ДЕРЖАВНИЙ УНІВЕРСИТЕТ
"КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

Кваліфікаційна наукова
праця на правах рукопису

Фесенко Владислав Олексійович

УДК 621.396.43

ДИСЕРТАЦІЯ

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ МОБІЛЬНИХ МЕРЕЖ ЗВ′ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

за спеціальністю 172 «Телекомунікації та радіотехніка»
галузь знань 17 «Електроніка та телекомунікації»

Подається на здобуття ступеня доктора філософії

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

_____В.О. Фесенко
(підпис, ініціали та прізвище здобувача)

Науковий керівник: Одарченко Роман Сергійович,
доктор технічних наук, професор

КИЇВ – 2025

АНОТАЦІЯ

Фесенко В.О. Методи підвищення ефективності функціонування мобільних мереж зв′язку спеціального призначення. − Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії зі спеціальності 172 «Телекомунікації та радіотехніка» галузі 17 «Електроніка та телекомунікації» . – Державний університет “Київський авіаційний інститут“, Київ, 2025.

У дисертаційній роботі досліджено теоретичні засади та практичні аспекти підвищення ефективності функціонування мобільних мереж зв’язку спеціального призначення, зокрема з урахуванням впровадження архітектури 5G. Сучасні тенденції розвитку систем урядового радіозв’язку потребують комплексного підходу до проєктування, управління ресурсами, гарантування якості обслуговування (QoS), інформаційної безпеки та стійкості до загроз. В роботі запропоновано концептуальну архітектуру та аналітичні моделі, які дозволяють задовольнити вимоги до мобільних комунікацій критичного призначення.

Обґрунтовано доцільність використання технології 5G як базової платформи для створення мереж урядового зв’язку нового покоління. Зроблено акцент на ключових компонентах архітектури: мережевих функціях (AMF, SMF, UPF, PCF, AUSF, UDM), сервісно-орієнтованому підході (SBA), можливості створення ізольованих логічних сегментів за допомогою Network Slicing, застосуванні відкритих інтерфейсів, підтримці критичних сервісів MCX (MCPTT, MCData, MCVideo). Наведено модель побудови архітектури із застосуванням мікросервісів, віртуалізації функцій (NFV) та програмно-конфігурованих мереж (SDN).

Особливу увагу приділено забезпеченню захищеності системи. Розглянуто процедури автентифікації на основі 5G-AKA/EAP-AKA′, алгоритми обміну ключами (KSEAF, KAMF, KRSF), використання захищених протоколів NAS та можливості інтеграції інфраструктури відкритих ключів (PKI). Представлено

узагальнені схеми двофазної автентифікації для урядових терміналів, включаючи підтримку стійких до загроз каналів.

Розроблено метод планування мережі зв’язку спеціального призначення з урахуванням просторово-частотних обмежень, карти рельєфу, типу місцевості (місто, передмістя, відкрита місцевість), розподілу навантаження, резервування каналів та критичності обслуговування. Проведено частотне планування із залученням рекомендацій ITU-R та моделей поширення сигналу 3GPP TR 38.901. Проаналізовано використання RIS (reconfigurable intelligent surfaces) та THz-комунікацій для підвищення надійності покриття у складних умовах.

Запропоновано багаторівневу QoS/SLA-інфраструктуру для управління пріоритетами обслуговування в залежності від категорії користувачів (цивільні, урядові, силові структури), критичності сервісу, затримки, пропускної здатності та інших KPI/KQI. Розроблено симуляційні моделі, які дозволяють враховувати динаміку навантаження та адаптивне резервування. Введено метод оцінювання ефективності мережі за допомогою гібридного підходу — поєднання пасивного моніторингу, активних вимірювань та аналізу пробної затримки.

Наукова новизна полягає у: формуванні нової архітектури ядра мережі спеціального призначення на базі 5G; побудові методики планування мережі з урахуванням особливостей топографії та сценаріїв надзвичайних ситуацій; створенні багаторівневої QoS/SLA-інфраструктури для спеціального зв’язку; моделюванні функціонування урядової мережі з урахуванням автентифікації, безпеки, ізоляції сервісів та резервування. Практичне значення результатів дисертаційної роботи підтверджено їх впровадженням у навчальний процес, тестуванням на імітаційних стендах, а також можливістю адаптації під реальні проєкти з цифровізації безпекової інфраструктури.

Ключові слова: мобільні мережі спеціального призначення, критична інфраструктура, критична інформаційна інфраструктура, кібербезпека, кіберзагрози, інформаційно-телекомунікаційна система, критична інфраструктура на базі 5G, критерії оцінки безпеки, функціональний профіль безпеки, оцінка загроз, хмарна архітектура, технологія 5G, мобільний зв’язок 5G, архітектура

мережі, конфіденційність в мобільному зв’язку, канал зв’язку, безпілотні літальні апарати, аналіз ефективності мобільної мережі, доступність сервісів, математичне моделювання процесів у мережі, процеси в телекомунікаціях, бездротові комунікаційні системи, терагерцовий зв’язок, аналітичний огляд телекомунікаційних технологій, застосування мереж спеціального призначення, урядовий радіозв’язок, супутниковий сегмент мобільної мережі, антенні системи, система бездротової передачі даних, криптографічний захист, мобільний ультраширокий зв’язок, методи модуляції в мобільному зв’язку, методи кодування сигналів, соціально-кіберфізичні комунікаційні системи, машинне навчання в телекомунікаціях, нейронні мережі для цифрових модуляцій, адаптивна маршрутизація в критичних мережах, автентифікація в 5G, KPI/KQI, SDN, NFV, QoS/SLA, Network, сервіси місієкритичного зв’язку, RIS, критичні комунікації, мікросервісна архітектура в 5G.

ANNOTATION

Fesenko V.O. Methods for Improving the Efficiency of Operation of Special-Purpose Mobile Communication Networks – Qualification research manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 172 "Telecommunications and Radio Engineering" in field 17 "Electronics, Automation and Telecommunications" State University “Kyiv Aviation Institute”, Kyiv, 2025.

This dissertation explores theoretical foundations and practical aspects of improving the efficiency of special-purpose mobile communication networks, particularly considering the implementation of 5G architecture. Modern trends in the development of governmental radio communication systems require a comprehensive approach to design, resource management, quality of service (QoS) assurance, information security, and threat resilience. The work proposes a conceptual architecture and analytical models that meet the requirements of mission-critical mobile communications.

The feasibility of using 5G technology as the foundational platform for next-generation government networks is substantiated. Emphasis is placed on key architectural components: network functions (AMF, SMF, UPF, PCF, AUSF, UDM), the service-based approach (SBA), the ability to create isolated logical segments via Network Slicing, the use of open interfaces, and support for mission-critical services MCX (MCPTT, MCData, MCVideo). A model of network architecture construction is presented using microservices, network function virtualization (NFV), and software-defined networking (SDN).

Particular attention is given to ensuring system security. Authentication procedures based on 5G-AKA/EAP-AKA′, key exchange algorithms (KSEAF, KAMF, KRSF), secure NAS protocols, and public key infrastructure (PKI) integration possibilities are analyzed. Generalized two-phase authentication schemes for government terminals are proposed, including support for threat-resilient communication channels.

A method for planning special-purpose networks is developed considering spatial-frequency constraints, terrain mapping, land type (urban, suburban, open), load distribution, channel reservation, and service criticality. Frequency planning was conducted using ITU-R recommendations and 3GPP TR 38.901 propagation models. The use of RIS (reconfigurable intelligent surfaces) and THz communications is analyzed to improve coverage reliability in challenging environments.

A multi-level QoS/SLA infrastructure is proposed for managing service priorities based on user categories (civilian, governmental, security forces), service criticality, latency, throughput, and other KPI/KQI indicators. Simulation models were developed to account for load dynamics and adaptive reservation. A hybrid network performance evaluation method is introduced – combining passive monitoring, active measurements, and probe delay analysis.

