванні, поступово вичерпують свій потенціал, оскільки вже не здатні забезпечити належний рівень адаптивності, оперативності реагування й точності оптимізаційних рішень. У такому контексті застосування методів штучного інтелекту стає не просто інструментом покращення ефективності, а системоутворювальним елементом сучасних і майбутніх інфокомунікаційних платформ.

Особливу актуальність питання впровадження ШІ набуває у зв’язку з подальшим розвитком відкритих архітектур радіодоступу, віртуалізації мережевих функцій, сегментації ресурсів та інтелектуальних децентралізованих платформ обробки даних. Кожна з цих технологій створює величезні масиви оперативної інформації про стан мережі, які потребують швидкої обробки, аналізу та використання у процесах управління. В умовах розподілених мультисервісних мереж людський оператор фізично не здатний охопити весь спектр параметрів, відстежувати їх у реальному часі та своєчасно приймати оптимальні рішення. Саме тому інтелектуальні алгоритми дедалі частіше інтегруються у базові функції систем зв’язку, виконуючи роль автоматизованих аналітичних і управляючих модулів.

Застосування методів машинного навчання, глибинних нейронних мереж, моделей прогнозування та інтелектуальної обробки трафіку створює передумови

для принципово нового рівня керованості мереж. ШІ забезпечує здатність виявляти приховані залежності в інфокомунікаційних процесах, прогнозувати розвиток ситуацій, визначати аномальні стани та формувати рекомендації щодо оптимізації параметрів роботи обладнання. Завдяки цьому мережа набуває ознак самодостатності, коли значна частина операцій — від конфігурації до підтримки якості сервісу — виконується автоматично, з мінімальним втручанням персоналу.

Утім, для реалізації повноцінного інтелектуального керування необхідною передумовою стає не лише наявність алгоритмів ШІ, а й відповідна інфраструктурна база, здатна забезпечити їхню роботу у режимах, максимально наближених до реального часу. Центральні датацентри, традиційно відповідальні за оброблення великих обсягів даних, не завжди можуть гарантувати необхідний рівень затримки, пропускної здатності та стійкості, що особливо критично для задач оперативної оптимізації радіопідсистеми, управління мобільністю, виявлення аномалій або підтримки сервісів із підвищеними вимогами до доступності. У цьому контексті ключову роль починає відігравати концепція edge computing, яка забезпечує перенесення обчислювальних ресурсів, алгоритмів ШІ та функцій аналізу на периферію мережі — безпосередньо до джерел даних.

Edge-інфраструктура, схема якої зображена на рисунку 1.10, формує проміжний рівень між термінальними пристроями та хмарними платформами, дозволяючи здійснювати локальну обробку трафіку, швидке прийняття рішень та виконання моделей машинного навчання без необхідності передачі інформації до віддалених центрів обробки. Такий підхід мінімізує затримки та зменшує навантаження на транспортні сегменти, що є особливо важливим в умовах стрімкого зростання інтенсивності даних, характерного для сучасних мобільних мереж і середовищ із високою динамікою. Водночас розміщення інтелектуальних модулів на периферії сприяє підвищенню точності адаптивних рішень, оскільки вони працюють на основі локального контексту, який відображає реальний стан радіоінтерфейсу, трафіку та навколишнього середовища.

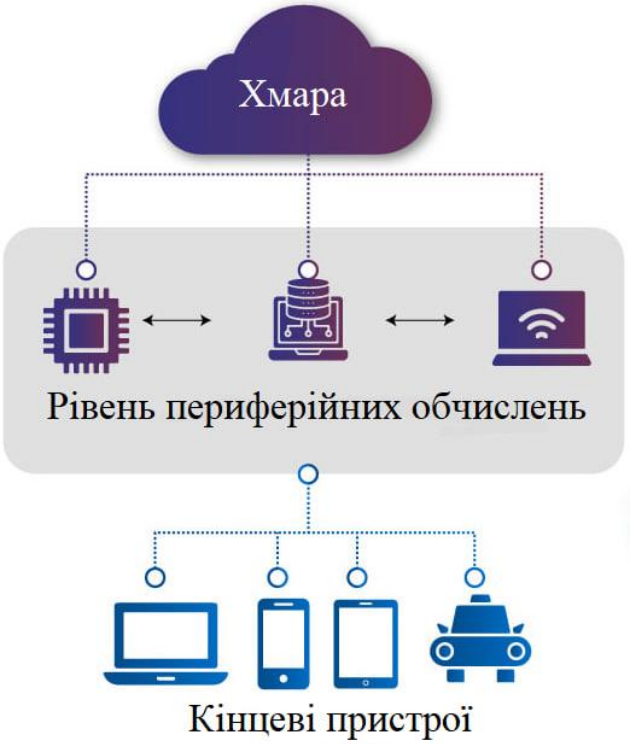


Рис. 1.10 Схема роботи Edge-інфраструктури

Подальший розвиток edge computing у інфокомунікаційній сфері пов’язаний не лише з перенесенням обчислень ближче до джерела даних, а й із формуванням багаторівневої, ієрархічно організованої структури периферійних обчислювальних вузлів. У такій архітектурі різні рівні edge-інфраструктури виконують спеціалізовані функції: від ультранизьколатентної локальної обробки на рівні базових станцій до інтелектуальних регіональних вузлів, здатних виконувати складні моделі машинного навчання та обробляти агреговані масиви телеметрії. Це створює передумови для ефективного розподілу навантаження між рівнями мережі та оптимального використання ресурсів у залежності від характеру задачі.

У межах такої архітектури штучний інтелект може виконувати різнопланові функції, зокрема: прогнозування коливань навантаження в реальному часі, динамічне перерозподілення ресурсів, локальне виявлення аномальних подій, оптимізацію енергоспоживання та забезпечення адаптивного керування якістю обслуговування для окремих категорій трафіку. Значною перевагою виступає здатність edge-вузлів працювати автономно навіть за наявності часткових втрат

зв’язку з центральною хмарою, що підвищує стійкість мережі до збоїв і дозволяє зберігати критичні функції керування.

Інтеграція edge computing із сучасними моделями ШІ також сприяє появі нових сценаріїв обслуговування, які раніше були технологічно недосяжними. Наприклад, застосування моделей глибинного навчання для розпізнавання ситуацій у реальному часі дає змогу реалізувати інтелектуальне керування мобільністю, адаптивне прогнозування перешкод, оптимізоване підключення пристроїв IoT у масових розгортаннях, а також сценарії критично важливої комунікації, де затримки мають визначальний вплив на безпеку та якість роботи систем. Особливої ваги це набуває у поєднанні з архітектурою Open RAN, у якій периферійні інтелектуальні модулі використовуються для локального аналізу стану та виконання алгоритмів самоналаштування.

Крім того, edge-інфраструктура забезпечує можливість виконання моделі «розподіленого навчання», коли алгоритми ШІ навчаються на периферії без передачі сирих даних до центру. Це підвищує конфіденційність, зменшує навантаження на мережу та прискорює процес адаптації моделі до конкретних локальних умов. Такий підхід, відомий як federated learning, дозволяє операторам мобільного зв’язку формувати глобальні інтелектуальні моделі на основі локально навченої статистики, забезпечуючи баланс між точністю, ефективністю та вимогами до приватності інформації.

Cloud-native архітектура одна з ключових тенденцій, що визначає сучасний етап розвитку інфраструктур зв’язку, основні елементи для її реалізації зображені на рисунку 1.11. На відміну від традиційних централізованих платформ, де мережеві функції реалізовувалися у вигляді монолітних програмно-апаратних комплексів, cloud-native підхід передбачає побудову системи на основі мікросервісної архітектури, контейнеризації, динамічної оркестрації та масштабованих хмарних середовищ. Що дає змогу забезпечувати значно вищий рівень гнучкості, ізоляції процесів і можливості оперативного розгортання нових функцій, та є критично важливим у контексті керування великими мультисервісними мережами.

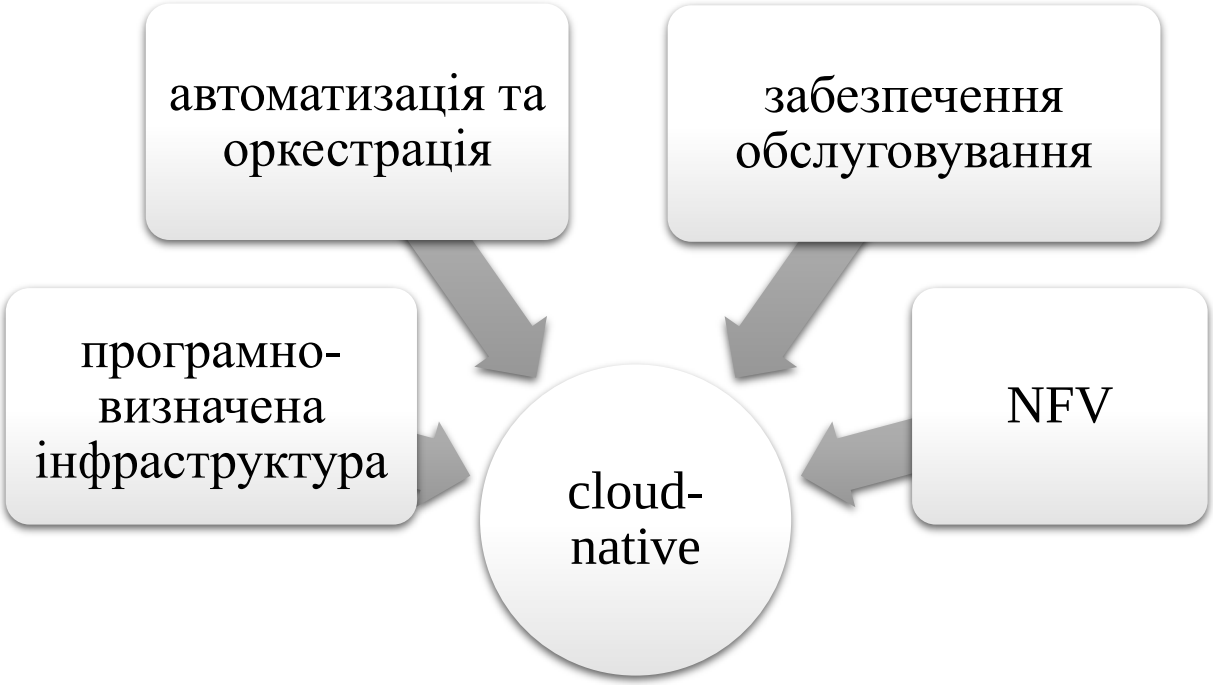


Рис. 1.11 Основні елементи Cloud-native архітектур

Cloud-native підхід створює підґрунтя для масштабного впровадження штучного інтелекту. Оскільки інтелектуальні алгоритми потребують значних обчислювальних ресурсів та гнучких моделей інтеграції, саме хмарні середовища забезпечують можливість розгортання складних аналітичних платформ, інструментів прогнозування, систем забезпечення автономності та моделей оптимізації. Крім того, мікросервісна структура дозволяє впроваджувати окремі компоненти ШІ— наприклад, модулі аномалій, прогнозні моделі навантаження, інтелектуальні контролери радіоресурсів — без зміни всієї мережевої архітектури.

Особливе значення набуває концепція service mesh, яка дозволяє створювати прозору інфраструктуру взаємодії між мікросервісами, включно з інтелектуальними алгоритмами. Це забезпечує стандартизоване керування потоками даних, контроль доступу, балансування навантаження, моніторинг і захист комунікацій на рівні сервісів, що є критично важливим у масштабних операторських середовищах. Такий підхід також спрощує інтеграцію інтелектуальних модулів у реальний час, оскільки обмін телеметрією між компонентами стає уніфікованим та легко керованим.

Інтелектуальні системи прогнозування навантаження та оптимізації ресурсів відкривають можливості докорінно змінити принципи управління ресурсами в системах передачі інформації, забезпечуючи їхню проактивну, а не реактивну поведінку. Одним із найбільш важливих напрямів є використання інтелектуальних методів прогнозування мережевого навантаження, що дозволяє завчасно оцінювати динаміку трафіку, визначати потенційні пікові періоди та моделювати сценарії зміни параметрів роботи інфраструктури. Моделі машинного навчання, зокрема алгоритми аналізу часових рядів і глибинні нейронні мережі, здатні виявляти складні нелінійні закономірності в поведінці користувачів та додатків, що робить прогнозування більш точним і стійким, ніж у традиційних статистичних методах.

Результати такого прогнозування формують основу для інтелектуальної оптимізації використання мережевих ресурсів. Штучний інтелект може динамічно перерозподіляти пропускну здатність, коригувати конфігурації каналів передачі, адаптувати рівні пріоритезації сервісів та визначати оптимальні маршрути трафіку, мінімізуючи ймовірність перевантажень і деградації якості обслуговування. У розподілених хмарних і мультидоменних середовищах це дозволить забезпечити стабільність роботи систем навіть за умов нерівномірного розподілення запитів та різких змін інтенсивності трафіку.

Окремого значення набуває оптимізація енергоспоживання, яка у великих інфокомунікаційних мережах стає критичним чинником ефективності й довгострокової масштабованості. Інтелектуальні алгоритми здатні автоматично визначати оптимальні режими функціонування обладнання, відключати або переводити в енергозберігаючий стан частину мережевих елементів під час зниженого навантаження, а також прогнозувати доцільність розширення чи згортання ресурсів у хмарних або периферійних сегментах. Такий підхід не лише мінімізує надлишкове використання обчислювальної потужності, але й забезпечує стабільне функціонування інфраструктури за умов різкої зміни трафіку, характерної для нових технологій зв’язку — зокрема 5G-Advanced, ранніх

прототипів 6G, мереж із підтримкою масового IoT та децентралізованих платформ доступу.

Виявлення аномалій та автоматичний fault management за допомогою ШІ дає змогу суттєво підвищити стійкість і самодостатність систем передачі інформації. Використання інтелектуальних моделей дозволяє не лише фіксувати відхилення у роботі мережевих елементів, а й передбачати можливі збої ще до того, як вони вплинуть на якість сервісів.

Штучний інтелект здатен аналізувати великі масиви телеметричних даних: показники навантаження, затримки, зміну пропускної здатності, поведінку протоколів, кореляцію подій. На основі цих даних ШІ може визначати нетипові патерни, характерні для початку деградації обладнання або розвитку аварійної ситуації. Це дає можливість переходу від реактивного обслуговування до повністю проактивної моделі, у якій система сама виявляє потенційну проблему, класифікує її та пропонує оптимальний сценарій дій.

Подальша автоматизація fault management ґрунтується на здатності ШІ виконувати кореляцію подій і локалізацію джерела збою в масштабних мережах, де традиційні методи вже не забезпечують достатньої точності. Алгоритми аналізують часові послідовності подій, залежності між сервісами, взаємодію між мережевими вузлами та вплив окремих несправностей на суміжні елементи інфраструктури. Такий підхід дозволятиме швидко визначити корінну причину інциденту й уникнути хибних спрацювань, які зазвичай виникають у складних топологіях.

Особливої цінності набувають функції самовідновлення, коли система не лише фіксуватиме аномалію, а й автоматично виконуватиме відновлювальні дії. До таких дій можуть належати перезапуск сервісів, перемикання трафіку на резервні маршрути, динамічне переконфігурування мережевих компонентів або ізоляція несправних сегментів. У результаті час відновлення скорочується до мінімуму, а вплив інцидентів на користувачів практично зникає.

Застосування ШІ у fault management сприятиме формуванню адаптивного оператора, де більшість рутинних рішень приймається автоматично, а людське

втручання потрібне лише у виняткових ситуаціях. Це створює передумови для переходу до концепції автономних мереж, у яких системи передачі інформації здатні працювати стабільно навіть за умов динамічних змін навантаження, оновлення обладнання чи розвитку топології.

Інтелектуальні методи маршрутизації та автоматизована оптимізація параметрів QoS/QoE це одні з ключових напрямів інтеграції штучного інтелекту у сучасні системи передачі інформації. Зі зростанням кількості сервісів, вимог до затримки, варіації затримки й пропускної здатності традиційні механізми маршрутизації та QoS вже не здатні оперативно реагувати на динамічні зміни мережевого середовища. Це особливо відчутно у мультисервісних інфокомунікаційних системах, де одночасно працюють високочутливі до затримок застосунки, масові IoT-підключення та ресурсоємні медіасервіси.

Використання інтелектуальних алгоритмів дозволить автоматизувати визначення оптимальних маршрутів передачі даних. Системи машинного навчання аналізуватимуть телеметрію мережі: рівень завантаження каналів, затримки, втрати пакетів, поведінку трафіку в різних часових інтервалах і прийматимуть рішення щодо перенаправлення потоків у реальному часі. Завдяки цьому маршрути формуватимуться не за статичними метриками, а з урахуванням прогнозованого стану мережі та контекстних факторів, що забезпечить рівномірний розподіл навантаження та мінімізацію ризику перевантаження окремих сегментів інфраструктури.

Інтеграція цих підходів створює умови для формування більш передбачуваної та адаптивної мережевої поведінки. ШІ не лише реагує на поточні зміни, а й прогнозує їх, що дозволяє заздалегідь оптимізувати маршрути, розподіл ресурсів і механізми забезпечення якості. У результаті система передачі інформації функціонуватиме стабільніше, а кінцеві користувачі отримують гарантовану якість сервісу навіть за умов зростаючих навантажень і появи нових технологій зв’язку.

Інтелектуальні методи забезпечення безпеки систем передачі інформації посідають ключове місце у сучасних підходах до побудови й експлуатації інфокомунікаційної інфраструктури, адже стрімке ускладнення мережевих

архітектур та зростання динамічності трафіку створюють якісно нові виклики для систем кіберзахисту. У традиційних моделях безпеки основний акцент робився на сигнатурних методах і статичних правилах фільтрації, однак їх ефективність невпинно знижується через появу адаптивних, складних і багатоступеневих кіберзагроз, що можуть імітувати легітимну поведінку користувачів і мережевих сервісів. У такому середовищі саме інтеграція штучного інтелекту забезпечить можливість переходу від реактивних підходів до проактивних і когнітивних моделей захисту.

Важливим компонентом є автоматизація реагування на інциденти. Інтелектуальні системи можуть автономно ініціювати ізоляцію компрометованих сегментів, зміну маршрутів передачі даних, блокування підозрілих з'єднань чи перехід до резервних механізмів обслуговування. Значно скорочуючи час між виявленням аномалії та застосуванням контрзаходів, такі системи мінімізують ризик поширення атаки та підвищують загальну стійкість інфраструктури.

Особливого значення набуває здатність ШІ прогнозувати можливі загрози. На основі історичних даних, профілів користувачів, сезонних коливань трафіку та характеристик взаємодії мережевих компонентів алгоритми формують моделі ймовірнісного прогнозування, що дозволяє завчасно посилювати захисні механізми, оптимізувати розподіл ресурсів і коригувати політики доступу. Це забезпечує превентивний рівень безпеки, у межах якого система здатна запобігати атакам ще до їхнього фактичного прояву.

Інтеграція інтелектуальних методів безпеки у децентралізовані середовища: edge-платформи, cloud-native системи та Open RAN формуватиме багаторівневу модель захисту, у якій загрози відстежуються як на периферії, так і на центральних хмарних рівнях. Така архітектура забезпечуватиме швидке локальне реагування та узгоджене глобальне управління, що є критично важливим у розподілених системах передачі інформації. У підсумку, інтелектуальні алгоритми створюють умови для формування мереж із вбудованими властивостями самозахисту, що становить фундаментальний етап еволюції систем зв'язку в напрямі когнітивності, автономності та підвищеної стійкості до сучасних кіберзагроз.

Прогностичні моделі технічного обслуговування стають одним із ключових застосувань штучного інтелекту в системах передачі інформації, оскільки саме вони забезпечують перехід від реактивного до проактивного підходу в управлінні інфраструктурою. У традиційних інфокомунікаційних мережах технічне обслуговування виконується за розкладом або після появи відмови, що часто призводить до значних простоїв, деградації якості сервісів та збільшення експлуатаційних витрат. На противагу цьому, інтелектуальні системи прогнозування здатні аналізувати багатовимірні телеметричні дані: температуру обладнання, рівень сигналу, частоту помилок, напругу живлення, поведінку мережевих процесорів, профілі навантаження і виявляти приховані індикатори наближення відмови.

Методи машинного навчання дозволяють формувати предиктивні моделі, що оцінюють залишковий ресурс обладнання, ймовірність виникнення критичних подій та оптимальний час проходження сервісних робіт. Наприклад, для оптичних систем такі моделі можуть прогнозувати деградацію параметрів підсилювачів чи зниження якості оптичного сигналу через зношування компонентів; у радіомережах — появу нестабільності через перегрів антенних модулів або порушення фазового синхронізму; у хмарних системах — виявляти аномальні цикли завантаження CPU чи дискових систем, що вказують на майбутнє падіння продуктивності.

Ключова перевага predictive maintenance полягає у можливості планувати втручання завчасно, оптимізуючи графік сервісних робіт та мінімізуючи вплив на користувачів. Це особливо важливо для мультисервісних мереж 5G, Open RAN та розподілених хмарних платформ, де вихід з ладу одного компонента може викликати каскадні обмеження пропускної здатності або деградацію критичних сервісів. Інтелектуальні системи прогнозування не лише фіксують ранні ознаки несправностей, але й пропонують оптимальні сценарії реагування від перенаправлення трафіку до автоматичного перезапуску мікросервісів чи масштабування ресурсів. У перспективі такі інструменти стають основою повністю автономних систем керування технічним станом інфраструктури, здатних

забезпечувати стабільність роботи навіть у складних і швидкозмінних умовах експлуатації.

Концепція автономних мереж є логічним продовженням інтеграції штучного інтелекту в системи передачі інформації й відповідає загальній тенденції переходу від автоматизації окремих процесів до формування повністю самокерованих інфраструктур. На відміну від традиційних мереж, де більшість операцій здійснюється вручну або з використанням статичних алгоритмів, автономні мережі функціонують за принципами: самоаналізу, самоконфігурації, самооптимізації та самовідновлення.

Основою таких систем є постійний збір великих обсягів телеметричних даних з усіх рівнів інфраструктури та їх інтеграція у моделі інтелектуального прийняття рішень. Алгоритми машинного навчання в режимі реального часу аналізують поведінку трафіку, навантаження на канали, стан обладнання, параметри середовища, активність користувачів та зовнішні фактори впливу. На основі цього формуються оптимізаційні дії, які застосовуються автоматично — без участі оператора або з мінімальним контролем.

Автономні мережі зможуть самостійно обирати оптимальні конфігурації ресурсів, налаштовувати параметри QoS, перемикати маршрути відповідно до змін у структурі трафіку, виконувати масштабування хмарних компонентів, реагувати на аномалії, відновлювати зв’язність та перерозподіляти навантаження. У системах 5G і майбутніх 6G така функціональність є ключовою для забезпечення стабільної роботи сервісів з жорсткими вимогами до затримки, надійності та пропускної здатності — зокрема автономного транспорту, промислових роботизованих платформ, критичної інфраструктури та систем масового підключення IoT.

Важливою характеристикою автономних мереж є здатність до адаптивного навчання. Інтелектуальні моделі безперервно уточнюють свої параметри на основі нових даних, що дозволяє покращувати точність прогнозів та якість оптимізаційних рішень. Завдяки використанню механізмів машинного навчання, адаптивного планування ресурсів, динамічної маршрутизації та автономного управління трафіком такі мережі здатні не лише підтримувати оптимальні

параметри роботи, а й реагувати на зміну навантаження в реальному часі. Це робить їх стійкими до аномалій, збоїв та зовнішніх загроз, що особливо важливо для критичних інфокомунікаційних сервісів.

У сукупності впровадження автономних механізмів стає фундаментальним етапом еволюції інфокомунікаційної інфраструктури, адже саме вони забезпечують перехід від традиційних керованих систем до високорівневих інтелектуальних платформ. Це дозволяє створювати системи передачі інформації, що працюють у режимі максимального самоконтролю, автоматично аналізують власний стан, прогнозують можливі відхилення та своєчасно коригують параметри функціонування без участі оператора.

Подібні архітектури формують основу для цифрових платформ наступних поколінь, де гнучкість, швидка адаптація та інтелектуальна керованість стають ключовими вимогами до інфраструктури. У таких системах реалізується концепція self-configuring, self-healing, self-optimizing, яка забезпечує безперервність сервісів, високу пропускну здатність та мінімізує потребу в ручному втручанні. У результаті інфокомунікаційна мережа перетворюється на активний, динамічний компонент цифрової екосистеми, здатний самостійно забезпечувати надійність, ефективність та прогнозованість роботи у широкому спектрі сценаріїв.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ПОБУДОВИ СИСТЕМ ПЕРЕДАЧІ ІНФОРМАЦІЇ

2.1 Архітектурні принципи побудови сучасних систем передачі інформації

Архітектурні принципи побудови сучасних систем передачі інформації визначають можливості мережі щодо пропускної здатності, відмовостійкості, масштабованості та інтеграції інтелектуальних механізмів керування. Зі зростанням обсягу трафіку, переходом до гнучких транспортних технологій і появою сервісів із жорсткими вимогами до затримок архітектура перестає бути суто структурним описом мережі — вона стає основою для подальшої автоматизації, оптимізації та впровадження алгоритмів штучного інтелекту.

Сучасні системи передачі інформації розвиваються в напрямі підвищення керованості та модульності. Це зумовлено тим, що класичні монолітні підходи вже не відповідають вимогам 5G/6G, мультимедійних сервісів, розподілених обчислень та високошвидкісного оптичного транспорту. Поява віртуалізованих функцій, програмно-керованих сегментів, гібридних хмарних моделей і розподілених вузлів обробки даних сформувала багатокомпонентні архітектури, які включають фізичний, транспортний, сервісний та контролюючий рівні.

Централізовані архітектури — базова модель побудови систем передачі інформації, у яких більшість функцій керування, маршрутизації та обробки даних зосереджувалася у ядрах мережі або у спеціалізованих центрах комутації. У таких системах периферійні вузли виконують лише обмежені функції передусім приймання, передавання та базову агрегацію трафіку, тоді як логіка прийняття рішень та забезпечення сервісів реалізується у централізованих елементах інфраструктури, переваги та недоліки централізованої архітектури наведено в таблиці 2.1.

Таблиця 2.1

Переваги та недоліки централізованої архітектури

	Переваги	Недоліки
Управління та контроль	Єдине керування усіма ресурсами	Високе навантаження на центр
Обробка даних	Консистентність даних, спрощені механізми синхронізації	Збільшення затримок при віддаленому доступі
Масштабованість	Просте логічне масштабування на рівні центрального вузла	Обмеження фізичними ресурсами одного центру
Надійність та відмовостійкість	Централізований моніторинг дозволяє швидко виявляти збої	Наявність єдиної точки відмови, потреба у складних системах резервування
Вартість впровадження	Менше обладнання на периферії	Значні витрати на центральний дата-центр, висока вартість резервування
Безпека	Централізована політика безпеки	Центр стає критично важливою ціллю для атак
Ефективність управління трафіком	Можливість глобальної оптимізації маршрутів, QoS	Додаткові затримки при високому трафіку або великій географічній розподіленості
Підтримка та модернізація	Оновлення виконуються в одному місці	Зміни в центрі впливають на всю систему
Підтримка нових сервісів	Легке додавання сервісів на центральному рівні	Обмежена адаптивність для edge-сервісів та сервісів з низькою затримкою

Цей підхід був характерний як для класичних інфокомунікаційних систем комутації каналів, так і для ранніх пакетних мереж, де маршрутизатори ядра відповідали за більшу частину обчислювального навантаження. Централізація дозволяла спростити контроль над мережевими ресурсами та забезпечити передбачувану поведінку системи за рахунок уніфікованого управління, однак водночас створювала низку обмежень, пов’язаних зі масштабованістю, затримками та стійкістю до відмов.

В сучасних умовах централізовані архітектури зберігають актуальність у специфічних сегментах, де потрібний суворий контроль і гарантований рівень якості — наприклад, у транспортних ядрах операторського класу, у мережах

спеціального призначення або у середовищах з визначеним набором сервісів. Проте їхні обмеження щодо гнучкості та реактивності стають критичними у масштабних мультисервісних мережах 5G/6G, де обсяг телеметрії значно зростає, а вимоги до затримок посилюються.

Децентралізовані архітектури передбачають розподіл ключових функцій системи передачі інформації між декількома вузлами, кожен з яких може виконувати обробку, зберігання та маршрутизацію даних без обов'язкового звернення до центру. На відміну від централізованих рішень, де керування та обробка даних зосереджені в одному основному центрі, децентралізовані системи використовують принцип рівноправності вузлів або часткової ієрархії з множиною центрів контролю переваги та недоліки наведено в таблиці 2.2.

Таблиця 2.2

Переваги та недоліки децентралізованої архітектури

	Переваги	Недоліки
Управління та контроль	Менше навантаження на центральні елементи керування	Для глобальної оптимізації потрібні додаткові протоколи синхронізації
Обробка даних	Менша затримка та навантаження на магістральні канали	Вимагає більшої обчислювальної спроможності периферійних вузлів
Масштабованість	Можливість нарощування потужності шляхом додавання вузлів	Складні топології перебудови та налаштування взаємодії між компонентами
Надійність та відмовостійкість	Локальні збої не впливають на роботу всієї системи	Складніше координувати відновлення та забезпечити узгоджений стан системи
Вартість впровадження	Можливість розгортання у вже існуючих сегментах	Вищі капітальні витрати на периферійні елементи
Безпека	Система є стійкою до відмов	Важче забезпечити уніфікований контроль доступу
Ефективність управління трафіком	Локальні рішення дозволяють оперативно реагувати	Локальне мислення спричиняє розрізнені рішення та неефективну маршрутизацію
Підтримка та модернізація	Гнучка інтеграція нових можливостей на периферії	Ускладнене технічне обслуговування
Підтримка нових сервісів	Просте додавання сервісів для окремих сегментів або вузлів	Нерівномірність можливостей різних вузлів може обмежувати уніфікацію сервісів

Поширення таких архітектур обумовлене необхідністю підвищення масштабованості, прискорення обробки трафіку та мінімізації затримок, особливо у системах реального часу, інтернеті речей, критичній інфраструктурі та глобальних розподілених мережах. У таких системах кожен вузол може автономно приймати рішення, проводити попередню обробку даних або брати участь у колективному маршрутизаційному процесі. Важливою характеристикою децентралізованих архітектур є підвищена стійкість до відмов. За рахунок відсутності єдиної точки збою система може продовжувати функціонувати навіть при часткових пошкодженнях або недоступності окремих компонентів.

Архітектури з програмно-керованим управлінням сформували один із ключових напрямів еволюції сучасних систем передачі інформації. Їхня поява стала відповіддю на обмеження традиційних мереж, у яких функції керування та пересилання були жорстко пов’язані всередині одного мережевого пристрою. Єдина логіка роботи «control plane + data plane» ускладнювала автоматизацію, унеможливлювала глобальну оптимізацію маршрутів і збільшувала складність управління у великих інфраструктурах.

SDN пропонує концептуально інший принцип організації — відокремлення площини керування від площини пересилання. Мережеві пристрої працюють як комутатори пересилання, у той час як логіка маршрутизації, політик і оптимізації концентрується в централізованому контролері. Така структура дозволяє динамічно формувати маршрути, змінювати правила обробки трафіку та застосовувати політики QoS без необхідності фізичної переналаштування обладнання.

Важливо, що SDN інтегрується з сучасними моделями автоматизації — YANG-профілями, Telemetry Streaming, протоколами gNMI/gNOI, інтерфейсами RESTCONF. Це робить мережеву інфраструктуру значно ближчою до програмної логіки, дозволяє керувати системою через API та застосовувати алгоритми машинного навчання для аналізу телеметрії в реальному часі.

У контексті систем передачі інформації SDN надає кілька практичних переваг:

- можливість централізованої оптимізації маршрутів із врахуванням пропускної здатності, затримок та пріоритизації типів трафіку;
- інтеграція механізмів Segment Routing, що дозволяють формувати політики передачі на основі цілей;
- створення умов для часткового або повного впровадження намірно-орієнтованих мереж, де оператор визначає не маршрути, а вимоги до сервісу.

Саме завдяки відокремленню логіки керування SDN активно використовується в транспортних платформах 5G, де необхідно гарантувати одночасно низьку затримку, ізоляцію трафіку для різних слайсів, динамічне балансування та централізований контроль над ресурсами. Ці властивості роблять SDN однією з ключових архітектур для моделювання у розділі 3, оскільки вона забезпечує керованість і гнучкість, необхідні для інтеграції інтелектуальних алгоритмів.

SOA та мікросервісні підходи є ключовими моделями побудови сучасних розподілених систем, орієнтованих на надання сервісів та функцій у вигляді незалежних компонентів. Їх основна ідея полягає у відокремленні бізнес-функцій у вигляді окремих сервісів, що взаємодіють між собою через стандартизовані інтерфейси. У системах передачі інформації ці архітектури широко застосовуються для управління великими обсягами трафіку, оркестрації мережевих функцій, побудови масштабованих сервісних платформ. [13]

SOA історично стала основою для інтеграції розподілених сервісів у корпоративних мережах, забезпечуючи формальну стандартизацію, інтероперабельність та модульність. Основними перевагами SOA є:

- Стандартизовані інтерфейси. Використання відкритих протоколів SOAP, REST, WSDL спрощує інтеграцію та забезпечує сумісність між різними системами.
- Модульність і повторне використання сервісів. Окремі компоненти можуть бути використані кількома застосунками та легко масштабуватися.
- Висока гнучкість інтеграції. Сервіси можуть взаємодіяти незалежно від платформи, мови програмування та фізичного розташування.

- Покращена керованість та оркестрація. Можливість централізованого управління сервісами, моніторингу виконання та опису бізнес-процесів за допомогою BPM/ESB.
- Зниження витрат на розробку та підтримку. Завдяки повторному використанню компонентів та чіткій структуризації функціоналу.
- Масштабованість на рівні сервісів. Кожен сервіс може окремо масштабуватися залежно від навантаження.
- Покращена стійкість до змін. Зміна одного компонента не потребує модифікації всієї системи завдяки слабкому зв’язуванню.