Scientific novelty includes: development of a new 5G-based core network architecture for special-purpose networks; formulation of a network planning methodology considering topography and emergency scenarios; creation of a multi-level QoS/SLA framework; modeling the functioning of a governmental network considering authentication, security, service isolation, and reservation. The practical significance of the results is confirmed by their implementation in academic processes, testing on simulation platforms, and adaptability for real-world public safety digitalization projects.

Keywords: special-purpose mobile communication networks, critical infrastructure, critical information infrastructure, cybersecurity, cyber threats, information and telecommunication system, 5G-based critical infrastructure, security assessment criteria, functional security profile, threat evaluation, cloud architecture, 5G technology, 5G mobile communications, network architecture, mobile communication confidentiality, communication channel, unmanned aerial vehicles, mobile network efficiency analysis, service availability, mathematical modeling of network processes, telecommunications processes, wireless communication systems, terahertz communication, analytical review of telecommunication technologies, application of special-purpose networks, governmental radio communication, satellite segment of mobile network, antenna systems, wireless data transmission system, cryptographic

protection, mobile ultra-wideband communication, modulation methods in mobile communication, signal coding methods, socio-cyber-physical communication systems, machine learning in telecommunications, neural networks for digital modulation, adaptive routing in critical networks, authentication in 5G, KPI/KQI, SDN, NFV, QoS/SLA, Network Slicing, mission-critical communication services, RIS, critical communications, microservice architecture in 5G.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Одарченко Р.С., Григоренко Д.К., Дрофа Т.С., Фесенко В.О. Удосконалення ядра мережі 5G з метою підвищення рівня захищеності зв'язку // Наукоємні технології. – 2023. – №1(57). – С. 47–57. DOI: 10.18372/2310-5461.57.17444;

2. Chumachenko S.S., Chumachenko B.S., Maloyed M.M., Odarchenko R.S., Fesenko V.O. Метод маршрутизації в бездротових мережах IoT із високою щільністю пристроїв // Проблеми інформатизації та управління. – 2024. – Т. 4 № 80. – С. 99–112. DOI:10.18372/2073-4751.80.19778;

3. Dudnik A.S., Fesenko V.O Mathematical models and localization algorithms wireless networks // Electronics and Control Systems. – 2025. – №1(83). – С. 50–58. DOI:10.18372/1990-5548.83.19874;

4. Фесенко В. О., Козловська Д. В., Вишневська Н. С. Метод визначення матриці опорів лінії зі змінним по довжині хвильовим опором // Наукоємні технології. – 2025. – №1(65). – С. 93–98. DOI: 10.18372/2310-5461.65.19930

Статті в іноземних виданнях:

1. Odarchenko R., Sunduchkov K., Fesenko V., Didenko A., Verkhovets O., Fesenko A. The concept of a channeling system for satellite mobile communication for media delivery with increased efficiency // Proceedings of the 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 22–26 February 2022, Lviv–Slavske, Ukraine. – P. 775–779. DOI: 10.1109/TCSET55632.2022.9767051, ISBN:978-1-6654-6861-9

2. Saiko V., Odarchenko R., Zhurakovskyi B., Yevdokymenko M., Fesenko V., Tkachova O. A model for building a wireless terahertz network for 5G NR // 12th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems, 7–9 September 2023, Dortmund, Germany. – P. 1071–1076. DOI:10.1109/IDAACS58523.2023.10348670, ISSN:27704262

3. Kotyk B., Bakhtiiarov D., Lavrynenko O., Chumachenko B., Antonov B., Fesenko V., Chupryn V. Neural network approach to 5G digital modulation recognition // Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024), 24–27 January 2024, Kyiv, Ukraine. – P. 82–92. ISSN:16130073

Наукові праці, які додатково відображають наукові результати дисертації)

1. Dudnik A.S., Fesenko A.O., Fesenko V.O., Grinenko O.O., Grinenko S.A., Kvashuk D.M. Models and methods of determining penetration by means of wireless sensor networks // Monographic series “European Science”. Book 21. Part 1. Karlsruhe, Germany, 2023. – P. 161–171.

2. Юдін. О.Ю., Фесенко В.О. Аналіз можливості одночасного впровадження в державній установі міжнародних стандартів ISO 31000 та ISO27005 // VII міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту інформації», 24-27 лютого 2021р.:тези доп. – с. Верхнє Студене., *2021*, С. 94-96.

3. Фесенко А., Хоменко О., Фесенко В. Дослідження критеріїв безпеки у сучасних системах обміну миттєвими повідомленнями // V Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS), 27–28 жовтня 2022 р., Київ, Україна. – С. 139–140.

4. Фесенко В.О. Підвищення характеристик стільникових мереж зв'язку // XXIII Міжнародна науково-практична конференція здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки», 4–7 квітня 2023 р., Київ, Україна. – С. 59.

5. Фесенко А., Хоменко О., Фесенко В. Вплив мережевої архітектури додатків для обміну миттєвими повідомленнями на їх безпеку // VI Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS), 27 квітня 2023 р., Київ, Україна. – С. 51–53.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

5G –	п’яте покоління мобільного зв’язку / fifth generation of mobile communication
QoS –	якість обслуговування / Quality of Service
KPI –	ключові показники ефективності / Key Performance Indicators
KQI –	ключові показники якості / Key Quality Indicators
SDN –	програмно-конфігуровані мережі / Software-Defined Networking
NFV –	віртуалізація мережевих функцій / Network Functions Virtualization
PCF –	функція управління політиками / Policy Control Function
AMF –	функція управління доступом і мобільністю / Access and Mobility Management Function
SMF –	функція управління сесіями / Session Management Function
UPF –	функція користувацької площини / User Plane Function
AUSF –	функція аутентифікації / Authentication Server Function
UDM –	модуль керування даними користувачів / Unified Data Management
RIS –	реконфігуровані інтелектуальні поверхні / Reconfigurable Intelligent Surfaces
PKI –	інфраструктура відкритих ключів / Public Key Infrastructure
SLA –	рівень угоди про якість обслуговування / Service Level Agreement
URLLC –	ультранадійний зв’язок із низькою затримкою / Ultra-Reliable Low-Latency Communication

NAS – сигнальна підсистема, що не належить до доступу / Non-Access Stratum

MCX – сервіси місієкритичного зв’язку / Mission Critical Services

MCPTT – місієкритичний передача голосу / Mission Critical Push-To-Talk

MCData – місієкритична передача даних / Mission Critical Data

MCVideo – місієкритична передача відео / Mission Critical Video

ВСТУП

Актуальність теми дослідження. У сучасному світі мобільні мережі зв’язку стали невід’ємною складовою інфраструктури інформаційного суспільства. Стрімке зростання обсягів переданої інформації, кількості користувачів та різноманіття застосованих пристроїв вимагає постійного вдосконалення існуючих технологій зв’язку. Особливої актуальності це питання набуває у контексті створення та функціонування мобільних мереж спеціального призначення, які повинні забезпечувати гарантований рівень захищеності, надійності, автономності та мобільності, а також інтеграцію з урядовими, військовими та аварійно-рятувальними комунікаційними системами.

Розгортання технологій п’ятого покоління (5G) відкриває нові перспективи для удосконалення мобільних мереж спеціального призначення. Стандарти 5G передбачають високошвидкісну передачу даних, наднизьку затримку, підтримку масового підключення пристроїв (mMTC), наднадійного обміну (URLLC), а також використання хмарних обчислень, віртуалізації мережевих функцій (NFV), програмно-орієнтованих мереж (SDN), технологій Massive MIMO, beamforming, MEC та інших інновацій.

Зростаючі загрози кібербезпеці та висока вразливість до інформаційних атак зумовлюють потребу в багаторівневому криптографічному захисті, системах виявлення аномалій трафіку, механізмах автоматичного відновлення критичних сервісів та побудові ізольованих сегментів з незалежною маршрутизацією.

У світлі цих викликів, важливим завданням є розробка інтелектуальних методів оптимізації архітектури мереж, включаючи динамічне управління топологією, гнучке балансування навантаження, автоматизоване управління мобільністю вузлів, а також планування мережевих ресурсів на основі пріоритетів трафіку та критичності послуг. Особливу роль відіграє впровадження розподілених систем управління, що поєднують машинне навчання для адаптації до змін

середовища з технологіями SDN/NFV для динамічного переналаштування мережевих функцій.