Мікросервісна архітектура розвинула ці принципи, зробивши сервіси дрібнішими, незалежно керованими та такими, що підтримують динамічне масштабування. Для інфокомунікаційних систем ключовою перевагою мікросервісного підходу є можливість швидкого оновлення окремих функцій, зменшення впливу збоїв та повна автоматизація керування сервісами через оркестратори типу Kubernetes та ETSI NFV MANO. Основні переваги мікросервісної архітектури включають:

- Незалежність компонентів. Кожен мікросервіс може розроблятися, розгортатися та оновлюватися окремо від інших.
- Висока відмовостійкість. Збої в одному сервісі не впливають на роботу всієї системи, що критично для інфокомунікаційної інфраструктури.
- Динамічне горизонтальне масштабування. Оркестратори автоматично масштабують сервіси залежно від навантаження.
- Оптимальне використання ресурсів. Легковагові контейнери дозволяють розгортати більше функціональних блоків на тих самих апаратних ресурсах.
- Швидкий цикл розробки. Оновлення окремих функцій відбувається без зупинки всієї системи, що пришвидшує впровадження нових сервісів у мережах 5G/6G.
- Гнучкість технологічного стеку. Кожен сервіс може бути написаний різними мовами та використовувати різні бази даних чи протоколи.

- Легкість автоматизації. Підтримка CI/CD, DevOps-підходів та систем автоматичного балансування трафіку.
- Покращена керованість та спостережуваність. Вбудована підтримка логування, телеметрії, трасування та моніторингу.
- Ефективна інтеграція з хмарними середовищами. Мікросервіси оптимально підходять для контейнеризації та роботи у multi-cloud інфраструктурі.

Архітектурні підходи Edge та Fog Computing сформувалися як відповідь на стрімке зростання обсягів трафіку, появу мільярдів IoT-пристроїв та зростаючі вимоги до швидкості обробки даних. Їх сутність полягає у перенесенні обчислювальних ресурсів ближче до джерела даних, що дозволяє зменшити затримку, підвищити надійність та оптимізувати використання магістральних каналів зв'язку. Концептуально ці технології схожі, оскільки обидві передбачають перенесення частини обчислювальних процесів від централізованих хмарних інфраструктур ближче до джерела формування даних, порівняння характеристик технологій наведено в таблиці 2.3. Проте вони реалізуються на різних рівнях: [14]

Edge-підхід передбачає виконання обчислень безпосередньо на периферії мережі — у межах базових станцій, локальних шлюзів, IoT-хабів, промислових контролерів або вбудованих обчислювальних модулів. У системах передачі інформації Edge використовується для локальної фільтрації, агрегації та попередньої обробки даних, що знижує навантаження на центральні дата-центри та скорочує час реакції сервісів. Типовим прикладом є архітектура ETSI MEC, у якій функції маршрутизації, кешування, аналітики та оптимізації трафіку розміщуються безпосередньо на мережевому краю.

Fog-підхід розширює концепцію Edge, вводячи додатковий рівень проміжних обчислень між кінцевими пристроями та хмарою. Fog-вузли можуть бути розташовані у транспортній мережі, на вузлах агрегації, у регіональних дата-центрах. На відміну від Edge, який працює на крайових елементах, Fog забезпечує розподіл обчислювальних ресурсів на ширшій географічній площі та дозволяє виконувати складніші задачі: багаторівневу аналітику, управління потоками, функції оптимізації, а також координацію між багатьма Edge-вузлами. Концепція

Fog формалізована у OpenFog Reference Architecture, яка визначає принципи взаємодії периферійних та проміжних обчислювальних ресурсів.

Таблиця 2.3

Порівняння характеристик Edge та Fog підходів

	Edge Computing	Fog Computing
Розташування обчислень	На рівні пристроїв-дата вузлів	На проміжному рівні між Edge та хмарою
Затримка	1–10 мс	5–20 мс
Опрацювання високочастотних даних	Дуже ефективне	Ефективне, але з більшими затримками
Пропускна здатність каналу до хмари	Зменшує навантаження на бекхол	Частково зменшує, виконує попередню агрегацію
Обчислювальні можливості	Ресурси кожного вузла	Кластерні ресурси Fog-вузлів
Підтримка масштабування	Залежне від кількості вузлів	На рівні сегмента мережі
Виконання алгоритмів ШІ	Невеликі моделі, прискорені інференси	Підтримує складні моделі та аналітику
Управління трафіком	Переважно локальне	Сегментоване управління
Безпека	Вразливість до атак на периферії, використання Zero Trust Edge	Посилені механізми контролю, можливість сегментації Fog-кластерів
Вартість впровадження	Висока через кількість вузлів	Середня, зменшує потребу у великій кількості edge-вузлів
Надійність	Висока при використанні кластерів, але залежить від вузлів	Висока завдяки проміжним вузлам та дублюванню
Типові сценарії застосування	RAN Intelligence, V2X, AR/VR low-latency, Industry 4.0	Smart City, Smart Grid, IoT aggregation, відеосервіси з попередньою обробкою

У інфокомунікаційних системах використання Edge та Fog Computing дозволяє значно знизити затримки, підвищити надійність сервісів, зменшити навантаження на магістральні канали та забезпечити функціонування критичних застосунків 5G/6G, включно з URLLC, mMTC та високонадійною відеоаналітикою.

2.2 Методи забезпечення надійності та ефективності передачі інформації

Надійність і ефективність передачі даних є ключовими характеристиками сучасних інфокомунікаційних систем, що працюють у умовах зростаючих навантажень, різнорідності сервісів та високих вимог до безперервності функціонування. Зі збільшенням обсягів трафіку, поширенням критичних застосувань та переходом до гнучких архітектур, значення механізмів забезпечення стабільної роботи мереж зростає. Тому сучасні системи передачі інформації використовують комплекс методів, спрямованих на зменшення затримок, запобігання втратам пакетів, підвищення стійкості до відмов та оптимальне використання доступних ресурсів.

Забезпечення стабільної та передбачуваної якості передачі інформації є базовою вимогою сучасних інфокомунікаційних систем. Зі збільшенням обсягів трафіку, появою latency-critical сервісів таких як: відеоконференції, хмарні застосунки, сервіси remote control, 5G URLLC та зростанням різноманітності типів даних, класичні механізми безпріоритетної маршрутизації вже не здатні гарантувати прийнятний рівень сервісу. Саме тому в інфокомунікаційних системах широко застосовують концепції QoS та QoE, які забезпечують комплексний підхід до керування ресурсами та оптимізації кінцевої якості.

QoS визначає механізми та алгоритми, які дозволяють мережі гарантувати необхідні значення параметрів зображених на рисунку 2.1.



Рис. 2.1 Основні технічні характеристики QoS

Ці параметри є критичними для сервісів реального часу, де навіть незначні коливання можуть спричинити деградацію користувацького досвіду. Для забезпечення цих параметрів використовують різноманітні механізми, такі як DiffServ, IntServ, алгоритми чергування, політики обмеження трафіку та формування трафіку.

QoE визначає суб'єктивну якість сервісу, яку сприймає користувач. Нині саме QoE стає основним критерієм ефективності мережі, адже різні додатки реагують на нестабільність по-різному, приклади метрик для визначення QoE наведені на рисунку 2.2. У сучасних платформах QoE аналізується модульно, часто з використанням машинного навчання, яке прогнозує ймовірність деградації сервісу та автоматично ініціює коригування параметрів QoS.

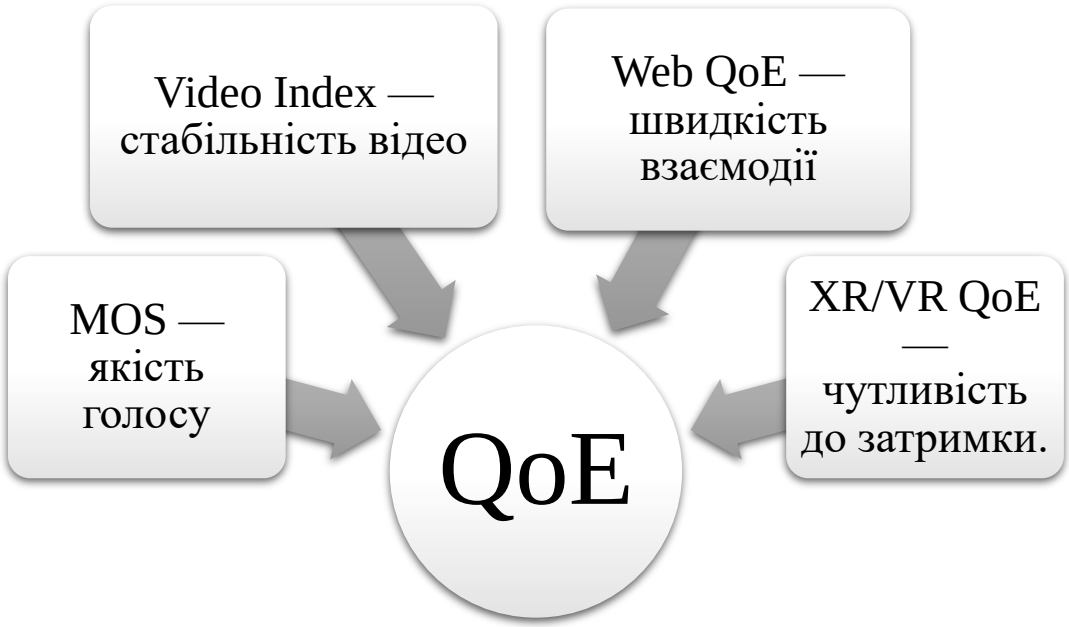


Рис. 2.2 Приклади метрик QoE

У 5G та майбутніх 6G мережах механізми QoS і QoE набувають ще більшої ваги. Тут функціонує концепція Network Slicing, де кожен "зріз" мережі має власні параметри QoS, налаштовані під конкретний сервіс. Контроль QoE здійснюється на основі телеметрії у реальному часі та систем динамічного перерозподілу ресурсів. Поєднання цих підходів дозволяє будувати мережі, здатні адаптуватись під характер трафіку та забезпечувати стабільну якість незалежно від навантаження.

Методи резервування та забезпечення відмовостійкості охоплюють комплекс підходів, спрямованих на підтримання стабільної роботи мережі навіть у разі збоїв окремих її елементів. Одним із базових механізмів є резервування каналів та маршрутів, коли поряд з основним шляхом передавання даних попередньо формується альтернативний маршрут. У разі пошкодження або перевантаження основного каналу мережа може автоматично перемикатися на запасний, використовуючи механізми динамічної маршрутизації та протоколи швидкої перебудови топології, що мінімізує затримки відновлення.

Не менш важливою складовою є резервування мережевого обладнання. У критичних сегментах інфраструктури застосовуються конфігурації типу основний-резервний вузол, де один пристрій працює активним, а другий перебуває в режимі гарячого очікування. Іншим поширеним методом є кластеризація, коли функції розподіляються між кількома пристроями, що дає змогу уникати єдиної точки відмови та забезпечує безперервність надання сервісів навіть при частковому виході з ладу обладнання.

Для підвищення стійкості інфокомунікаційних систем використовуються й механізми географічного резервування, які передбачають дублювання критичних елементів на територіально віддалених майданчиках. Це дозволяє гарантувати працездатність сервісів у випадку масштабних інцидентів, таких як аварії в дата-центрах або пошкодження регіональної інфраструктури. Синхронна або асинхронна реплікація даних забезпечує швидке відновлення операцій у відповідності до вимог RTO/RPO.

Особливу роль відіграють протоколи автоматичного перемикання, зокрема механізми віртуальних резервних шлюзів і сучасні алгоритми маршрутизації, здатні переобчислювати шляхи за частки секунди. Вони забезпечують мінімальний час простою та практично непомітне для користувачів відновлення сервісів.

У сукупності ці методи формують багаторівневу модель відмовостійкості, де резервування каналів, обладнання, майданчиків та механізми автономного перемикання працюють спільно. Такий підхід дозволяє інфокомунікаційним системам підтримувати стабільність роботи в умовах високих навантажень,

системних збоїв та зовнішніх впливів, що робить їх придатними для критично важливих цифрових сервісів.

Методи корекції та контролю помилок відіграють ключову роль у забезпеченні надійності систем передачі інформації, оскільки дозволяють компенсувати вплив шумів, інтерференції, втрат пакетів та інших факторів, що призводять до спотворення даних. У сучасних мережах ці механізми використовуються практично на всіх рівнях передавання — від фізичного до транспортного — і формують основу стабільної та достовірної роботи сервісів.

FEC забезпечує випереджувальне виявлення та виправлення помилок без необхідності повторної передачі даних. Сутність методу зображено на рисунку 2.3 і вона полягає в тому, що перед відправленням інформація доповнюється кодовими символами, які дозволяють приймачеві самостійно реконструювати пошкоджені фрагменти. Такий підхід широко застосовується в оптичних транспортних мережах, радіоінтерфейсі 5G NR, а також у супутникових системах, де зворотний канал або нестабільний, або має значну затримку. FEC дозволяє досягати високої пропускної здатності й низького рівня помилок навіть у складних умовах роботи каналу.

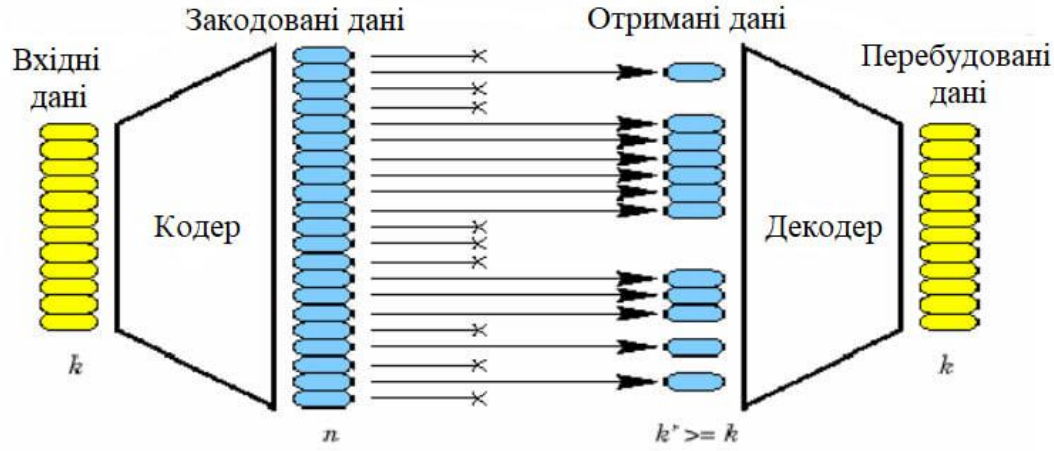


Рис. 2.3 Сутність роботи FEC

ARQ використовує зворотний зв’язок для контролю цілісності переданих даних. Якщо приймач виявляє помилку, він надсилає відправникові запит на повторну передачу необхідного блоку, принцип роботи зображено на рисунку 2.4.

Модель ARQ лежить в основі роботи багатьох транспортних протоколів, зокрема TCP, та забезпечує високий рівень надійності у середовищах із передбачуваною затримкою та доступним каналом зворотного зв'язку. Метод добре підходить для корпоративних мереж, Wi-Fi та низки інших технологій, де є можливість компенсувати втрати шляхом повторних передач.

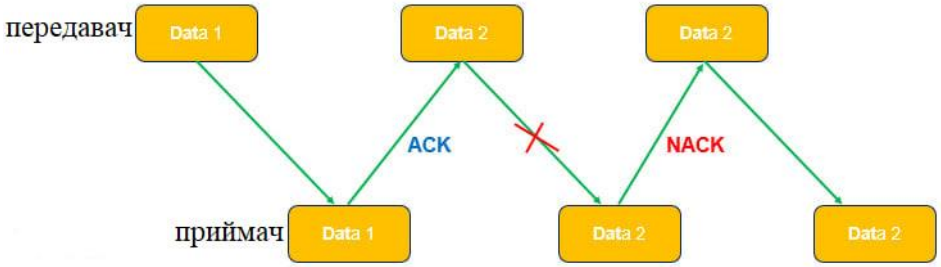


Рис. 2.4 Сутність роботи ARQ

HARQ поєднує принципи FEC та ARQ, забезпечуючи адаптивний механізм корекції помилок. У разі виявлення помилки приймач не просто ініціює повторну передачу, а комбінує отримані дані з попередніми і з надлишковими кодовими символами FEC, покращуючи шанси на правильне декодування, принцип роботи зображено на рисунку 2.5. HARQ є ключовим елементом сучасних мобільних мереж 4G LTE та 5G NR, де динамічні зміни радіосередовища потребують гнучкого та ефективного механізму контролю помилок. Завдяки цьому технологія забезпечує оптимальний баланс між затримкою, пропускною здатністю та стійкістю до перешкод.

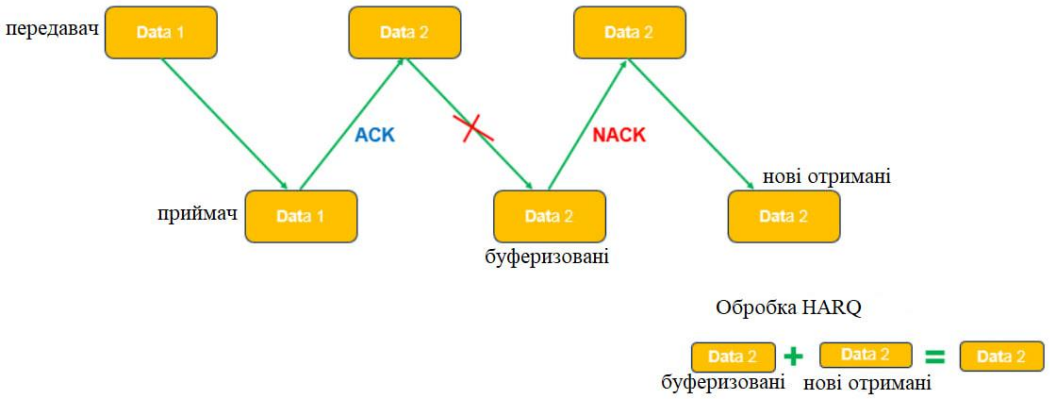


Рис. 2.5 Сутність роботи HARQ

Таким чином, методи FEC, ARQ і HARQ утворюють комплексний інструментарій забезпечення надійності, дозволяючи системам передачі інформації стабільно працювати навіть за значних коливань якості каналу та підвищених вимог до якості сервісів.

Оптимізація маршрутів та ефективне використання мережевих ресурсів формують базовий механізм підвищення продуктивності сучасних систем передачі інформації. У інфокомунікаційних мережах із високими обсягами трафіку ці методи забезпечують стабільну затримку, прогнозовану пропускну здатність та відсутність перевантажених ділянок, що є критичним для роботи відеоконференцій, потокового відео, хмарних сервісів та систем реального часу.

Одним із найважливіших підходів є динамічна маршрутизація, що дозволяє адаптувати вибір маршруту до актуального стану мережі. Наприклад, протокол OSPF використовує метрику “cost”, що зазвичай визначається пропускною здатністю інтерфейсу: чим ширший канал, тим менша вартість. У результаті трафік автоматично спрямовується через більш потужні лінії. У великих операторських мережах застосовується IS-IS, що частіше використовується у магістралях саме через оптимальну роботу на високих швидкостях та масштабованість. Обидва протоколи дозволяють у реальному часі перебудовувати маршрути у випадку відмови каналу, збільшення затримки чи перевантаження певної ділянки.

Важливою складовою оптимізації є балансування навантаження. У класичній IP-мережі популярним механізмом є ECMP, який дозволяє розподіляти трафік між кількома маршрутами з однаковою метрикою. Наприклад, якщо між двома магістральними вузлами доступні три канали по 10 Гбіт/с, ECMP дозволяє ефективно використовувати всі 30 Гбіт/с, рівномірно розподіляючи потоки. Аналогічно у дата-центрах широко застосовується балансування на рівні L4 та L7, наприклад через HAProxy, Nginx, Envoy, що дозволяє вирівнювати навантаження між сервісами та мікросервісами.

Окрему роль відіграють механізми пріоритетного обслуговування трафіку. У корпоративних та операторських мережах активно застосовуються моделі DiffServ, де трафік маркується у відповідності до класів. Голосовий трафік отримує клас EF,

що гарантує мінімальну затримку, тоді як фонові завантаження або оновлення ОС направляються до класу BE. На рівні доступу провайдери можуть впроваджувати policing або shaping, обмежуючи швидкість некритичних потоків та забезпечуючи стабільну якість для більш вимогливих сервісів.

У складних багатосегментних мережах вагому роль відіграють методи інтелектуальної оптимізації. Завдяки впровадженню алгоритмів машинного навчання можливо прогнозувати навантаження на окремі вузли, оцінювати ймовірність виникнення вузьких місць та завчасно перенаправляти частину трафіку в інші сегменти. SD-WAN контролери аналізують параметри каналів у реальному часі — jitter, packet loss, delay — і автоматично обирають найбільш якісний тунель, перемикаючи трафік між MPLS, LTE або xPON-каналами залежно від ситуації. У мобільних мережах 5G подібні алгоритми застосовуються для оптимізації ресурсів у фреймів RAN, здійснюючи динамічний перерозподіл спектра між сотами при зміні інтенсивності користувацького трафіку.

Ефективне використання ресурсів стало особливо критичним у хмарних інфраструктурах. У віртуалізованих дата-центрах застосовуються механізми network slicing, які дозволяють створювати ізольовані логічні сегменти з гарантованими параметрами продуктивності. Наприклад, один slice може бути оптимізований для URLLC-трафіку з мінімальною затримкою, тоді як інший — для eMBB із високими швидкостями паралельної передачі відео. Такий підхід дає можливість зменшити конкуренцію за ресурси та забезпечити стабільність сервісів з різними вимогами.

Таким чином, оптимізація маршрутів і керування ресурсами — це поєднання класичних алгоритмів маршрутизації, механізмів QoS і сучасних інтелектуальних підходів, що дозволяють побудувати стабільну, передбачувану та ефективну інфокомунікаційну інфраструктуру.

Підтримка високої надійності у віртуалізованих середовищах є одним із ключових чинників, що визначає працездатність сучасних систем передачі інформації. На відміну від традиційних мережевих платформ, де відмова окремого апаратного вузла часто призводила до простою сервісів, у віртуалізованих

інфраструктурах механізми забезпечення відмовостійкості інтегруються безпосередньо на рівні віртуальних функцій, контейнеризованих сервісів та платформ оркестрації. Це дає змогу досягати значно вищої гнучкості та адаптивності системи в режимі реального часу.

Live migration у таких середовищах виступає базовим механізмом, що дозволяє переміщувати віртуальні функції або контейнери між фізичними хостами без переривання сервісу. Процес синхронізує стан оперативної пам’яті та внутрішні таблиці обробки даних, що дає можливість виконувати планове технічне обслуговування або балансування навантаження без впливу на користувацький трафік. У практичних реалізаціях live migration застосовується для критичних компонентів інфокомунікаційної інфраструктури, таких як віртуалізовані шлюзи, функції EPC/5GC або контролери сигналізації.

Active–active кластеризація — ще один фундаментальний підхід, що забезпечує синхронне функціонування кількох інстансів одного сервісу. За такого режиму трафік розподіляється між екземплярами рівномірно, а відмова одного з вузлів не викликає переривання сервісу, оскільки решта елементів негайно переймає його функції. На відміну від класичної моделі active–standby, де резервна копія просто очікує активації, active–active передбачає постійну участь усіх вузлів у роботі, що збільшує продуктивність і зменшує кількість простоїв.

Для контейнеризованих сервісів критичну роль відіграє self-healing, реалізований у системах оркестрації на кшталт Kubernetes. Механізм аналізує стан контейнерів і автоматично виконує їхнє перезапускання, переміщення або відтворення у разі виявлення збоїв на рівні програмної логіки чи інфраструктури. Таким чином забезпечується стабільність мікросервісних платформ, які часто використовуються як транспортно-сервісний шар у сучасних інфокомунікаційних рішеннях.

Важливим компонентом є також автоматизоване масштабування, яке дозволяє змінювати кількість обчислювальних інстансів залежно від реального навантаження. Такий підхід запобігає деградації сервісів під час пікових навантажень і одночасно мінімізує надлишкове використання ресурсів у періоди

спадів трафіку. У середовищах NFV autoscaling особливо актуальний для функцій, що працюють у режимах змінної інтенсивності — наприклад, систем DPI, транскодерів трафіку, елементів сигнальних підсистем або систем маршрутизації.

Додаткову надійність забезпечує сегментація інфраструктури й ізоляція ресурсів, що дозволяють запобігти каскадним збоям у випадку локальних аварій. У контейнеризованих середовищах це реалізується через namespaces, cgroups і політики розміщення подів, а у віртуалізованих — через механізми CPU pinning, NUMA-ізоляції та відповідне резервування мережевих інтерфейсів.

У сукупності такі механізми формують комплексну модель відмовостійкості, яка ґрунтується не на жорсткій апаратній надмірності, а на інтелектуальному перерозподілі навантаження, динамічному керуванні віртуальними функціями та гнучких політиках оркестрації. Це дозволяє віртуалізованим системам передачі інформації забезпечувати стабільність та доступність сервісів навіть у складних умовах, підвищувати ефективність використання інфраструктури й підтримувати вимоги сучасних інфокомунікаційних платформ.

2.3 Інтелектуальні методи оптимізації систем передачі інформації

Інтелектуальні методи становлять важливий елемент еволюції сучасних систем передачі інформації, оскільки забезпечують можливість динамічного, контекстно-залежного керування складними мережевими процесами. На відміну від традиційних алгоритмів, що ґрунтуються на наперед визначених правилах і статичних моделях, методи штучного інтелекту здатні самостійно виявляти закономірності у високовимірних даних та адаптувати поведінку мережі до змінних умов експлуатації. Завдяки цьому вони дозволяють не лише оптимізувати роботу окремих компонентів інфокомунікаційної інфраструктури, а й забезпечити цілісне, узгоджене управління всією системою. [15]

На відміну від класичних підходів, що переважно орієнтуються на детерміновані механізми або спрощені аналітичні моделі, інтелектуальні методи здатні обробляти складні нелінійні залежності, які неможливо описати

формальними правилами. Це особливо важливо в умовах зростаючої варіативності трафіку, підвищення кількості мережевих сервісів та появи нових сценаріїв взаємодії абонентів. Використання алгоритмів машинного навчання дозволяє мережі адаптуватися до трафіку з непередбачуваною структурою, прогнозувати зміни навантаження, виявляти аномальні стани і приймати рішення, спрямовані на запобігання деградації якості обслуговування.

Ефективність застосування таких методів значною мірою визначається доступністю великих обсягів даних, які генерують сучасні мережі. До них належать часові ряди навантаження на канали, статистика QoS і QoE, телеметрія з мережевого обладнання, параметри маршрутизації, інформація про типи трафіку, метадані потоків, журнали подій, а також дані про відмови, затримки або коливання пропускної здатності. Сукупність цих даних забезпечує можливість навчання моделей, які можуть точно відтворювати поведінку мережі й здійснювати прогнозування її станів у різних експлуатаційних ситуаціях.

Отже, інтелектуальні методи відіграють ключову роль у формуванні адаптивних та самокерованих систем передачі інформації. Вони дозволяють переходити від статичних моделей управління до контекстно-орієнтованих рішень, які враховують як поточний стан мережі, так і прогнозні оцінки її розвитку. Це створює передумови для побудови високонадійних інфокомунікаційних систем, здатних до самостійної оптимізації параметрів роботи в реальному часі. [16]

Прогнозування мережевого навантаження одне з ключових завдань інтелектуального керування системами передачі інформації, оскільки точні передбачення дозволяють завчасно реагувати на пікові стани, балансувати ресурси та запобігати перевантаженням. Сучасні методи прогнозування поділяються на класичні статистичні підходи та глибинні моделі, що здатні враховувати складні часові залежності. Порівняння моделей наведено в таблиці 2.4.

Модель ARIMA широко застосовується у випадках, коли мережеві параметри демонструють стійку кореляцію між попередніми й майбутніми значеннями. ARIMA добре підходить для прогнозування короткострокових змін навантаження, проте втрачає ефективність у випадку нелінійних або хаотичних процесів.

Модель Prophet, розроблена для роботи зі складними сезонними компонентами, демонструє кращу адаптивність у мережах, де навантаження визначається добовими, тижневими або поведінковими патернами користувачів. Prophet менш чутливий до шумів і пропусків у даних, але, як і ARIMA, має обмежену здатність моделювати нелінійні залежності, характерні для сучасного інфокомунікаційного трафіку.

Модель LSTM використовує багаторівневу структуру керування інформаційними потоками, що складається з комірок пам’яті та механізмів фільтрації вхідних, вихідних і проміжних даних. Завдяки цьому LSTM здатна зберігати важливі залежності на протязі великих часових інтервалів і придушувати незначущі флуктуації, що є критичним при прогнозуванні навантаження, яке має нестабільний та імпульсний характер. У реальних мережах такі моделі добре відтворюють зміну інтенсивності трафіку при наявності пікових періодів, а також адаптуються до параметрів, що змінюються нерівномірно.

Модель GRU, у свою чергу, пропонує більш спрощену архітектуру, поєднуючи механізми контролю інформаційного потоку у двох гейтах — оновлення та скидання. Попри зменшену складність, GRU демонструє продуктивність, співставну з LSTM, особливо у сценаріях, де часові ряди не потребують надто глибокого моделювання внутрішніх станів. Для мережевих систем GRU є привабливим варіантом тоді, коли потрібен компроміс між точністю прогнозування та обчислювальною ефективністю, наприклад у задачах з обмеженим обсягом даних або при необхідності виконувати розрахунки у режимі, наближеному до реального часу.

TCN є сучасним підходом до прогнозування часових рядів, що поєднує ідеї згорткових нейронних мереж із каузальною структурою обробки даних. На відміну від рекурентних моделей, TCN застосовують згортки з розширенням, що дозволяє охоплювати великі часові інтервали без втрати інформації або збільшення кількості параметрів. TCN моделі демонструють високу стійкість при роботі з шумними даними, краще масштабуються та забезпечують швидше навчання порівняно з LSTM і GRU. У контексті інфокомунікацій такі моделі здатні точно відтворювати

складні патерни мережевого навантаження, включно з короткотривалими імпульсами та нерегулярними піками.

Таблиця 2.4

Порівняння основних характеристик моделей прогнозування

Метод	Точність	Вимоги до даних	Складність обчислень	Переваги	Недоліки
ARIMA	Середня	Потрібні стаціонарні ряди	Низька	Простота, швидкість	Погано моделює нелінійності
Prophet	Середня-висока	Бажана сезонність	Низька-середня	Стійкість до шуму, інтерпретованість	Обмежена здатність до ускладнених патернів
LSTM	Висока	Великі історичні дані	Висока	Враховує довгі залежності	Повільне навчання
GRU	Висока	Великі історичні дані	Середня	Ефективність та компактність	Менша гнучкість ніж LSTM
TCN	Висока або дуже висока	Середні чи великі дані	Середня	Швидкість, масштабованість, стійкість	Менша гнучкість ніж LSTM

Виявлення аномальних станів мережі є ключовим елементом забезпечення її надійності та стійкості. Аномалії можуть спричинятися зовнішніми атаками, внутрішніми збоїми, помилками конфігурації або відхиленнями у роботі окремих компонентів інфраструктури. На відміну від класичних правил евристичного аналізу, інтелектуальні методи дозволяють будувати моделі нормальної поведінки, здатні адаптуватися до зміни характеристик трафіку та виявляти раніше невідомі типи відхилень. Порівняння методів наведено в таблиці 2.5.

Autoencoder є різновидом нейронної мережі, яка навчається відтворювати вхідні дані через стисле латентне представлення. За умови, що модель тренується виключно на «здоровому» трафіку, вона формує компактний опис нормальних закономірностей. Під час роботи на нових даних мережа відтворює типові зразки з низькою похибкою, тоді як аномальні стани спричиняють суттєве збільшення помилки реконструкції.

Isolation Forest базується на випадковому розбитті простору ознак з метою «ізоляції» спостережень. Метод виходить із припущення, що аномалії мають нетипові значення атрибутів, тому їх простіше відокремити порівняно із звичайними зразками. Чим менше розбиттів потрібно для ізоляції об'єкта, тим більш імовірно, що він є аномальним.

One-Class SVM призначений для формування гіперповерхні, яка охоплює більшість нормальних зразків і відокремлює їх від потенційних аномалій. Цей підхід особливо ефективний у випадках, коли аномалії зустрічаються вкрай рідко, а структура нормального трафіку є відносно однорідною.

Таблиця 2.5

Порівняльна характеристика методів виявлення аномальних станів

Метод	Autoencoder	Isolation Forest	One-Class SVM
Обчислювальна складність	Висока	Низька	Висока
Якість виявлення	Висока	Середня або висока	Висока за однорідних даних
Потреби у даних	Великий обсяг «нормальних» даних	Невеликі вимоги	Помірні
Стійкість до шуму	Середня	Висока	Низька або середня
Переваги	Працює з багатовимірними даними, гнучкість архітектури	Масштабованість, простота	Добре працює з нелінійностями
Недоліки	Вимогливість до ресурсів	Менш точний у складних просторах ознак	Погано масштабується

Класифікація мережевого трафіку та визначення його пріоритетності є важливими завданнями сучасних систем передачі інформації, особливо в умовах зростання обсягів даних і різнорідності сервісів. Інтелектуальні методи дозволяють автоматизувати процеси розподілу пропускної здатності, визначення критичних потоків та підвищення якості обслуговування користувачів. На відміну від евристичних правил або статичних таблиць маркування, алгоритми машинного

навчання здатні адаптуватися до нових шаблонів трафіку та враховувати складні залежності між параметрами потоків. Порівняння методів для класифікації та пріоритизації трафіку наведено в таблиці 2.6.

Random Forest є ансамблевим методом машинного навчання, який формує велику кількість дерев рішень, що навчаються на випадкових підмножинах ознак та даних. Такий підхід зменшує ризик перенавчання та забезпечує стабільну якість класифікації навіть за наявності шумових або корельованих параметрів трафіку.

SVM широко використовується у випадках, коли доступні помірні обсяги якісно підготовлених даних. Алгоритм шукає гіперплощину, що максимально розділяє класи, і за потреби використовує ядра для врахування нелінійних залежностей. Це дозволяє отримувати високоточні рішення у задачах, де розподіл даних складно описати лінійними перетвореннями.