Крім того, розробка технічних та організаційно-функціональних рішень, які забезпечують високу якість обслуговування (QoS) і рівень обслуговування (SLA) відповідно до нормативів урядового радіозв'язку, є пріоритетною. Це передбачає інтеграцію механізмів SLA-моніторингу, відмовостійких маршрутів, багатоканального резервування та адаптивного управління мережею в режимі реального часу.

Серед вчених, які зробили вагомий внесок у розвиток присвячених дослідженню мобільних мереж зв'язку спеціального призначення, сучасних телекомунікаційних систем, технологій мобільного зв'язку п'ятого покоління , варто відмітити таких вітчизняних і закордонних фахівців, як Калашніков В.В., Гречко Ю.М., Сидоренко О.В., Теодор С. Раппапорт, Ґергард Феттвайс, Міша Долер, Петар Поповскі,Антоніо Де Доменіко.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота відповідає Пріоритетним напрямам розвитку науки і техніки в Україні, зокрема у сферах інформаційних та телекомунікаційних технологій, безпеки та оборони. Робота узгоджується із Стратегією національної безпеки України (2020), Стратегією розвитку ОПК до 2030 року, а також з ініціативами з цифрової трансформації сектору безпеки. Запропоновані підходи узгоджуються з науковими пріоритетами Horizon Europe (кластер 3) та технологічними трендами НАТО у сфері стійкого та захищеного зв'язку. Також дослідження проводилось у межах науково-дослідних робіт, що виконувались в Державному університеті "Київський авіаційний інститут": "Методи побудови захищених мереж мобільного урядового радіозв'язку на базі мереж 5G в Україні" (номер держреєстрації 0120U101401, 2020-2021 рр.) та "Методи побудови захищених багатошарових стільникових мереж 5G/6G на основі використання алгоритмів штучного інтелекту для моніторингу об'єктів критичної інфраструктури держави" (номер держреєстрації 0124U000197, 2024-2025 рр.), ДКР ДержНДІ технологій кібербезпеки та захисту інформації «Сакура».

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення ефективності функціонування мобільних мереж зв’язку спеціального призначення.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Сформувати архітектурну модель ядра мережі 5G, адаптовану до вимог урядового радіозв’язку, яка б забезпечувала можливість масштабування, ізоляції функціональних сегментів та стійкості до сучасних кіберзагроз.

2. Розробити удосконалений метод планування мереж урядового зв’язку, що враховує просторово-частотні обмеження, критичність обслуговування, умови топографії, загрози інформаційній безпеці, а також сценарії функціонування в умовах надзвичайних ситуацій.

3. Розробити метод оцінювання ефективності функціонування спеціалізованих мобільних мереж, який включає комплекс технічних (QoS) і стратегічних показників — рівень захищеності інформації, оперативність реагування, стійкість до ризиків — з метою обґрунтування архітектурних та організаційно-функціональних рішень.

4. Удосконалити метод підвищення надійності стільникових мереж за рахунок інтеграції супутникового сегменту з механізмами адаптивної маршрутизації, резервування критичних каналів та динамічного перемикання, для забезпечення зв’язку в умовах руйнування або втрати наземної інфраструктури.

Об’єктом дослідження є процеси функціонування мобільних мереж зв’язку спеціального призначення та підвищених вимог до захищеності, надійності та адаптивності систем комунікації.

Предметом дослідження є методи, моделі, що забезпечують підвищення ефективності, надійності та функціональної гнучкості мобільних мереж зв’язку спеціального призначення на базі інфраструктури п’ятого покоління (5G).

Методи досліджень. Для досягнення поставлених цілей в дисертаційній роботі використано: *методи системного аналізу* (формалізація предметної області, структурування складових мобільної мережі спецпризначення, визначення взаємозв’язків між функціональними модулями), *математичного та імітаційного моделювання* (опис процесів функціонування мережі: моделювання трафіку,

розрахунку затримок, пропускної здатності, навантаження на мережеві вузли), теорії графів (реалізація задач маршрутизації, пошуку мінімальних покриттів, розрахунку критичних шляхів і виявлення вразливих елементів структури), *теорії ймовірностей* (моделювання випадкових процесів у мережі, таких як надходження трафіку, відмова елементів мережі, зміна завантаження ресурсів), *оптимізації* (ресурсне планування, балансування навантаження, розміщення інфраструктури та оптимізації структури ядра 5G), *методи оцінювання QoS* (аналіз рівня обслуговування користувачів і служб) та захищеності (моделювання загроз, оцінювання рівнів стійкості до атак), а також сучасні інструменти для моделювання архітектур мобільних мереж.

Практичне значення отриманих результатів. Результати дослідження можуть бути використані в проектуванні та модернізації мобільних мереж спецпризначення, які функціонують у сфері безпеки, оборони, цивільного захисту та урядових комунікацій. Запропоновані рішення можуть бути адаптовані для побудови систем екстреного зв’язку та мобільної інфраструктури в умовах надзвичайних ситуацій.

Наукова новизна отриманих результатів. У роботі отримані наступні наукові результати.

1. Вперше сформовано нову архітектурну модель ядра мережі 5G, адаптовану для використання в системах урядового радіозв’язку, яка, на відміну від існуючих, дозволяє гнучко масштабувати мережу, забезпечувати ізоляцію функціональних зон та підвищену стійкість до кіберзагроз.

2. Удосконалено метод планування мережі урядового радіозв'язку на базі технологій стільникових мереж**,** який враховує просторово-частотні обмеження, рівень критичності обслуговування, вимоги до інформаційної безпеки, а також сценарії надзвичайних ситуацій**,** що дало можливість забезпечити гарантований рівень якості зв’язку (QoS), оптимальне покриття територій з урахуванням топографії та оперативне реагування мережі на зміну навантаження і загрозових умов**.**

3. Вперше розроблено метод оцінки ефективності функціонування спеціалізованих мобільних мереж, який, на відміну від існуючих, враховує не лише традиційні технічні показники (пропускна здатність, затримка, надійність), а й інтегральні індикатори рівня захищеності інформації та оперативності реагування в надзвичайних ситуаціях, що дало можливість забезпечити оцінку функціональної готовності мережі до роботи в умовах підвищених ризиків.

4. Удосконалено метод підвищення надійності зв'язку стільникових мереж за рахунок використання супутникового сегменту з адаптивною маршрутизацією, резервуванням критичних каналів передачі та динамічним перемиканням між наземною та космічною інфраструктурою, що дозволило забезпечити безперервність зв'язку в умовах руйнування або перевантаження наземної мережі, підвищити стійкість до зовнішніх впливів і реалізувати автономне функціонування в регіонах з обмеженим покриттям або в надзвичайних ситуаціях.

Практична цінність та практичні результати

Практична цінність дисертаційної роботи полягає у створенні моделей та проведенні експериментального аналізу ефективності запропонованих технічних рішень, що дозволило обґрунтувати вибір архітектури та ключових параметрів перспективної мережі зв'язку спеціального призначення на базі 5G Результати дослідження орієнтовані на впровадження в системах критичної інфраструктури, оборони, цивільного захисту, а також в урядовому, рятувальному та оперативному зв'язку.

Практичні результати:

1. **Розроблено узагальнену архітектуру мобільної мережі зв'язку спеціального призначення на базі 5G**, яка враховує потреби урядового зв'язку, інтеграцію з державними комунікаційними платформами, підтримку автономних зон зв'язку та підвищену стійкість до порушення інфраструктури.

2. **Розроблено концепцію побудови захищеного ядра мережі 5G**, адаптованого для урядового зв'язку, з урахуванням політик безпеки, систем шифрування та сегментування архітектури ядра.

3. **Сформовано модель багаторівневої QoS/SLA-інфраструктури**, що дозволяє контролювати та підтримувати задані рівні обслуговування для різних типів користувачів і сервісів, зокрема в екстрених режимах.

4. **Реалізовано імітаційне моделювання ключових сценаріїв роботи мережі**, що підтвердило ефективність запропонованих технічних рішень у порівнянні з **традиційними** підходами.