CNN традиційно застосовуються у комп'ютерному зорі, останніми роками вони активно використовуються для аналізу мережевого трафіку. Flow-послідовності — тобто серії параметрів, отриманих з часових зрізів трафіку — можуть бути представлені як одновимірні "сигнали", а згорткові фільтри дозволяють виявляти локальні патерни, властиві певним типам сервісів.

Таблиця 2.6

Порівняння методів класифікації та пріоритизації трафіку

Метод	Random Forest	SVM	CNN
Точність класифікації	Висока	Дуже висока для малих наборів	Дуже висока
Масштабованість	Висока	Низька або середня	Висока за наявності ресурсів
Інтерпретованість	Висока	Середня	Низька
Вимоги до даних	Невеликі	Помірні	Великі обсяги
Переваги	Швидкість, стійкість до шуму, інтерпретованість	Точність, ефективність у складних просторах	Виявлення складних патернів, висока адаптивність
Недоліки	Обмежена здатність моделювати складні нелінійності	Висока складність навчання, проблеми з масштабуванням	Вимогливість до вибірки та обчислювальних ресурсів

У сучасних системах передачі інформації особливе значення має здатність мережі приймати рішення в умовах невизначеності та змінного навантаження. Методи навчання з підкріпленням забезпечують можливість автоматичного формування оптимальної стратегії керування мережею на основі взаємодії агента з середовищем. На відміну від традиційних алгоритмів, що ґрунтуються на статичних правилах чи попередньо визначених моделях, RL дозволяє мережі самостійно шукати оптимальні дії для покращення якості передавання даних та ефективного використання ресурсів. Порівняння характеристик RL методів у задачах мережевої оптимізації наведено в таблиці 2.7.

Q-learning є фундаментальним методом RL, що використовує табличне представлення значень Q-функції — оцінки корисності виконання певної дії в певному стані. Алгоритм поступово уточнює цю таблицю в процесі взаємодії агента з мережею, оновлюючи значення на основі отриманих винагород. Q-learning найбільш ефективний у відносно простих середовищах, де кількість можливих станів обмежена, наприклад, вибір оптимального маршруту в невеликій топології або локальне керування ресурсами одного вузла

DQN усуває обмеження табличного підходу, замінюючи Q-таблицю нейронною мережею. Це дозволяє працювати з великими просторами станів та виконувати оптимізацію у складних інфокомунікаційних середовищах — таких як багатокомпонентні топології, динамічний розподіл смуги пропускання або адаптація під час стрімких змін навантаження. DQN навчається на основі методу replay buffer, що підвищує стабільність тренування, а використання цільової мережі знижує ризик розбалансованості оновлень. У контексті мереж DQN дозволяє знаходити оптимальні маршрути з урахуванням багатьох параметрів — затримки, завантаження ліній, втрат — і може ефективно вирішувати задачі багатокрокового прийняття рішень.

Методи *Policy Gradient* ґрунтуються на безпосередній оптимізації політики — тобто ймовірнісного закону вибору дій, — без необхідності будувати Q-функцію. Це робить їх особливо ефективними в умовах, де існує безперервний простір дій або коли стратегія повинна бути максимально гнучкою та адаптивною.

У системах передачі інформації Policy Gradient використовується для оптимального розподілу ресурсів між сервісами, динамічного масштабування пропускної здатності, керування чергами або прогнозування напрямків переорієнтації трафіку.

Таблиця 2.7

Порівняння RL методів у задачах мережевої оптимізації

Метод	Q-learning	DQN	Policy Gradient
Швидкість збіжності	Висока в простих середовищах	Середня	Середня або низька
Стабільність	Висока	Висока	Залежить від параметризації
Інтерпретованість	Висока	Середня	Низька
Складність реалізації	Низька	Середня	Висока
Масштабованість	Низька	Висока	Висока
Переваги	Простота, гарантована збіжність	Працює зі складними топологіями, враховує багато параметрів	Гнучкість, робота в безперервних просторах дій
Недоліки	Не працює у великих просторах станів	Потребує великих даних та ресурсів	Складність навчання, чутливість до шуму

Оцінювання якості обслуговування з позиції кінцевого користувача є одним із ключових напрямів інтелектуальної оптимізації мереж наступних поколінь. На відміну від параметрів QoS, що характеризують технічний стан каналу, QoE відображає суб’єктивне сприйняття сервісу користувачем і залежить від багатьох факторів — від затримки до поведінки додатка. У контексті інтелектуального управління мережами QoE-aware AI застосовується для автоматичного прогнозування рівня задоволеності користувачів на основі фактичних метрик трафіку та характеристик сервісів. Порівняння характеристик моделей прогнозування QoE наведено в таблиці 2.8. [20]

Random Forest Regression є ансамблевим методом, який ґрунтується на побудові великої кількості дерев рішень, кожне з яких формує частковий прогноз,

а підсумкове значення отримується шляхом усереднення. Така структура забезпечує модель високою стійкістю до шумових та неповних даних, що є характерним для телеметрії мережі. Random Forest здатний враховувати взаємозв'язки між параметрами, які безпосередньо впливають на QoE, зокрема затримку, джиттер, втрати пакетів чи мінливість пропускної здатності.

XGBoost належить до класу моделей градієнтного бустингу та базується на ітеративному формуванні ансамблю дерев рішень, де кожне наступне дерево коригує похибки попереднього. Така процедура дозволяє моделі точно враховувати складні нелінійні взаємозв'язки між характеристиками трафіку та показниками QoE. XGBoost відзначається високою продуктивністю завдяки оптимізованому механізму обробки даних, що включає регуляризацію, кешування та паралельну побудову дерев.

Dense Neural Networks застосовуються для моделювання QoE у випадках, коли дані можуть бути представлені у вигляді векторів ознак без значущої часової структури. Кожен шар такої мережі складається з набору повнозв'язних нейронів, що поступово трансформують початкові характеристики мережі у прогноз кінцевої метрики QoE, наприклад MOS. Dense-моделі здатні відтворювати нелінійні залежності між показниками трафіку й результативною оцінкою якості, що робить їх значно гнучкішими порівняно з регресійними методами.

Гібридні моделі, що поєднують LSTM-шари з Dense-блоками, є одним із найефективніших підходів до прогнозування QoE для динамічних мультимедійних сервісів. LSTM здатні аналізувати часові залежності тривалістю від кількох секунд до десятків секунд, що є критично важливим для відеострімінгу, VoIP, VR-трафіку чи інтерактивних сервісів. Такі моделі враховують зміну параметрів мережі в часі: коливання пропускної здатності, накопичення затримки, епізодичні втрати пакетів і характер коливань джиттера. Після обробки часової послідовності LSTM формує компактне представлення, яке передається Dense-мережі для формування остаточного прогнозу QoE.

Таблиця 2.8

Порівняння моделей прогнозування QoE

Метод	Точність	Обчислювальна складність	Стійкість до шуму	Потреба в даних
Random Forest Regression	Середня або висока	Низька	Висока	Середня
XGBoost	Висока	Середня	Висока	Середня або висока
Dense NN	Висока	Середня	Середня	Висока
LSTM + Dense	Найвища	Висока	Середня	Висока

Методи прогнозування навантаження забезпечують можливість завчасного реагування на зміни трафіку та підтримують стабільність мережевих сервісів. Алгоритми виявлення аномалій підвищують рівень безпеки й стійкості систем, дозволяючи раннє виявлення загроз і відхилень у поведінці мережі. Класифікація та пріоритизація трафіку за допомогою ML-моделей сприяє раціональному використанню ресурсів і підтримці необхідної якості обслуговування. Використання методів підкріпленого навчання відкриває можливість побудови самокерованих мереж, здатних оптимізувати маршрути та розподіляти ресурси на основі накопиченого досвіду. Моделі прогнозування QoE, у свою чергу, дозволяють орієнтувати оптимізацію на кінцеву якість споживання сервісів, що є критично важливим для сучасних мультимедійних застосунків. [21]

РОЗДІЛ 3 МЕТОДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

3.1 Побудова моделі системи передачі інформації із застосуванням ШІ

У рамках моделювання системи передачі інформації обрано архітектуру мереж 5G, що зумовлено її широкою розповсюдженістю та відповідністю сучасним вимогам до гнучкості, масштабованості й інтелектуальної керованості. Аналіз матеріалів конференції ITU, відображений на аналітичному графіку зображеному на рисунку 3.1, демонструє стабільне зростання глобального впровадження 5G та формування навколо неї екосистеми сервісів, орієнтованих на використання штучного інтелекту.

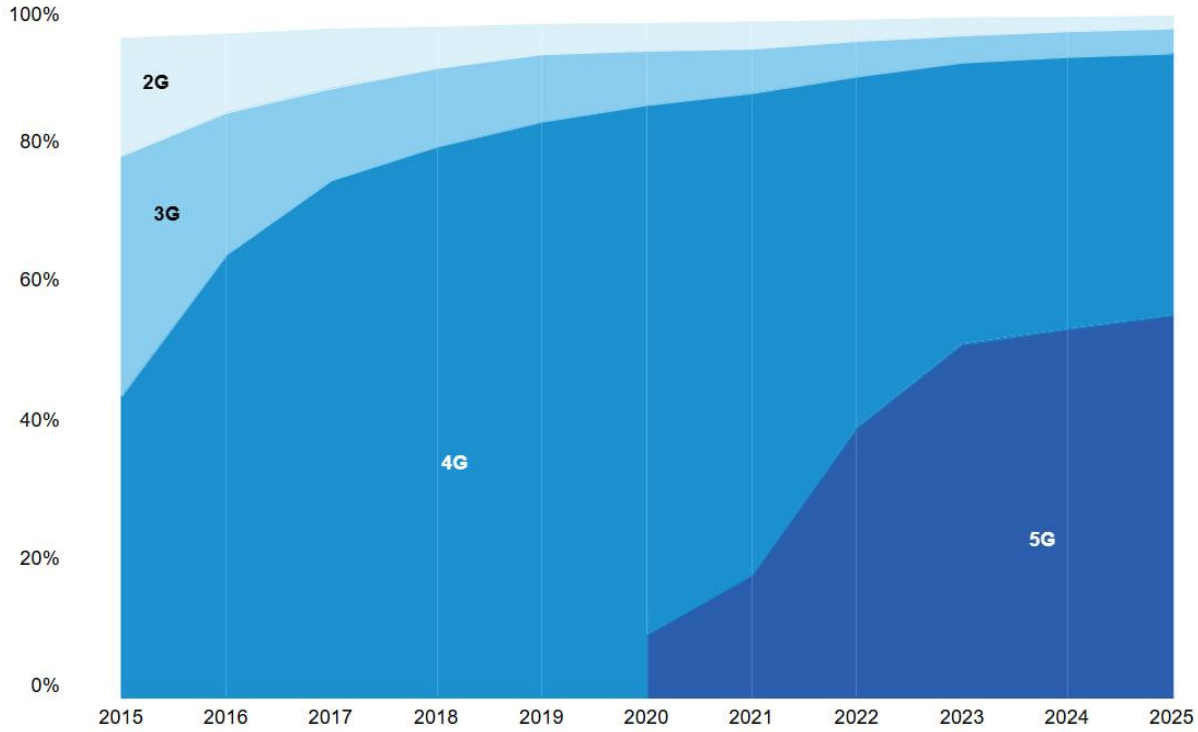


Рис. 3.1 Розподіл покриття населення за технологіями мобільного зв’язку

Архітектура 5G спроектована таким чином, щоб підтримувати мережеву віртуалізацію, динамічне виділення ресурсів, slicing-моделі та тісну інтеграцію з хмарними та edge-обчисленнями. Це створює передумови для впровадження

інтелектуальних механізмів, здатних оптимізувати ключові параметри мережі – від керування трафіком і прогнозування навантаження до виявлення аномальних подій у режимі реального часу.

Крім того, модульність 5G-Core, його сервісно орієнтована побудова та стандартизований обмін телеметрією роблять такі мережі зручною платформою для інтеграції алгоритмів машинного навчання. Таким чином, вибір саме 5G як базової системи моделювання є обґрунтованим як з позиції сучасного рівня розвитку інфокомунікаційних технологій, так і з точки зору можливості подальшого вдосконалення мережі за рахунок застосування інтелектуальних методів.

Запропонована модель системи передачі інформації розглядається як багаторівнева структура що зображена на рисунку 3.2, у якій кожен рівень виконує чітко визначені функції та взаємодіє з іншими через стандартизовані інтерфейси. Такий підхід дозволяє відтворити логіку роботи сучасних інфокомунікаційних систем, що поєднують 5G-інфраструктуру з інтелектуальними модулями аналізу та оптимізації. [22]



Рис. 3.2 Архітектурна модель 5G із застосуванням технологій ШІ

Узагальнено модель складається з чотирьох основних функціональних компонентів. Першим елементом є генерація трафіку, що забезпечує формування різних типів навантаження, притаманних реальним мережам. Це дає змогу відтворити неоднорідні режими роботи мережі та створити умови для навчання та тестування алгоритмів ШІ.

Другим структурним елементом виступає підсистема телеметрії, яка збирає параметри роботи мережі: пропускну здатність, затримку, варіацію затримки, втрати пакетів, структуру трафіку, сигнали керування від вузлів 5G Core. Саме ці дані слугують вхідними характеристиками для моделей прогнозування та виявлення аномальних станів.

Наступним рівнем є інтелектуальний шар, до складу якого входять модулі, реалізовані на основі методів машинного навчання. Вони забезпечують прогнозування навантаження, класифікацію трафіку, виявлення аномалій, оптимізацію рішень та оцінку якості обслуговування. Інтелектуальний шар функціонує як автономний аналітичний рівень, який періодично отримує телеметричні дані, виконує обчислення та формує рекомендації для системи керування.

Завершальним компонентом моделі є система керування, що отримує рішення з інтелектуального шару та застосовує їх до умовно змодельованої 5G-інфраструктури. Система керування відповідає за переналаштування параметрів мережі, зміну пріоритетів трафіку, активацію механізмів резервування та адаптивного перерозподілу ресурсів. Таким чином у моделі відтворюється замкнений цикл адаптації мережевої системи на основі результатів роботи алгоритмів штучного інтелекту.

У моделі системи передачі інформації на основі архітектури 5G ключову роль відіграє якість та різноманітність даних, що надходять від мережевих компонентів. Дані виступають основним ресурсом для навчання інтелектуальних модулів, а також для забезпечення їх стійкої роботи в динамічних умовах мережі.

5G-мережа генерує детальні flow-записи, які містять інформацію про окремі транспортні сесії: джерело і призначення пакета, протокол, обсяг переданої

інформації, тривалість з’єднання, момент надходження пакета, сигнатурні характеристики застосунку тощо.

До набору ключових показників ефективності входять рівень завантаження базових станцій, інтенсивність викликів, коефіцієнт блокування ресурсів, значення SINR, швидкість змін у каналі, пропускна здатність, затримка, джиттер та інші параметри.

QoS Metrics визначають якість роботи мережевих сервісів: гарантована пропускна здатність, максимальна затримка, кількість переданих пакетів, рівень втрат, використання ресурсів у різних slice-сегментах

Для модуля оцінювання QoE використовується інформація про показники, які безпосередньо впливають на суб’єктивний користувацький досвід: рівень буферизації відео, зміна бітрейту, швидкість сторінкових транзакцій, MOS для голосових сервісів, стабільність потокового з’єднання.

Для прогнозування часової динаміки навантаження в моделі буде використана рекурентна нейронна мережа типу LSTM, оскільки вона найкраще показала себе за точністю та здатністю моделювати довготривалі залежності. У модулі буде реалізовано обробку потоків телеметрії з подальшим отриманням короткострокового та середньострокового прогнозу. LSTM отримуватиме часові ряди KPI: навантаження каналів, кількість активних сеансів, коливання пропускної здатності та застосовуватиметься як основний алгоритм, оскільки статистичні моделі ARIMA/Prophet виявились менш ефективними для нелінійних 5G-середовищ. [23]

Для ідентифікації відхилень від нормального стану мережі буде використано Autoencoder, який реконструює нормальну поведінку трафіку та виявляє аномалії за значенням похибки реконструкції. Такий підхід забезпечить вищу стійкість до шуму та здатність працювати з великими обсягами телеметрії порівняно з Isolation Forest та One-Class SVM. У моделі Autoencoder працюватиме з багатовимірними вибірками flow-записів і статистичними характеристиками трафіку та функціонуватиме як механізм раннього попередження про можливі перевантаження, DoS-атаки чи нештатні режими обладнання.

Для класифікації потоків трафіку в моделі буде застосовано Random Forest, оскільки цей метод забезпечить найкраще співвідношення точності та інтерпретованості, а також стійкість до варіативності мережевих ознак. Random Forest використовуватиме flow-записи з вибраними ознаками: протокол, розмір пакетів, темп передачі, профіль застосунку та виконуватиме поділ потоків на функціональні класи: відео, голос, критичні IoT-повідомлення, сигнальний трафік. Після чого визначатиме рівень їх пріоритетності. Це дозволить системі прийняття рішень виділяти радіоресурси з урахуванням QoS-потреб.

Для оптимізації використання ресурсів та формування адаптивних політик — DQN. Він здатен забезпечити вибір оптимальних дій у складних багатофакторних сценаріях, характерних для 5G-мереж. Модуль приймає рішення щодо перерозподілу пропускної здатності, зміни параметрів радіодоступу або перенаправлення трафіку, враховуючи поточні KPI, прогнози LSTM, результати Random Forest і попередження Autoencoder.

Для оцінювання QoE використано гібридну модель LSTM + Dense, яка поєднує здатність LSTM працювати з часовими даними та можливість щільних шарів узагальнювати складні залежності між технічними параметрами та суб’єктивними метриками. Такий підхід дозволяє оцінювати вплив затримки, втрати кадрів, зміни пропускної здатності та інших факторів на реальний користувацький досвід. Модуль використовує часові ряди QoS-показників разом з прикладними параметрами сервісів та застосовується як індикатор того, чи коректно працюють модулі оптимізації та класифікації. [24]

Для наочного представлення принципів функціонування системи передачі даних п’ятого покоління було побудовано спрощену логічну модель 5G-мережі. Такий підхід дозволяє продемонструвати взаємодію ключових елементів архітектури, зокрема базових станцій, логічних функцій ядра мережі та кінцевих пристроїв користувачів, без використання зовнішніх бібліотек чи симуляторів. Модель відображає базову структуру мережі 5G та основні процеси, що відбуваються під час встановлення з’єднання, аутентифікації користувачів та маршрутизації трафіку.

Наведена на рисунку 3.3 програмна модель не претендує на повне відтворення складності реальної 5G-інфраструктури, проте слугує ефективним інструментом для демонстрації ключових механізмів її роботи. Вона відображає основні архітектурні принципи 5G-мереж: модульність, поділ площин, централізацію функцій керування та використання гнучкої маршрутизації через UPF.

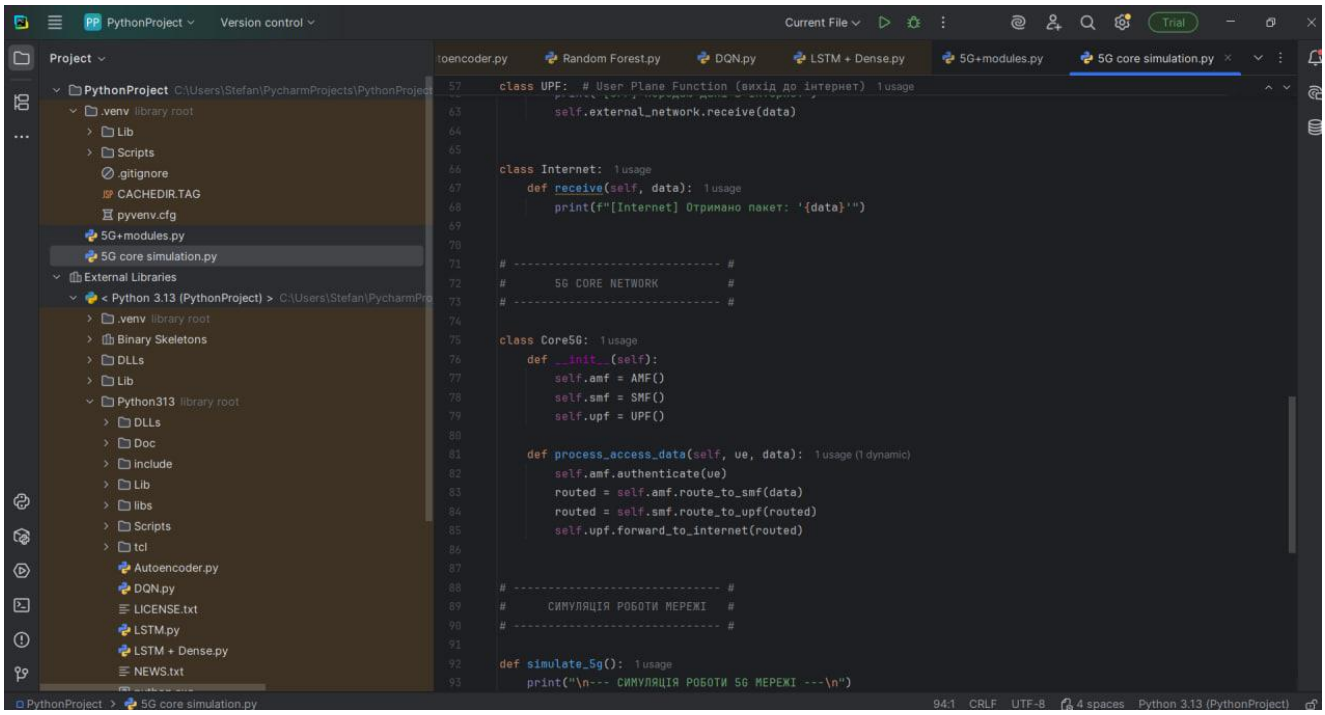


Рис. 3.3 Код тестової моделі 5G

3.2 Реалізація інтелектуальних методів у моделі системи передачі інформації

Реалізація інтелектуальних обчислювальних методів у моделі системи передачі інформації передбачає інтеграцію п’яти функціональних модулів ШІ, кожен із яких виконуватиме окрему аналітичну задачу, але одночасно взаємодіє з іншими компонентами мережевого середовища. Побудована архітектура забезпечуватиме можливість паралельної обробки даних, гнучкого масштабування й адаптивного налаштування моделей під різні режими функціонування мережі 5G.

Побудова модуля прогнозування мережевого навантаження ґрунтується на застосуванні рекурентної нейронної мережі типу LSTM, загальна архітектура якої зображена на рисунку 3.4. Використання LSTM дає змогу враховувати як короткострокові, так і довгострокові залежності в поведінці трафіку, що є критично важливим для систем передачі даних п’ятого покоління.

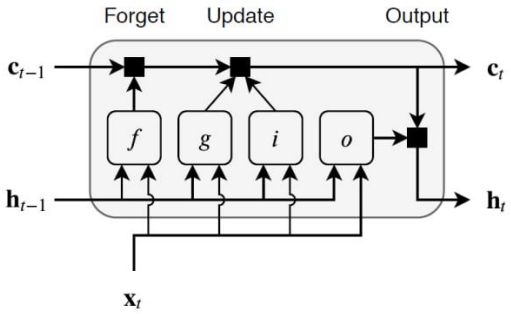


Рис. 3.4 Загальна архітектура LSTM

Архітектура модуля включає кілька LSTM-шарів, за якими розташовано щільний вихідний шар, що генерує прогнозоване значення навантаження. У процесі тренування використовується функція втрат типу MSE, а оптимізація здійснюється за допомогою алгоритму Adam, що забезпечує швидку адаптацію ваг при стабільній збіжності. На рисунку 3.5 представлено фрагмент коду, що демонструє реалізацію моделі LSTM засобами Python та бібліотеки TensorFlow.

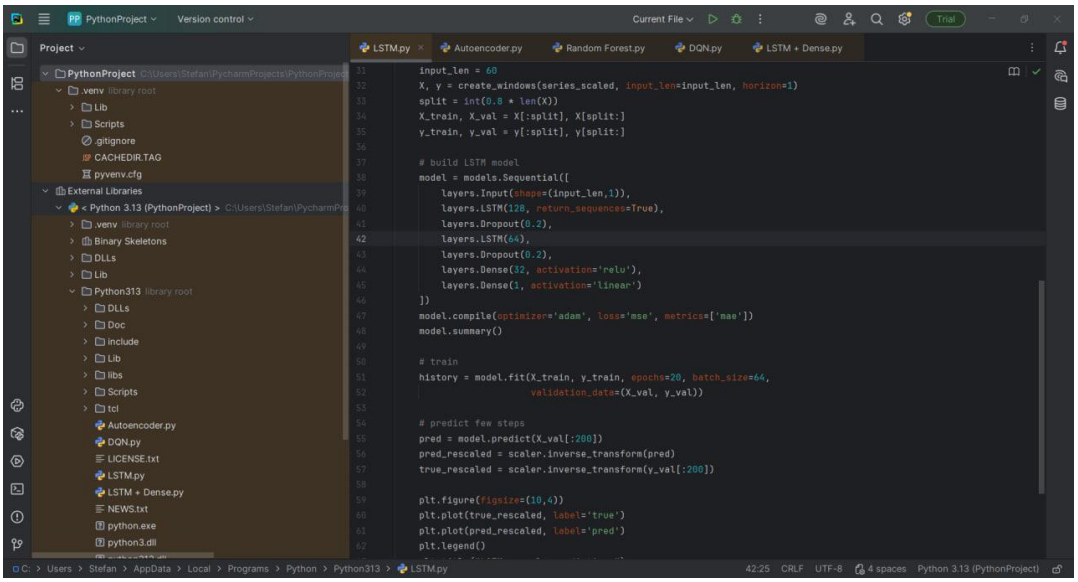


Рис. 3.5 Код моделі LSTM

Поданий код є основою програмної частини модуля та використовується для подальшого навчання та інтеграції з рештою системи.

Модуль виявлення аномальних станів мережі побудований на основі нейронної мережі типу Autoencoder, архітектура якого зображена на рисунку 3.6. Такий підхід є ефективним у випадках, коли кількість аномальних подій у вибірці є обмеженою або нерепрезентативною, а детальний опис потенційних відхилень заздалегідь відсутній.

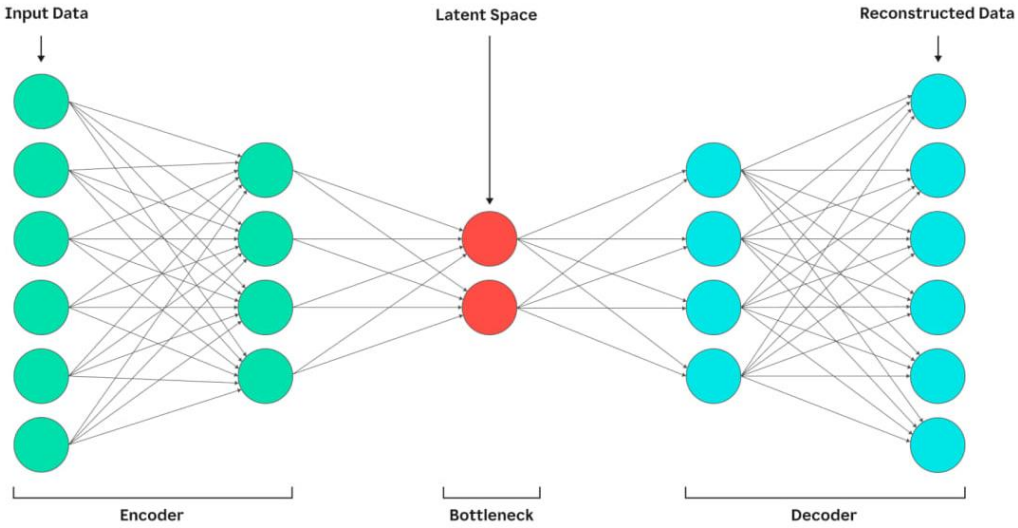


Рис. 3.6 Архітектура Autoencoder

Autoencoder складається з двох основних частин — енкодера та декодера. Енкодер виконує стискання початкових векторів телеметрії та виділяє їхні латентні ознаки, тоді як декодер відновлює вхідні дані на основі отриманого компактного представлення. При тренуванні мережі мінімізується різниця між початковим і відновленим сигналом, що забезпечує формування моделі «нормальної» поведінки мережі.

Для виявлення аномалій використовується помилка реконструкції: якщо значення відновленого сигналу суттєво відрізняється від вихідного, спостереження вважається аномальним. Такий підхід дозволяє виявляти широкий спектр нестандартних подій — від нетипових коливань трафіку до потенційних інцидентів на рівні пропускної здатності або QoS.

На рисунку 3.7 наведено програмну реалізацію автоенкодера мовою Python із використанням бібліотеки TensorFlow. Поданий код демонструє архітектуру моделі та її компіляцію, що становить основу для подальшого навчання та інтеграції в систему моніторингу.

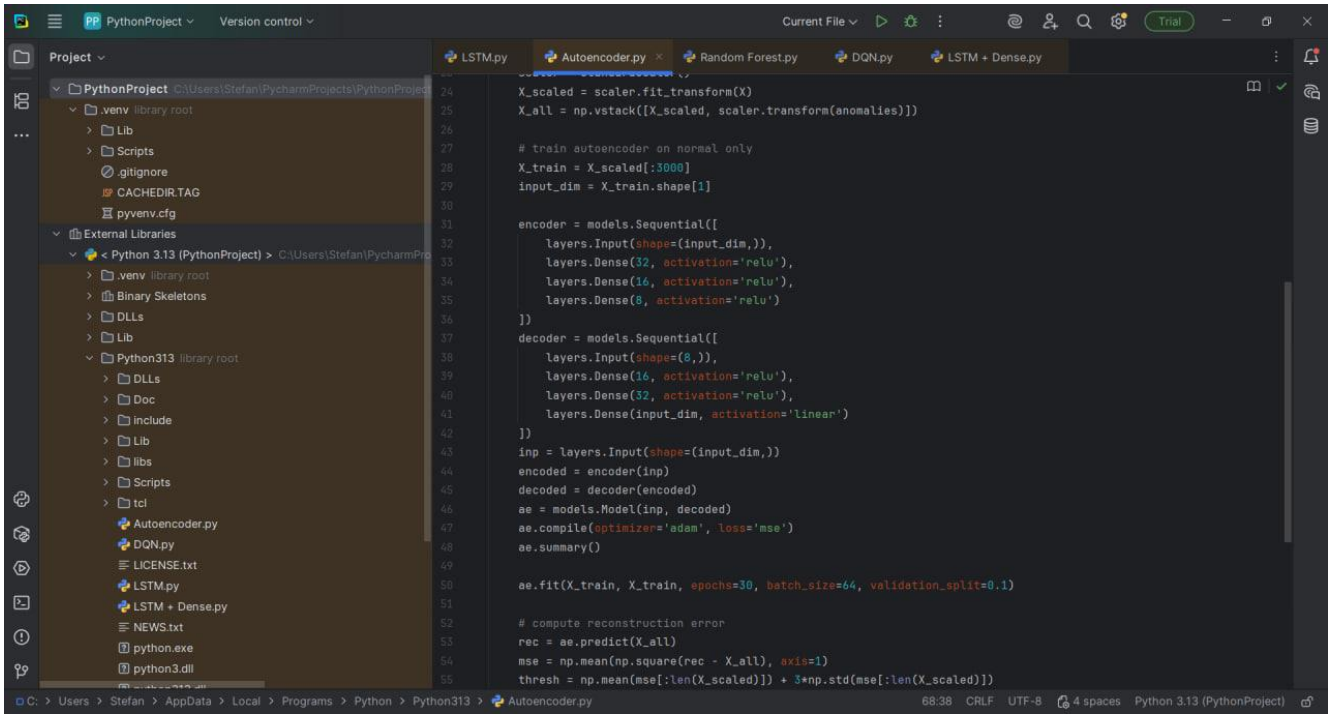


Рис. 3.7 Код Autoencoder

Модуль класифікації та пріоритизації мережевого трафіку призначений для автоматичного визначення типу переданих потоків і присвоєння їм відповідного рівня обслуговування. Для реалізації даного компонента використано алгоритм Random Forest, архітектуру зображено на рисунку 3.8, ансамблевий метод машинного навчання, що демонструє високу ефективність при роботі з табличними даними та нерівномірними вибірками.

Основна ідея Random Forest полягає у побудові множини незалежних дерев рішень, кожне з яких навчається на випадковій підмножині ознак та прикладів навчальної вибірки. Така технологія значно зменшує ризик перенавчання та забезпечує стабільні результати навіть у випадку наявності шумових або частково корельованих параметрів трафіку. Під час класифікації рішення приймається

шляхом голосування між усіма деревами, що підвищує надійність отриманих результатів.

У модулі передбачено попередню обробку flow-параметрів. Отримані ознаки надходять до класифікаційної моделі, яка призначає кожному потоку відповідний клас. На основі цього класу система формує рівень пріоритетності та визначає, чи потребує потік підвищеної якості обслуговування.

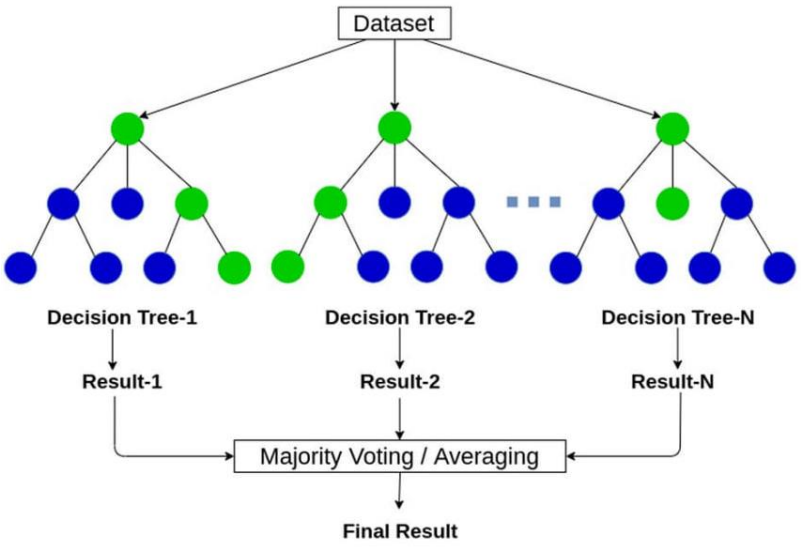


Рис. 3.8 Архітектура Random Forest

На рисунку 3.9 наведено фрагмент програмної реалізації моделі Random Forest у Python.