Особистий внесок здобувача. Дисертаційне дослідження є самостійно виконаною науковою працею, в якій відображено авторський підхід до вирішення актуальних проблем підвищення ефективності функціонування мобільних мереж зв'язку спеціального призначення. Особистий внесок здобувача у працях, що опубліковано у співавторстві, конкретизовано у списку публікацій.

Публікації. За матеріалами дисертаційної роботи опубліковано 12 наукових праць, в тому числі: 4 статей у фахових виданнях, які включені до переліку МОН, 3 праці, які індексуються в науково-метричній базі Scopus, 5 матеріалів доповідей на міжнародних науково-технічних конференціях.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи складає 179 сторінок друкованого тексту, у тому числі містить 42 рисунки та 16 таблиць. Список використаних джерел на 12 сторінках містить 98 найменувань.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СУЧАСНИХ СТІЛЬНИКОВИХ МЕРЕЖ

1.1. Аналіз функціонування мобільних мереж спеціального призначення

Ефективність сучасних мереж урядового радіозв'язку. TETRA (Terrestrial Trunked Radio) – це цифровий стандарт транкінгового радіозв'язку, розроблений ETSI (Європейським інститутом телекомунікаційних стандартів) спеціально для потреб урядових організацій та служб екстреної допомоги. Перша версія стандарту з'явилась у 1995 році, і з того часу TETRA став основою професійного мобільного радіозв'язку в багатьох країнах світу. Мережі TETRA забезпечують групові голосові виклики в режимі реального часу, підтримують передачу коротких повідомлень і низькошвидкісних даних. Хоча пропускна здатність для даних обмежена (стандартні мережі TETRA мають канал 25 кГц з 4 тайм-слотами TDMA), пізніші розширення на кшталт TETRA EDS (TEDS) дозволяють передавати дані на вищих швидкостях. Важливою особливістю є режими прямого зв'язку (DMO), що дають можливість терміналам спілкуватися безпосередньо один з одним без інфраструктури, а також ретрансляцію через спеціальні портативні ретранслятори у разі відсутності базової станції. Мережі TETRA широко впроваджені в Європі (наприклад, Airwave у Британії, ASTRID у Бельгії, VIRVE у Фінляндії тощо) та в багатьох країнах Азії, Африки й Америки – за даними, на кінець 2009 року системи TETRA були розгорнуті у 114 країнах.

Недоліки:

Обмежена передача даних: дуже низька швидкість (до ~28 кбіт/с без TEDS), непридатна для відео, карт тощо.

Застаріле шифрування: TEA1 виявлено вразливим до злому (наявний бекдор).

Потреба в інфраструктурі: складно масштабувати і дорого розгортати нові сайти.

Мала зона дії в місті: порівняно слабкий сигнал у будівлях без ретрансляторів.

Відсутність повноцінного мобільного інтернету: несумісна з вимогами до сучасної інформаційної взаємодії.

APCO Project 25 – це стандарт цифрового вузькосмугового радіозв'язку, розроблений у США для забезпечення взаємодії між різними відомствами. P25 широко використовується публічними службами Північної Америки та деяких інших регіонів (загалом у понад 50 країнах світу). Технологія P25, особливо Phase 1, зазвичай працює в діапазонах VHF/UHF з каналами шириною 12,5 кГц (у аналоговому або цифровому режимі), а Phase 2 впроваджує двослотний TDMA для підвищення ємності в тій самій смузі. P25-системи оптимізовані для покриття великої території з невисокою щільністю абонентів і підтримують режим одночастотного симуласту (одночасне мовлення на кількох передавачах) для розширення зони покриття. Як і TETRA, P25 підтримує групові виклики та може забезпечувати шифрування голосового трафіку. В США багато правоохоронних органів досі покладаються на P25-мережі для критичного голосового зв'язку, водночас впроваджуючи паралельно широкосмугові рішення (напр. FirstNet) для передачі даних і відео. Для прикладу, більшість федеральних агентств та значна частина місцевих служб мають P25-радіомережі для диспетчерського зв'язку, з можливістю шифрування AES для захисту переговорів.

Недоліки:

Обмежений спектр даних: хоча фаза 2 покращена, все одно мало придатна для великих обсягів даних.

Висока вартість обладнання: термінали і інфраструктура – дорогі, особливо Phase 2.

Сумісність обмежена: між різними вендорами трапляються проблеми інтероперабельності.

Уразливість до глушіння: навіть дешеві пристрої можуть створити радіоперешкоди.

Помилки користувачів: часто не використовується шифрування або погано налаштоване (людський фактор).

LTE для потреб урядового зв'язку

Зростаючі вимоги до передачі даних (відео з місця подій, мультимедійні повідомлення, GPS-координація тощо) привели до впровадження широкосмугових мереж на основі стандарту LTE (4G) для урядового та аварійно-рятувального зв'язку. На відміну від TETRA/P25, які орієнтовані переважно на голос, LTE забезпечує високошвидкісну передачу даних і здатен підтримувати відеоконференції, потокове відео з камер, великі файли тощо. Урядові LTE-мережі можуть бути побудовані як **приватні мережі** (спеціально виділені для державних потреб) або як **гібридні** рішення на базі комерційних операторів із виділенням ресурсів під критичний трафік. Наприклад, у США національна мережа FirstNet побудована у співпраці з оператором AT&T: вона має окреме ядро мережі для служб безпеки та використовує радіодоступ оператора із пріоритетом і преемпцією для екстрених служб. Завдяки цьому, FirstNet наразі охоплює понад 99% населення США, включаючи сільські території, використовуючи інфраструктуру стільникових веж AT&T. Подібним шляхом ідуть й інші країни: Великобританія розробляє Emergency Services Network (ESN) на основі 4G, Південна Корея побудувала мережу PS-LTE для екстрених служб, ряд країн ЄС (Франція, Фінляндія, Іспанія, Норвегія та інші) теж реалізують національні проекти широкосмугового зв'язку для потреб безпеки. Мережі LTE для урядового зв'язку пропонують більшу пропускну здатність і гнучкість, проте потребують впровадження спеціальних надбудов для забезпечення функцій критичного зв'язку (наприклад, безперервний груповий зв'язок push-to-talk, гарантований пріоритет і т.д.).

Недоліки:

Залежність від комерційної інфраструктури: у надзвичайних ситуаціях зв’язок може бути перевантаженим.

Відсутність прямих каналів без мережі (як у TETRA DMO): залежить від базової станції або транспортної мережі.

Вища складність у захисті: відкриті IP-протоколи потребують складних кіберзасобів захисту.

Необхідність виділеного ядра: щоб забезпечити безпеку й пріоритет, потрібна інфраструктура і контроль з боку держави.

Технологія 5G у державному радіозв'язку

5G – це наступне покоління мобільного зв'язку, що характеризується ще більшою швидкістю передачі даних, меншою затримкою та можливістю гнучкого **мережевого сегментування** (network slicing). Для урядових і місіонно-критичних мереж 5G відкриває нові можливості: виділені *слайси* мережі можуть бути зарезервовані під потреби служб екстреної допомоги, забезпечуючи гарантовану ширину каналу та ізоляцію від загального трафіку. Хоча більшість актуальних впроваджень широкосмугового зв'язку для безпеки все ще базуються на LTE, інтеграція 5G уже розпочалася. Зокрема, FirstNet (США) оголосила план інвестицій у $6,3 млрд для впровадження повноцінних можливостей 5G та розширення місійно-критичних сервісів. Перевагами 5G для урядового зв'язку є підтримка *ультранизьких затримок* (що важливо для застосувань типу доповненої реальності чи дистанційного керування робототехнікою у кризових ситуаціях) та *масштабованість* під великий обсяг пристроїв (наприклад, IoT-сенсори, дрони). Крім того, стандарт 5G розвиває технології прямого зв'язку між пристроями (sidelink), що потенційно покращить роботу в режимі відсутності мережі. Варто зазначити, що багато країн планують з 2025 року вводити в експлуатацію саме **5G-готові** мережі для критичного зв'язку. Наприклад, у Європі діапазон 68 (700 МГц) спеціально виділяється під потреби публічної безпеки, і вже з’являються базові станції та термінали з підтримкою цього діапазону для 4G/5G систем екстрених служб.