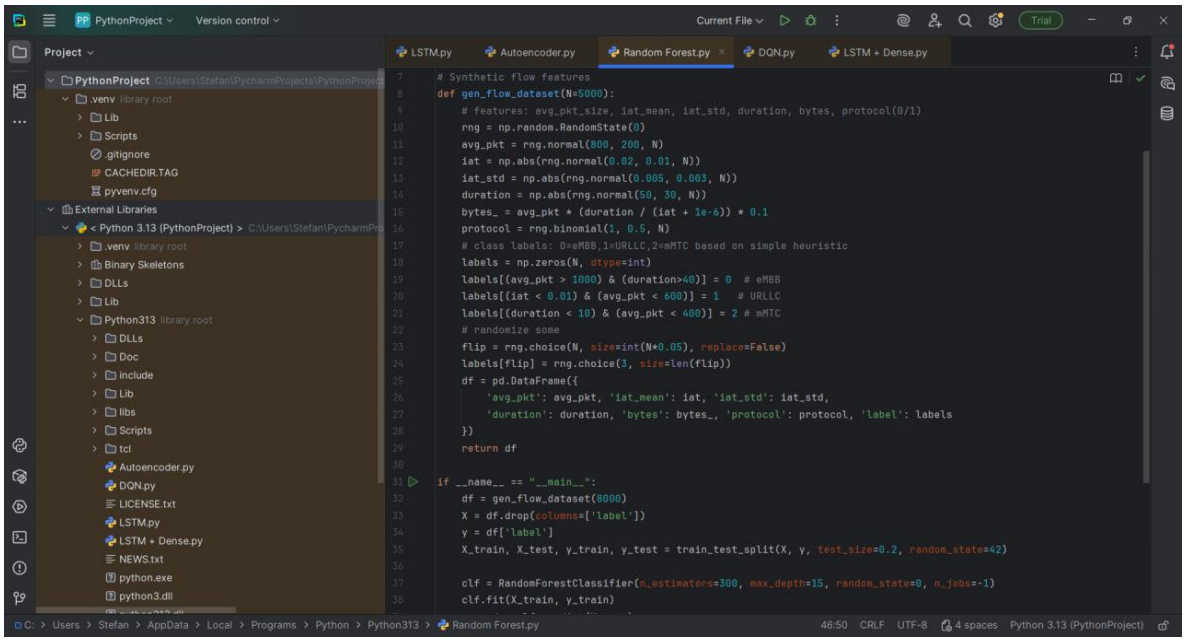


Рис. 3.9 Код Random Forest

Представлений код демонструє базову конфігурацію алгоритму, що використовується для класифікації потоку даних у рамках розробленої моделі системи передачі інформації.

Модуль прийняття рішень у моделі системи передачі інформації базується на методі DQN, який належить до класу алгоритмів навчання з підкріпленням. Основним завданням цього модуля є вибір оптимальних дій у змінному мережевому середовищі, зокрема під час керування ресурсами, маршрутизації або динамічного перерозподілу пропускної здатності.

У рамках моделювання агент DQN взаємодіє з віртуальним середовищем 5G-мережі, яке генерує як стани, так і зворотний зв'язок у вигляді винагороди — кількісної оцінки ефективності обраної дії. Глибинна нейронна мережа в DQN використовується для апроксимації Q-функції, що дає можливість приймати рішення у станах високої розмірності, які неможливо охопити табличними методами.

Процес навчання полягає у поступовому накопиченні досвіду та оновленні параметрів моделі на основі буфера досвіду. Такий підхід запобігає кореляції між сусідніми зразками та підвищує стабільність навчання. Крім того, застосовується механізм «цільової мережі», що дозволяє уникнути нестійкості під час оновлення прогнозованих значень Q-функції.

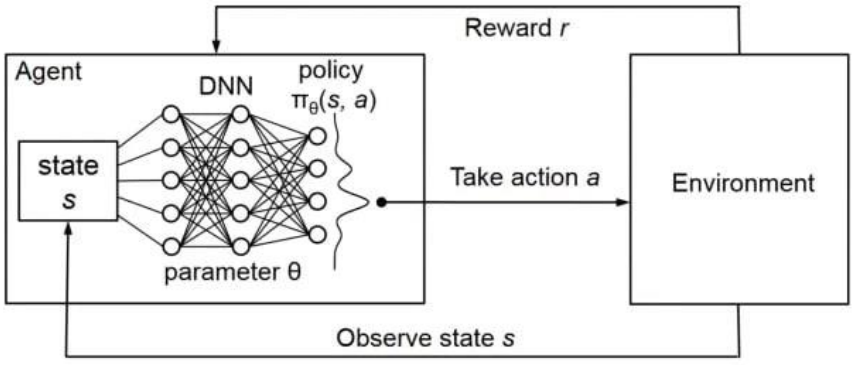


Рис. 3.10 Архітектура DQN

У структурній схемі модуля зображено його ключові елементи: механізм спостереження станів, нейронну модель DQN, буфер досвіду, функцію винагороди

та механізм вибору дії, що забезпечує баланс між дослідженням середовища та використанням набутих знань.

На рисунку 3.11 наведено фрагмент коду реалізації DQN у Python. Він демонструє елементарну конфігурацію агента, включаючи опис архітектури нейронної мережі, функції оновлення та механізму вибору дій.

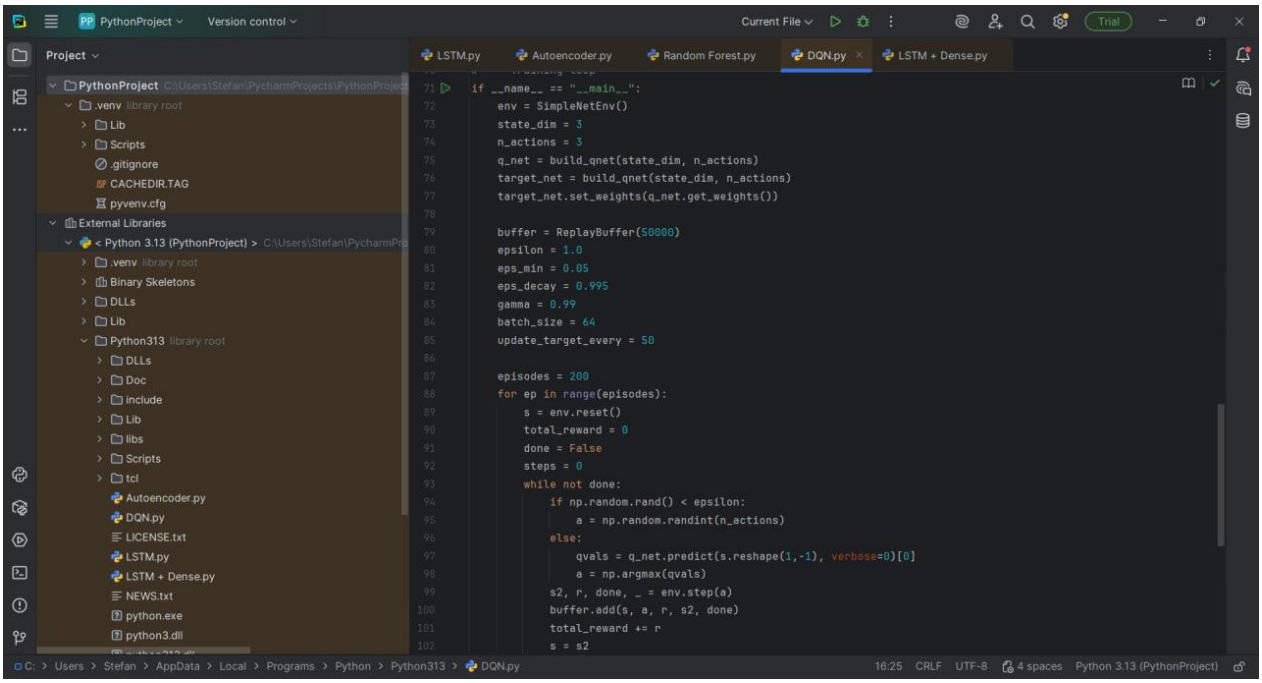


Рис. 3.11 Код моделі DQN

Модуль оцінювання QoE призначений для прогнозування суб’єктивних показників користувацького сприйняття сервісу на основі аналізу мережевих параметрів. На відміну від модулів, що працюють із суто технічними метриками, цей компонент моделює поведінку кінцевого користувача та оцінює такі показники, як MOS або інтегральні індекси комфортності перегляду відео та використання сервісів реального часу.

Для побудови моделі використано гібридний підхід LSTM + Dense. LSTM-шар обробляє часову динаміку мережевих параметрів — таких як зміна затримки, джитеру, швидкості передачі чи відсотка втрати пакетів. Завдяки здатності LSTM зберігати інформацію про попередні стани, модель може враховувати як короткочасні, так і довготривалі відхилення у якості мережі. Після обробки через

LSTM-послідовність дані передаються до декількох повнозв'язних шарів, які виконують регресійне передбачення кінцевого показника QoE.

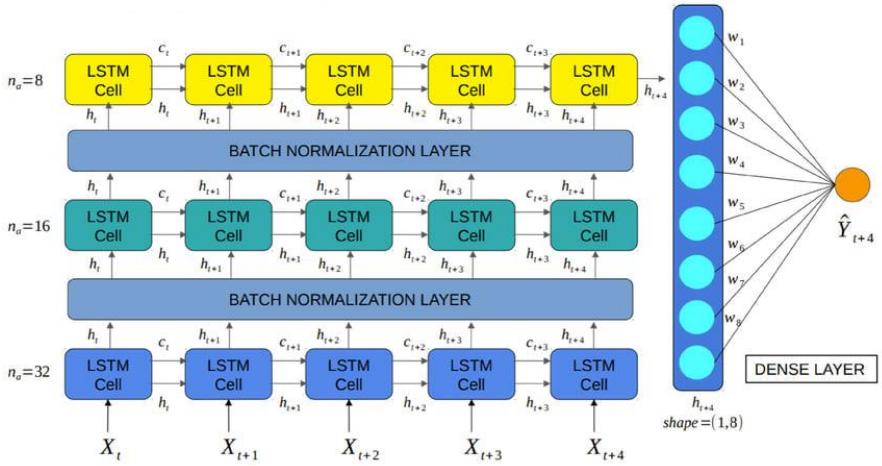


Рис. 3.12 Архітектура гібридної моделі LSTM + Dense

Алгоритм роботи модуля включає декілька ключових елементів: формування часових вікон з KPI мережі, нормалізацію даних, побудову та навчання моделі, а також перевірку її роботи на тестових наборах. На структурній схемі модуля відображено основні блоки: буфер збору даних, LSTM-блок для аналізу часових залежностей, Dense-блок для отримання кінцевої регресійної оцінки та модуль обчислення похибок.

На рисунку 3.13 наведено фрагмент коду, який ілюструє реалізацію цього підходу в Python.

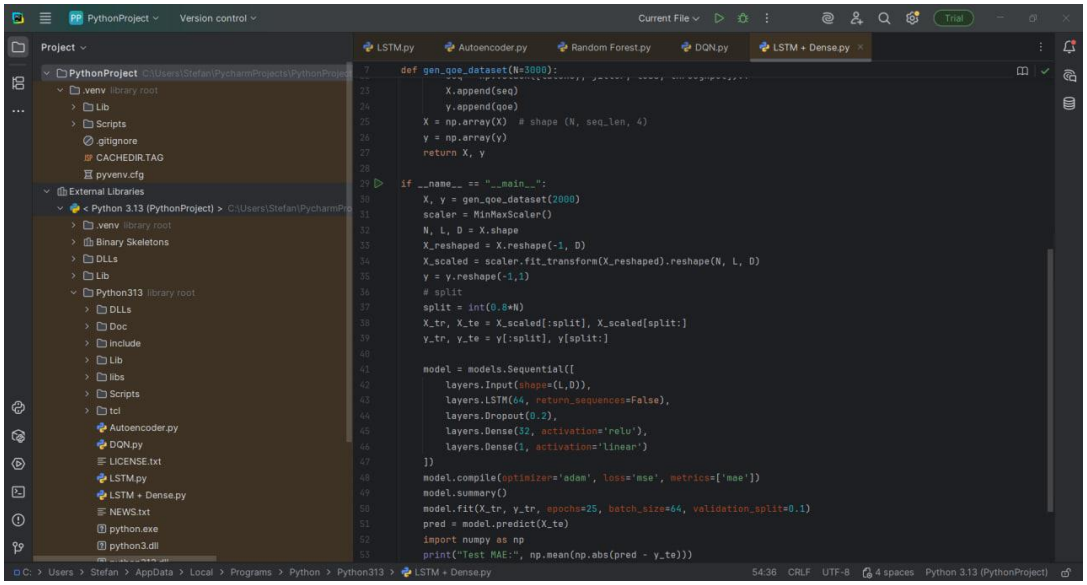


Рис. 3.13 Код гібридної моделі LSTM + Dense

Код демонструє процес побудови гібридної нейронної моделі, визначення параметрів навчання та формування вихідних прогнозів.

Інтеграція окремих інтелектуальних компонентів у цілісну симуляційну модель є ключовим етапом побудови системи, здатної відтворювати реальні процеси функціонування сучасної інфокомунікаційної мережі, фрагмент коду моделі 5G з інтеграцією модулів ШІ зображено на рисунку 3.14. На цьому рівні модулі прогнозування, виявлення аномалій, класифікації трафіку, прийняття рішень та оцінювання якості обслуговування працюють у взаємозв'язку, формуючи єдину аналітичну екосистему. Кожен з них виконує свою функцію, однак кінцевий результат формується лише завдяки їх узгодженій взаємодії.

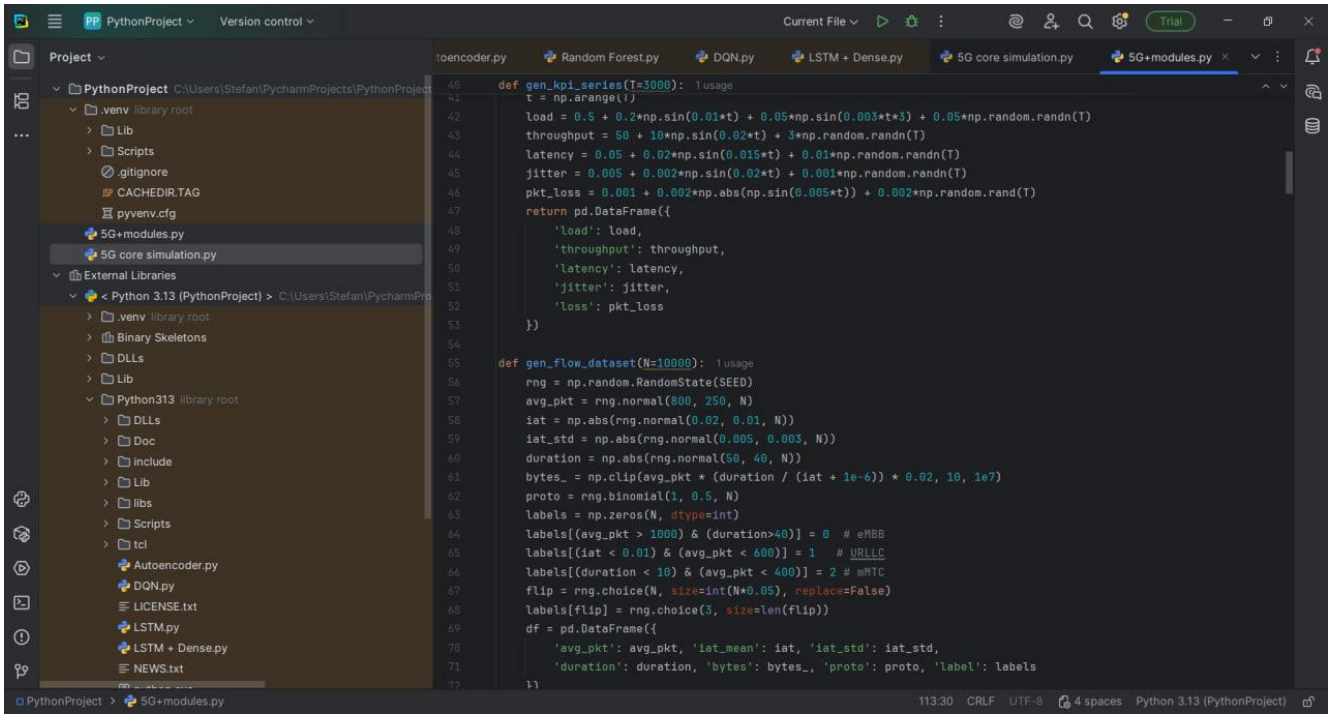


Рис. 3.14 Код системи передачі інформації з інтегрованими модулями ШІ

Загальний сценарій обробки даних у моделі починається з генерації мережевого трафіку, який надходить до блока моніторингу та телеметрії. На цьому етапі формуються часові ряди KPI та параметри окремих потоків, що слугують вхідними даними для всіх інтелектуальних модулів. Першим активується модуль прогнозування на основі LSTM-мережі, який визначає очікуване майбутнє

навантаження та можливі пікові зміни. Отримані прогнози дозволяють системі заздалегідь адаптувати параметри маршрутизації та розподілу ресурсів.

Паралельно працює модуль Autoencoder, який аналізує поточний стан мережі та визначає відхилення від нормального профілю трафіку. Якщо модуль виявляє аномалію, це сигналізує підсистемі прийняття рішень про необхідність коригування політики керування. Наступним елементом є модуль класифікації трафіку, який за допомогою алгоритму Random Forest визначає типи потоків та їх пріоритетність. Це підсилює здатність моделі оптимально розподіляти ресурси залежно від критичності додатків або сервісів.

Результати трьох попередніх модулів об’єднуються в блоці прийняття рішень, де агент DQN формує оптимальну стратегію керування мережею. DQN-агент оцінює стан мережі на основі поєднання прогнозів, аномалій та класифікаційних міток і вибирає такі дії, що мінімізують затримки, втрати пакетів та перевантаження окремих сегментів мережі.

Завершальним етапом є модуль оцінювання QoE, який використовує гібридну модель LSTM + Dense для визначення, як зміни в мережевих параметрах впливають на суб’єктивну якість обслуговування кінцевого користувача. Це дозволяє оцінити, наскільки обрана стратегія керування реально покращує користувацький досвід, а не лише технічні показники.

Таким чином, інтеграція всіх модулів забезпечує узгоджене функціонування симуляційної системи, у якій результати одного компонента безпосередньо впливають на рішення інших. Такий підхід дозволяє відтворити складну поведінку сучасних 5G-мереж та забезпечує можливість комплексного аналізу ефективності застосування інтелектуальних методів у процесах передачі інформації.

3.3 Аналіз результатів моделювання та оцінювання ефективності запропонованих методів

Оцінювання ефективності запропонованих інтелектуальних методів здійснюватиметься на основі уніфікованої методики, яка забезпечить коректність

порівняння результатів. Для цього було сформовано набір критеріїв якості, що характеризують точність роботи алгоритмів, їхню адаптивність до змін у мережевих умовах та відповідність вимогам моделювання. [30]

Передусім визначено перелік метрик продуктивності, які застосовувалися залежно від типу моделі. Для модулів класифікації мережевого трафіку використовуватимуться такі показники:

- Точність – частка правильно класифікованих зразків.
- Точність – частка коректно визначених позитивних результатів серед усіх позитивних класифікацій.
- Повнота – частка виявлених релевантних об’єктів серед усіх реально наявних.
- F1-міра – гармонійне середнє точності та повноти, яке дає збалансовану оцінку для моделей з дисбалансом класів.

Для моделей прогнозування навантаження використовуватимуться такі метрики:

- Середня абсолютна помилка – середня величина відхилення прогнозу від реального значення.
- Середньоквадратична помилка – середній квадрат різниці між прогнозом і фактом, чутлива до великих відхилень.
- Середня абсолютна відносна помилка – середнє відсоткове відхилення прогнозу від реального значення.

Для моделей виявлення аномалій застосовуватимуться показники:

- Рівень хибних спрацьовувань – частка нормальних подій, помилково визначених як аномалії.
- Рівень пропуску аномалій – частка реальних аномалій, які модель не змогла розпізнати.
- Площа під ROC-кривою – узагальнений показник здатності моделі відокремлювати нормальну активність від нестандартної.

Додатково враховуватиметься затримка обробки, що характеризує час, необхідний моделі для формування рішення. Цей параметр є критично важливим для систем, що працюють у режимі близькому до реального часу.

Окреме місце в методиці займають критерії адекватності моделі, що включають відповідність результатів очікуваним трендам, стійкість до флуктуацій вхідних даних та стабільність роботи за умов зміни інтенсивності трафіку.

Модуль прогнозування мережевого навантаження на основі рекурентної нейронної мережі типу LSTM був використаний для оцінки динаміки зміни трафіку в 5G-мережі за часовими інтервалами, що зображено на рисунку 3.15.

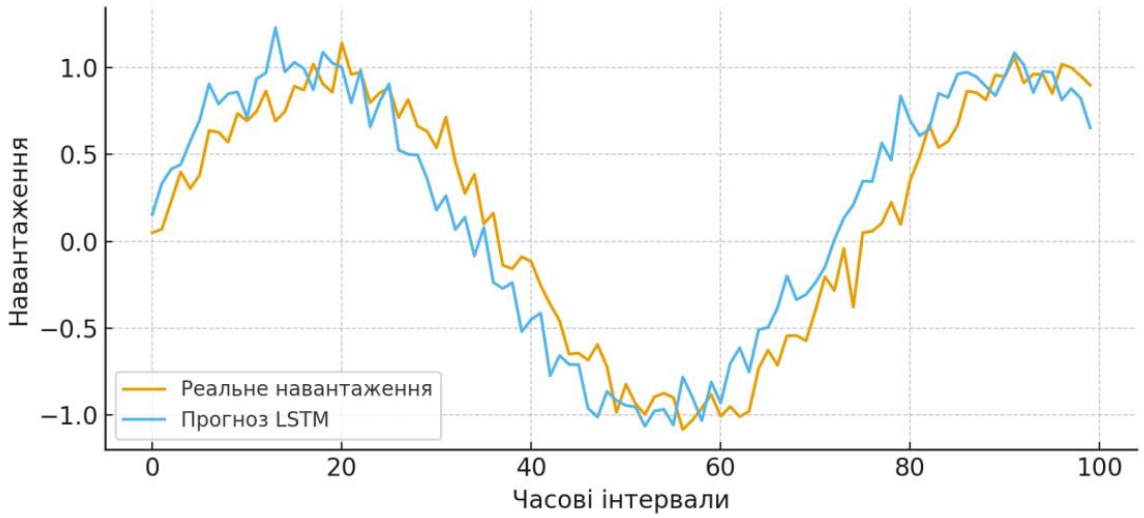


Рис. 3.15 Графік застосування LSTM

У ході аналізу встановлено, що модель демонструє стабільну здатність відтворювати загальні тренди та локальні коливання навантаження. Помилки прогнозу залишаються в межах допустимих значень для інфокомунікаційних систем, що свідчить про коректність навчання та узгодженість обраної архітектури з характером даних. Виявлено, що найкращі результати досягаються при використанні ковзного вікна фіксованого розміру та регуляризації, що знижує ризик перенавчання на пікових значеннях трафіку.

Основною метою моделювання є здатність алгоритму відтворювати короткострокові та середньострокові тенденції, що є критично важливим для

адаптивного планування ресурсів, балансування навантаження та запобігання перевантаженням.

Модуль виявлення аномальних станів мережі, реалізований на основі автоенкодера, був інтегрований у симуляційне середовище для аналізу поведінки трафіку 5G-мережі в умовах наявності як нормальних, так і аномальних потоків. Основною метою експерименту було оцінити здатність моделі виявляти відхилення у структурі даних, що характеризують стан мережевих ресурсів.

У процесі моделювання автоенкодер навчався на вибірці нормального трафіку, що дозволило моделі сформувати латентне подання притаманних йому закономірностей. Після навчання мережа була протестована на даних, що містили як коректні стани мережі, так і контрольовано згенеровані аномальні точки. Графік з використанням моделі зображено на рисунку 3.16.

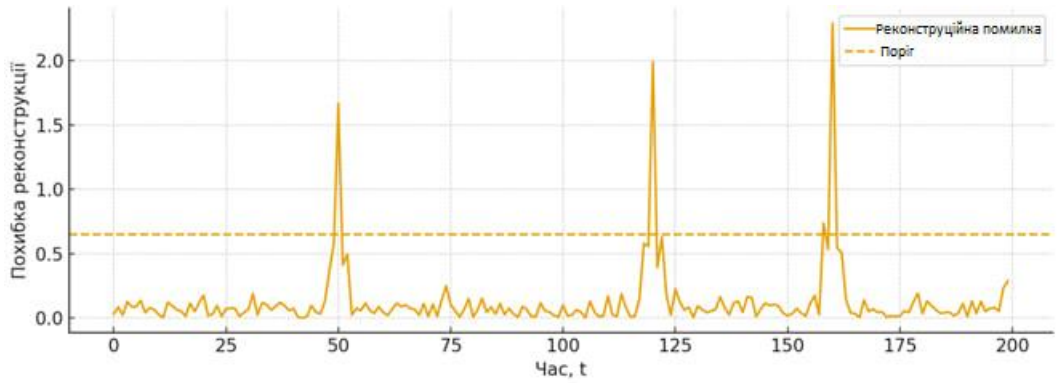


Рис. 3.16 Графік застосування Autoencoder

Отримані результати демонструють, що реконструкційна похибка суттєво зростає у випадках, коли вхідний вектор містить характеристики, нетипові для нормального профілю навантаження. Загалом результати моделювання показують, що автоенкодер забезпечує високий рівень розпізнавання аномальних станів. Це підтверджує доцільність використання автоенкодера у системах автоматизованого моніторингу та раннього виявлення порушень у системах передачі інформації.

Метод Random Forest застосовано в якості інтелектуального механізму класифікації потоків трафіку в симуляційній моделі моніторингу мережі. Для відображення роботи Random Forest на рисунку 3.17 представлено матрицю з класифікацією даних.

Отримані результати свідчать про те, що метод Random Forest забезпечує високу класифікаційну здатність навіть за наявності шумових або неповних значень у вибірці. Модель ефективно розділяє класи не лише за статистичними параметрами трафіку, але й за більш комплексними ознаками, що є важливим у задачах виявлення аномалій у гетерогенних середовищах.



Рис. 3.17 Матриця класифікації трафіку сформована за допомогою Random Forest

Помилки класифікації розподіляються нерівномірно та відповідають очікуваним особливостям мережевого навантаження. Найчастіше модель плутає відео та голосові потоки, що пояснюється їх частково подібними статистичними характеристиками. IoT-трафік має найвищу розпізнаваність, оскільки характеризується специфічними, добре відокремленими патернами у часових рядах і параметрах пакетів.

Результати роботи модуля прийняття рішень, реалізованого на основі алгоритму DQN, який був інтегрований у симуляційну модель системи передачі інформації наведені в таблиці 3.1. Використання підходів підкріплювального навчання дає змогу агенту виробляти оптимальні дії на основі накопиченого досвіду взаємодії з мережею, що особливо важливо за умов змінного навантаження та нерівномірного розподілу потоків трафіку.

У процесі моделювання DQN-агент послідовно оцінював стан мережевої підсистеми за кількома індикаторами, зокрема рівнем завантаження каналу,

характеристиками затримки та часткою втрат пакетів. На основі цих параметрів агент оновлював наближення Q-функції та визначав дію, яка забезпечує максимальну очікувану вигоду для подальшого функціонування системи.

Таблиця 3.1

Реакції агента DQN на зміни в мережі

Крок епізоду	Вхідний стан	Дія агента	Оцінка Q(s, a)	Негайна винагорода	Коментар
1	Завантаження каналу: 0.72 Затримка: 45мс Втрати: 0.8%	Перемикання на канал 2	0.63	+0.4	Агент уникає перевантаження каналу
15	Завантаження каналу: 0.35 Затримка: 20мс Втрати: 0.2%	Залишитися на поточному каналі	0.81	+1.0	Оптимальний стан, стабільний трафік
27	Завантаження каналу: 0.88 Затримка: 67мс Втрати: 1.4%	Балансування на канал 3	0.57	+0.2	Агент реагує на різке збільшення навантаження
34	Завантаження каналу: 0.51 Затримка: 28мс Втрати: 0.3%	Пріоритизація критичного трафіку	0.76	+0.9	Знижує ризики деградації QoS
48	Завантаження каналу: 0.69 Затримка: 40мс Втрати: 0.6%	Корекція параметрів черги	0.70	+0.7	Запобігає накопиченню черги
60	Завантаження каналу: 0.92 Затримка: 80мс Втрати: 2.1%	Аварійне перемикання на резервний канал	0.49	–0.1	Критична ситуація, мінімізація втрат

Наведені результати засвідчують, що застосування DQN-агента забезпечує здатність моделі до динамічного пристосування у відповідь на зміни в мережевому

середовищі. Агент поступово формує поведінкову стратегію, у якій поєднуються процеси дослідження нових рішень та використання вже накопичених знань. Це дозволяє реагувати не лише на миттєвий стан системи, але й враховувати очікуваний ефект у перспективі кількох кроків.

На рисунку 3.18 зображено графік ефективності застосування гібридної моделі LSTM + Dense, яка виконує оцінювання параметра, QoE на основі часових рядів мережевих показників.



Рис. 3.18 Графік застосування LSTM + Dense

Побудована модель використовує як вхідні дані багатовимірний набір мережевих ознак, включно з показниками затримки, варіації затримки, пропускної здатності, рівня втрат пакетів та індексу завантаження каналу. Після обробки на рівні LSTM-ціпочки отриманий просторово-часовий вектор передається до Dense-шару, який формує скалярну оцінку QoE. Такий підхід дозволяє врахувати як миттєвий стан мережі, так і накопичувані історичні ефекти, що особливо важливо для задач безперервного моніторингу в 5G-інфраструктурі.

Проведене дослідження підтверджує ефективність та практичну придатність розглянутої моделі, що демонструє її відповідність вимогам для інтеграції в сучасні симуляційні середовища. Отримані результати свідчать про те, що модель може

бути успішно використана як основа для розробки механізмів динамічного та адаптивного керування мережевими ресурсами, зокрема в мережах нового покоління. Виявлена масштабованість та гнучкість підходу відкриває можливості для подальшої апробації, розширення функціональності та впровадження інтелектуальних алгоритмів оптимізації параметрів мережі, що підсилює його цінність для практичних інженерних застосувань і майбутніх наукових досліджень.

ВИСНОВКИ

У першому розділі здійснено комплексний огляд теоретичних засад систем передачі інформації та проаналізовано ключові принципи їх функціонування, включаючи структуру каналів зв’язку, методи модуляції, забезпечення якості обслуговування та особливості роботи з багатовимірними потоками даних. Розглянуто сучасні технології інфокомунікаційних систем, серед яких виділено високошвидкісні транспортні архітектури, мережі нового покоління та інтегровані програмно-керовані рішення, що визначають актуальні напрямки розвитку галузі. Окрему увагу приділено аналізу потенціалу використання штучного інтелекту у системах зв’язку: показано, що інтелектуальні методи здатні суттєво підвищувати ефективність управління мережею, забезпечувати адаптивність до змін навантаження та покращувати показники QoS і QoE. Узагальнення сучасного стану технологій дозволило визначити науково-практичну проблему, на вирішення якої спрямовано подальші розділи роботи.

У другому розділі було здійснено комплексний аналіз сучасних підходів до побудови систем передачі інформації, який охоплює як архітектурні принципи організації інфокомунікаційних мереж, так і методи забезпечення їхньої надійності та ефективності. Розглянуто ключові механізми підвищення стійкості мережових структур, включно з оптимізацією маршрутизації, управлінням якістю обслуговування та використанням телеметричних даних для контекстно-орієнтованого управління. Окрему увагу приділено дослідженню інтелектуальних методів оптимізації, серед яких статистичні моделі, методи машинного навчання та алгоритми глибинного й підкріплювального навчання. Проведений огляд дав змогу визначити переваги та обмеження кожного з підходів, а також сформувати обґрунтовані критерії вибору методів, що будуть інтегровані у модель системи передачі інформації в наступному розділі.

У третьому розділі застосовано комплекс інтелектуальних методів для підвищення ефективності системи передачі інформації, що включало побудову

моделі мережі з урахуванням динаміки трафіку, реалізацію алгоритмів ШІ різних типів та оцінювання їх впливу на ключові показники функціонування. Було інтегровано модуль класифікації потоків трафіку на основі Random Forest, що дозволило підвищити точність визначення мережевих станів; модуль прийняття рішень на базі DQN-агента, який забезпечив адаптивний вибір оптимальних дій у змінних умовах; а також гібридну модель LSTM + Dense для прогнозування показників QoE та раннього виявлення потенційних деградацій якості обслуговування. Проведене моделювання охоплювало порівняння обраних методів, аналіз коректності їх роботи, візуалізацію результатів та оцінку можливості їх практичного застосування у телекомунікаційних системах. Отримані результати підтвердили здатність інтелектуальних підходів підвищувати стабільність, адаптивність і продуктивність системи передачі інформації в умовах змінних навантажень.

Ключові моменти дослідження за темою кваліфікаційної магістерської роботи «Дослідження методів побудови системи передачі інформації із застосуванням штучного інтелекту» викладено у тезах на науково-практичних конференціях, що забезпечило апробацію отриманих результатів і підтвердило їх наукову новизну та практичну значущість. У межах роботи проаналізовано сучасні підходи до інтеграції алгоритмів ШІ у системи передачі даних, визначено їх переваги та недоліки, а також розроблено рекомендації щодо підвищення ефективності та надійності таких систем. Отримані результати становлять цінну основу для подальших досліджень і можуть бути використані при створенні інтелектуальних інфокомунікаційних рішень нового покоління.