Недоліки:

Недостатня зрілість: багато функцій ще в стадії тестування або стандартизації (наприклад, sidelink).

Велика вартість впровадження: потребує повністю нової інфраструктури (особливо mmWave або standalone).

Складність у конфігурації: slicing, MEC, QoS-профілі вимагають високої кваліфікації персоналу.

Підвищена вразливість до кіберзагроз: більша кількість точок входу та програмної логіки.

Обмежене покриття на старті: щільне розміщення базових станцій потрібно для стабільної роботи.

MCX – сервіси критичного зв'язку (Mission Critical Services)

MCX (Mission Critical Services) – це узагальнена назва набору сервісів критично важливого зв'язку, стандартизованих 3GPP для роботи в LTE/5G мережах. До них відносяться: **MCPTT (Mission Critical Push-To-Talk)** – критично важлива передача голосу (аналог диспетчерського групового виклику), **MCVideo** – передача відео в реальному часі, **MCData** – передача даних (текст, файли) для екстрених служб. По суті, MCX – це програмно-апаратний рівень, що забезпечує в широкосмуговій мережі ті функції, які раніше надавали вузькосмугові LMR-системи. Наприклад, MCPTT дозволяє здійснювати групові виклики з натисканням кнопки, з мінімальною затримкою, високою надійністю та можливістю пріоритету – подібно до рацій TETRA чи P25. Реалізація MCX вимагає спеціального серверного обладнання і клієнтських додатків; багато постачальників (Motorola, Ericsson, Nokia, Airbus та ін.) розробляють рішення MCX, які можуть бути інтегровані в існуючі LTE/5G мережі. У Великій Британії, наприклад, ключовим елементом ESN має стати сервіс MCPTT, що забезпечить груповий голосовий зв'язок для поліції та рятувальників по 4G-мережі. Після виходу з проєкту компанії Motorola (колишнього постачальника цього сервісу), у 2023 р. оголошено новий тендер на побудову **3GPP-сумісної** MCX-системи (голос, відео, дані) для ESN і інтеграцію її з інфраструктурою 4G/5G. Сервіси MCX активно розвиваються: проводяться інтероперaційні тести між різними вендорами, демонструючи сумісність, наприклад, успішне тестування 5G sidelink для прямого зв'язку між абонентами MCX від Qualcomm, Softil та Alea (Leonardo) в 2023 році

Недоліки:

Затримки у запуску повнофункціональних сервісів: повна сумісність між виробниками ще не досягнута.

Залежність від LTE/5G мережі: без стабільного з'єднання MCX не функціонує.

Потреба у спеціалізованих додатках і терміналах: не кожен пристрій підтримує MCX.

Вищі затримки у порівнянні з TETRA/P25: особливо в початкових реалізаціях.

Необхідність інтеграції з іншими системами (CAD, відеонагляд, GPS): що ускладнює розгортання.

Вартість побудови мережі TETRA/P25 з «нуля»

Побудова національної мережі урядового зв'язку на базі технологій LMR (Land Mobile Radio), таких як **TETRA** або **P25**, потребує величезних капіталовкладень. Це включає встановлення тисяч базових станцій по всій території, розгортання центральних комутаторів і серверів, резервування каналів зв'язку, а також закупівлю спеціалізованих абонентських терміналів. Наприклад, найбільша у світі мережа TETRA в Німеччині (BOSNet) оцінювалася у **приблизно 4,7 млрд $** на десятирічний проект розбудови та експлуатації. Ця мережа охопила ~97% території та обслуговує близько 500 тисяч користувачів, використовуючи понад 4,500 базових станцій. Для порівняння, національна мережа **Airwave** у Великій Британії (теж на базі TETRA) при запуску мала ~3,400 базових станцій для ~200 тисяч користувачів, а початковий контракт на побудову й обслуговування протягом ~19 років становив **близько 1,9 млрд.$** Окрім початкових інвестицій, значними є і операційні витрати: утримання мережі, оренда інфраструктури та підтримка обладнання. Для прикладу, утримання британської мережі Airwave обходиться бюджету приблизно в **$470–500 млн щороку**, щоб забезпечити її 99,9% доступність для екстрених служб.

Додатково потрібно врахувати вартість **абонентських терміналів** (радіостанцій) для користувачів. Ці пристрої є спеціалізованими, захищеними та

підтримують криптозахист, тому значно дорожчі за масові споживчі гаджети. Типова ціна портативної радіостанції стандарту P25 або TETRA може сягати **кількох тисяч доларів США за одиницю**. За свідченням фахівців у США, вартість одного P25-радіо інколи досягає **$5,000 за штуку**, що створює серйозний фінансовий бар'єр для невеликих служб (наприклад, добровільних пожежних команд). Якщо ж рахувати оснащення десятків тисяч рятувальників і поліцейських такими пристроями, сума вимірюється сотнями мільйонів. Таким чином, **загальна вартість розгортання повноцінної LMR-мережі національного масштабу** (з урахуванням інфраструктури, резервування, терміналів та підтримки) становить **кілька мільярдів валютних одиниць** (доларів або євро) і потребує постійних витрат на обслуговування мережі. Для урядових бюджетів це дуже суттєве навантаження.

Витрати на LTE/5G мережу для урядового зв'язку

Альтернативою побудови окремої LMR-мережі "з нуля" є використання **наявної інфраструктури стільникового зв'язку** стандартів 5G. Ідея полягає в тому, щоб скористатися вже розгорнутою мережею комерційних мобільних операторів (тисячі їхніх веж, антени, магістральні канали), додавши до неї необхідні функції для екстрених служб – такі як пріоритетний доступ, захищений сегмент ядра мережі, спеціальні режими зв'язку «push-to-talk» тощо. **Модель державно-приватного партнерства (PPP)**, як у випадку програм *FirstNet* у США чи *ESN* у Великій Британії, передбачає співпрацю держави з оператором мобільного зв'язку. Держава інвестує певні кошти або надає ресурси (наприклад, радіочастотний спектр), а приватний партнер (оператор) розширює і модернізує свою мережу під вимоги безпеки. Це дозволяє значно скоротити прямі витрати бюджету, адже **більша частина інфраструктури вже існує** і обслуговується оператором для комерційних користувачів. Як зазначає аналітика ринку, використання комерційних мереж може бути **дешевшим**, оскільки вони **залучають наявні ресурси й інфраструктуру, що вже розгорнута**.

Для прикладу, у **Сполучених Штатах** перед початком FirstNet оцінювали, що створення окремої загальнонаціональної мережі зв'язку для перш responder'ів

могло б коштувати від **£8 до £30 млрд** (у перерахунку з доларів). Це колосальна сума, тож було вирішено укласти партнерство з приватним сектором. Контракт на розгортання FirstNet отримала компанія AT&T – уряд надав їй близько **$6,5 млрд фінансування на перші 5 років** і виділив 20 МГц цінного радіочастотного спектру, а натомість AT&T зобов'язалася побудувати та експлуатувати цю мережу протягом 25 років. Загальні витрати на побудову і підтримку мережі оцінюються у **близько $40 млрд**, які AT&T інвестує поступово із розрахунком окупити їх за рахунок комерційного використання надлишкової ємності мережі. Фактично, **FirstNet** функціонує як окрема захищена підмережа всередині широкої інфраструктури AT&T: перші респондери отримують пріоритетний доступ і спеціальні сервіси, тоді як невикористана пропускна спроможність може обслуговувати звичайних абонентів. Такий підхід істотно **зменшив прямі витрати держави** – замість будувати все власним коштом (десятки млрд), уряд витратив лише кілька млрд, а решту інвестицій та витрат на себе взяв приватний партнер. Більш того, у перспективі уряд США очікує, що FirstNet стане **самоокупним або навіть прибутковим проектом**, оскільки надана публічна мережа буде також використовуватися й для звичайних громадян за плату (оператор монетизує виділену ємність).

Розвиток стільникових мереж зв'язку. Мобільний (стільниковий) зв'язок — це форма радіозв'язку, що функціонує на основі стільникової інфраструктури. Такі мережі можуть включати базові станції, які працюють за різними стандартами, що дозволяє підвищити ефективність роботи мережі та забезпечити краще покриття. Завдяки технологіям бездротового зв'язку користувачі сучасних мобільних і цифрових пристроїв можуть вільно переміщатися без необхідності у дротових з'єднаннях [1].

Історія становлення мобільного зв'язку демонструє поступовий перехід від систем першого покоління до сучасних технологій, таких як LTE-Advanced, що стало відповіддю на постійно зростаючі потреби користувачів.

Еволюція мобільного зв' язку					
	Технології	Швикість	Функції	Початок розробки	Впровадження
1G - Аналоговий стільниковий зв' язок	NMT, AMPS та інші	до 1,9 Кбіт/с	дзвінки	1970	1984
2G - цифровий стільниковий зв' язок	GSM та інші	до 14,4 Кбіт/с	+ sms	1980	1991
3G - широкосмуговий цифровий стільниковий зв'язок	CDMA2000, UMTS та інші	до 3,6 Мбіт/с	+ доступ до інтернету	1990	2002
4G – швидше	LTE, WiMAX та інші	до 1 Гбіт/с	+ відеострімінг	2000	2010
5G – ще швидше	IMT-2020	до 20 Гбіт/с	+ UltraHD і 3D-відео AI-додатки, інтернет речей	2008	2020
6G	IMT-2030+	100 Гбіт/с до 1 Тбіт/с	+ AI	2023	2026-2030

Рис. 1.1. Історія становлення мобільного зв'язку

Стільникові мережі спочатку створювалися для голосового зв'язку на основі аналогових каналів. Проте з появою цифрових технологій та зростанням потреби у більшій кількості голосових каналів у 1990-х роках було впроваджено цифрові системи другого покоління (2G) (рис. 1.1). Перехід на цифрову передачу відкрив можливості для нових сервісів, зокрема обміну текстовими повідомленнями та доступу до даних із комутацією каналів.

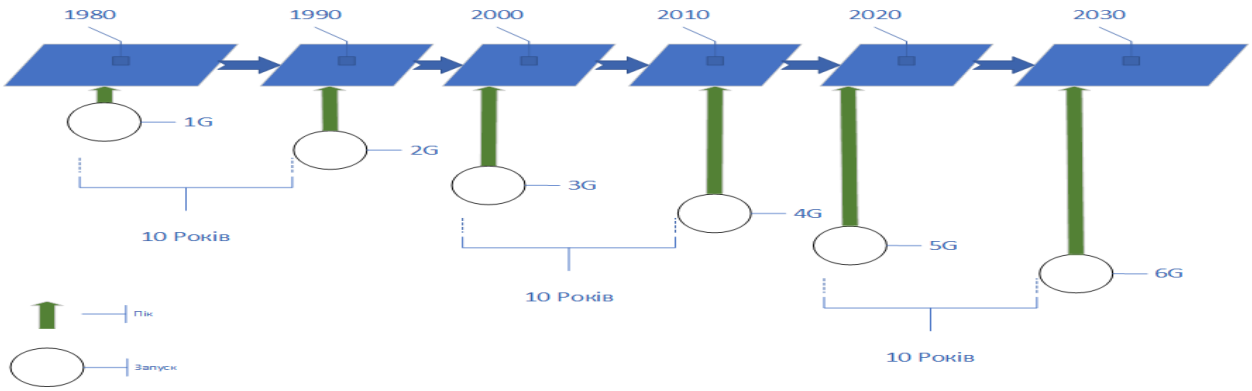

Рис. 1.2. Часове відображення еволюції стільникових технологій

Низькі швидкості передачі даних, що пропонувалися стандартом 2G, були недостатніми для задоволення зростаючого попиту на мобільний доступ до

Інтернету. Це призвело до розробки нових стандартів 3G, які розвинулися, щоб забезпечити швидшу обробку даних та розширені можливості передачі голосу.

За останні роки система стільникового зв'язку LTE значно просунулася, пропонуючи високі швидкості та високошвидкісні послуги передачі даних для мобільного мультимедіа з концепцією підключення «будь-де, будь-коли». Водночас широке впровадження смартфонів та додатків, що працюють на основі даних, спричинило революцію в поведінці та очікуваннях користувачів, що призвело до трансформації всієї телекомунікаційної галузі. [2].

На рис. 1.3 показана еволюції стандартів стільникового зв'язку, на основі комунікаційних потреб людей і об'єктів.

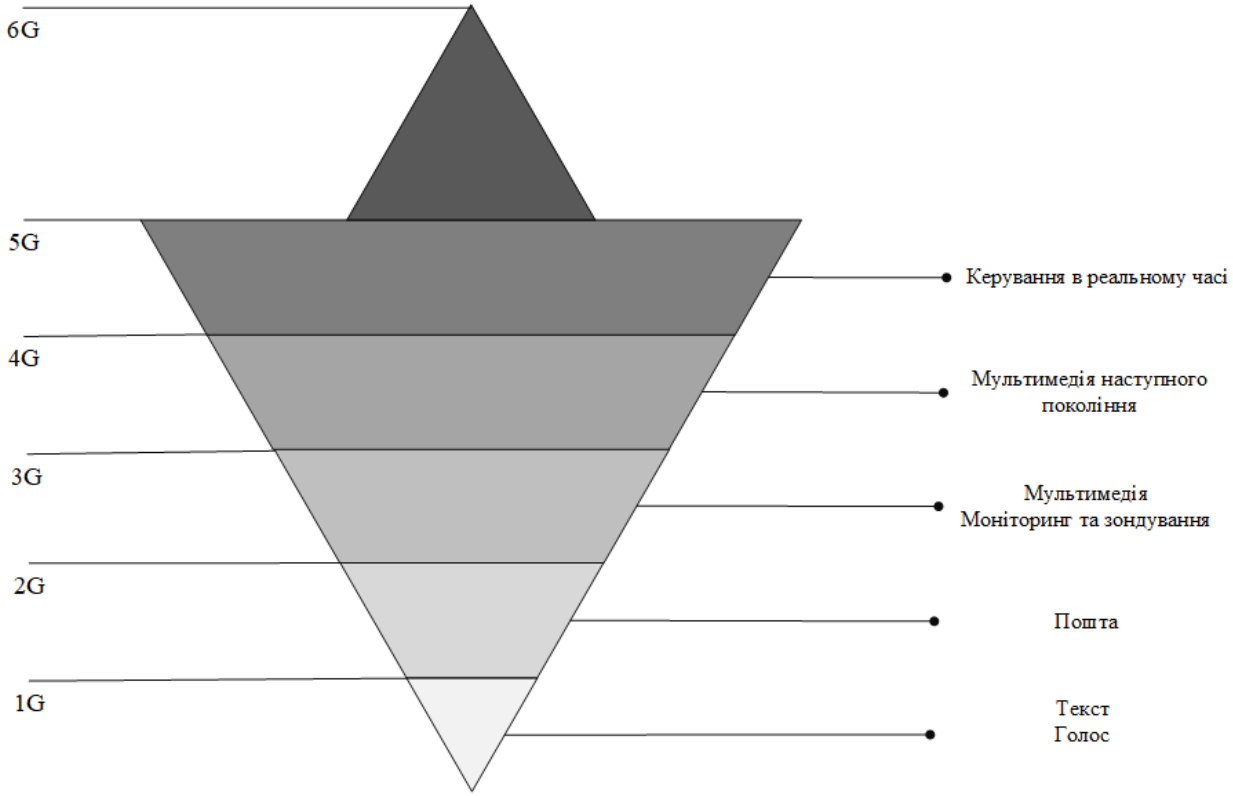

Рис. 1.3. Еволюції стільникових стандартів за потребами споживача

Судячи з діаграми еволюції кожен із стандартів стільникового зв'язку розвивався навколо набору ключових потреб використання:

- 1G – Голосові послуги.
- 2G – Поліпшення голосового зв'язку і обміну текстовими повідомленнями.
- 3G – Вбудований голос і доступний стільниковий Інтернет.

- 4G – Висока пропускна здатність стільникової мультимедіа.
- 5G – Керування в реальному часі.

Розвиток мереж 4G розпочався на початку 2000-х років, а масштабне розгортання почалося приблизно у 2010 році в багатьох країнах (Україна приєдналася у 2018 році). Ця технологія четвертого покоління побудована на IP-протоколі, який з'єднує окремі комп'ютерні мережі з глобальною мережею Інтернет, призначаючи унікальні IP-адреси. Інтернет-протокол (IP) дозволяє інтегрувати сегменти мережі в єдину систему, що дозволяє доставляти пакети даних між будь-якими вузлами в мережі.

Однією з ключових переваг 4G є його значно вища швидкість — до 250–450 разів швидше, ніж у мережах 3G. На відміну від свого попередника, 4G не використовує виділені голосові канали; натомість він повністю покладається на цифрову передачу даних. Як результат, голосовий зв'язок здійснюється через VoIP (Voice over IP), що потенційно сигналізує про занепад традиційних стільникових голосових послуг на користь інтернет-телефонії. VoIP стосується всіх форм передачі голосу через IP-мережі, включаючи ті, що не пов'язані зі звичайними телефонними дзвінками або взаємодією з людьми.

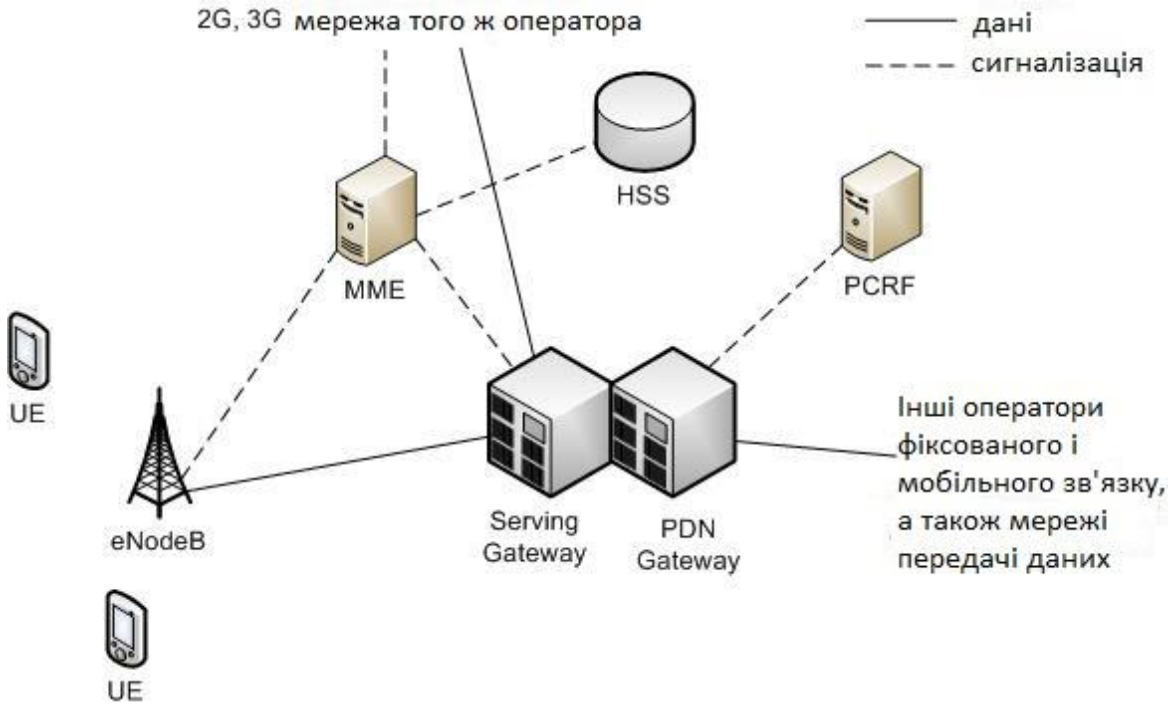

Рис. 1.4. Архітектура мережі LTE

На даний момент сімейство 4G складається з двох стандартів - WiMAX і LTE. Перший є еволюцією WiFi зі збільшеною площею покриття, а другий - черговим еволюційним втіленням GSM.

Очікується, що п'яте покоління мобільних мереж, відоме як 5G, стане справді трансформаційним. Вважається, що такі технології, як автономні транспортні засоби, віртуальна реальність та Інтернет речей, стануть частиною повсякденного життя завдяки 5G. Наразі ця система зв'язку наступного покоління активно тестується по всьому світу.

5G пропонує надзвичайно високу швидкість передачі даних, яка досягає кількох гігабіт за секунду. Він також значно зменшує затримку сигналу до однієї мілісекунди, порівняно з приблизно 10 мілісекундами у 4G та близько 100 мілісекундами в мережах 3G.

Кожне наступне покоління стільникових технологій забезпечує швидшу передачу даних, що дозволяє використовувати нові послуги та формати контенту. Критичним фактором у розгортанні 5G є наявність відповідних частотних діапазонів.

Технічно, пропустити 4G та перейти одразу на 5G практично неможливо. Таким чином, поточні інвестиції в розвиток та модернізацію мережі 4G закладають основу для майбутньої міграції на 5G. На ранніх етапах технології 4G та 5G співіснуватимуть та доповнювати одна одну.

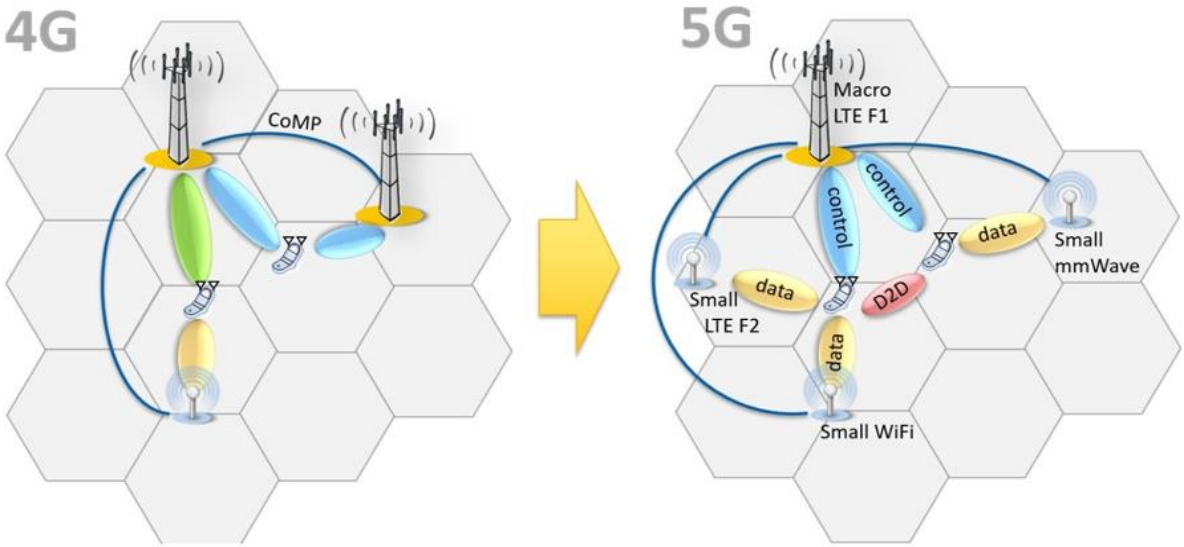

Рис. 1.5. Технологічний перехід від 4G до мобільного зв’язку п’ятого покоління

1.2 Аналіз основних вимог до мереж п’ятого покоління

Розгортання мереж 5G передбачає підтримку наднадійного з'єднання з мінімальною затримкою (URLLC), масової міжмашинної комунікації (mMTC) і мобільного широкосмугового доступу (eMBB), що забезпечує високу якість послуг в умовах надзвичайних ситуацій [4].

Однією з ключових тенденцій на сучасному ринку мобільного зв'язку є розвиток мережевих технологій п'ятого покоління (5G). У рамках еволюції мереж 5G розробляються найсучасніші рішення для широкосмугового бездротового доступу. Згідно з термінологією, що використовується Міжнародним союзом електрозв'язку (ITU), ці мережі називаються IMT-2020[5].

Очікується, що мережі 5G забезпечать підключення десятків тисяч пристроїв в одному стільнику, більш ніж на порядок підвищать швидкість передачі даних і на порядок зменшать мережеві затримки, що дозволить створювати нові телекомунікаційні сервіси для всіх галузей економіки, включаючи транспортну галузь, індустрію розваг, освіту, сільське господарство і багато іншого.

Мережі 5G покращать якість існуючих послуг зв'язку, включаючи голосові та відеодзвінки, онлайн-ігри та перегляд веб-сторінок, особливо у місцях з високою щільністю населення.

Мережі 5G значно розширюють обмежені можливості попередніх поколінь стільникових мереж. [6]. Ключові функціональні характеристики цих мереж включатимуть [5]:

- Покращений широкосмуговий мобільний зв’язок;
- Надійні та швидкодіючі комунікації з низькою затримкою.

Фахівці виділяють три основні тенденції вдосконалення послуг мереж 5G. [7]:

- надзвичайно мобільний широкосмуговий доступ, що пропонує швидкість передачі даних у кілька гігабіт за секунду;
- масивний машинний зв'язок, що забезпечує масштабне підключення для пристроїв Інтернету речей, потенційно охоплюючи десятки тисяч підключень на комірку;

- наднадійний машинний зв'язок, призначений для використання в промисловій автоматизації, транспортних системах, інфраструктурі громадської безпеки.

Рис. 1.6. Функціональні можливості технологій 5G [6]

Умови для розгортання стільникових мереж 5G

Категорія	**Вимоги 5G**
Максимальна швидкість завантаження	До 20 Гбіт/с
Максимальна швидкість вивантаження	До 10 Гбіт/с
Середня користувацька швидкість	Не менше 100 Мбіт/с

Затримка (латентність)	Від 1 мс (для критичних застосувань) до 4 мс (у звичайних умовах)
Щільність підключених пристроїв	До 1 000 000 пристроїв/км²
Надійність зв’язку	99,999% (для критичних додатків)
Підтримка мобільності	До 500 км/год

Рис. 1.8. Вимоги мереж стільникового зв’язку 5G

Майбутні інноваційні мережеві послуги 5G включають такі програми, як доповнена та віртуальна реальність, передача голографічних 3D-зображень, які вимагають високої пропускної здатності та надшвидкої передачі даних, доступної для користувачів або пристроїв, а також тактильний Інтернет та автоматизацію в промисловому та транспортному секторах. Ці послуги вимагають надзвичайно низької затримки та виняткової надійності зв'язку.Надширокосмуговий мобільний зв’язок (ExtremeMobileBroadband, eMBB) - реалізація ультраширокосмугового зв’язку з метою передачі «важкого» контенту;

Масовий машинний зв'язок – розроблений для підтримки Інтернету речей через надвузькосмугове з'єднання, що дозволяє великій кількості пристроїв одночасно взаємодіяти.

Наднадійний зв'язок з низькою затримкою – спрямований на надання спеціалізованих послуг, що вимагають надзвичайно низької затримки та виняткової надійності.

Послуги в мережах 5G можуть бути класифіковані за типом контенту, який надається користувачам:

- Мультимедійні сервіси, що включають 4K- та 8K-відео, тривимірне відео, онлайн-ігри, голографічні технології та мультимедіа з ефектом повної присутності;
- Хмарні сервіси, зокрема зберігання файлів, державні платформи та бізнес-застосунки;

- Сервіси віртуальної реальності, які створюють повністю цифрові середовища для взаємодії користувача;
- Сервіси доповненої реальності, що застосовуються в охороні здоров'я, оборонній промисловості, освітній сфері та індустрії розваг;
- Інтелектуальні сервіси, що базуються на аналізі великих даних — для підвищення ефективності бізнесу і покращення управління мережею;
- IoT-сервіси, засновані на масштабному підключенні пристроїв у таких сферах, як енергетика, транспорт, медицина, торгівля, безпека, промисловість і житлово-комунальне господарство;
- Сервіси з мінімальною затримкою, призначені для управління роботизованими системами, дистанційної медицини, автономного транспорту та інтерактивних 3D-ігор.

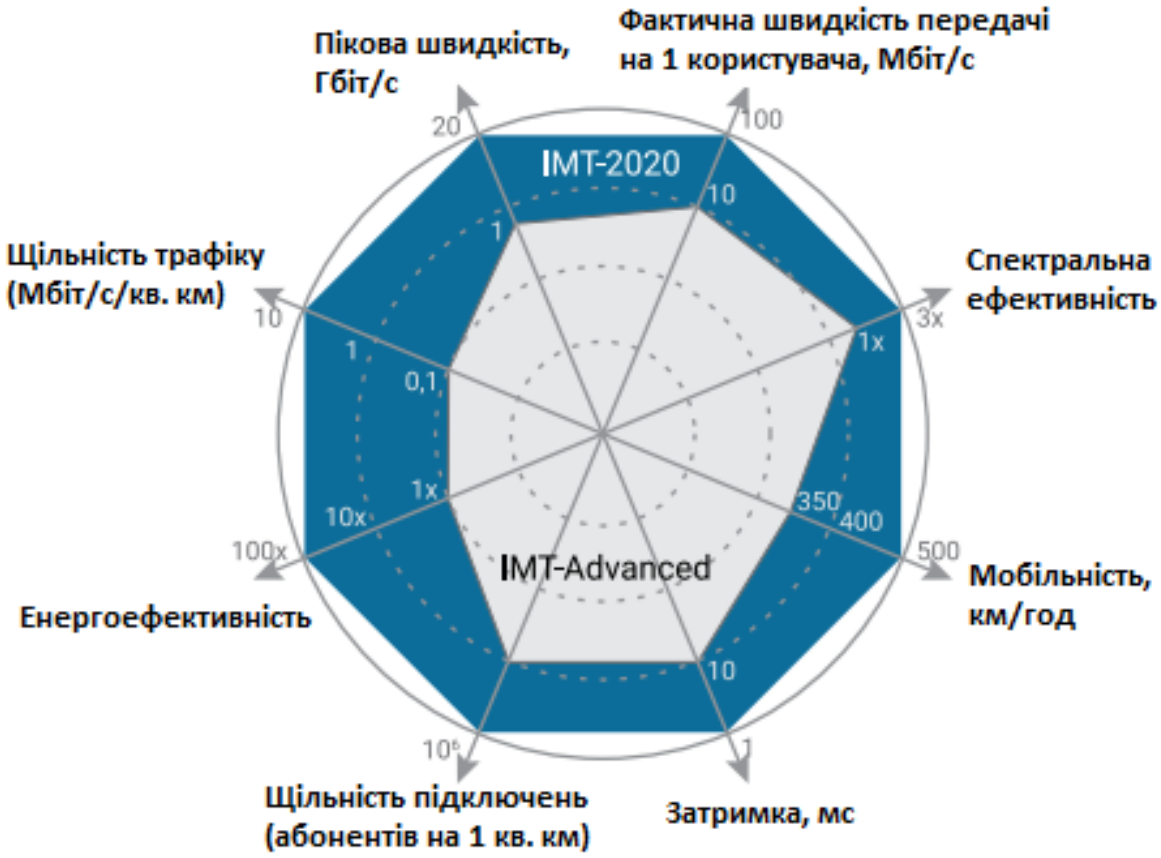

Рис. 1.7. Функціональні характеристики мереж 5G

В майбутньому кількість підключених до мережі пристроїв значно зросте, і більшість із них функціонуватимуть у режимі постійного з’єднання. Водночас одним із ключових технічних показників стане мінімальне енергоспоживання таких пристроїв.Порівняння технічних характеристик мереж 5G із параметрами систем 4G представлені на рис. 1.7.

Ключові технічні орієнтири для мереж п’ятого покоління (5G) включають наступні параметри:

- **Максимальна пропускна здатність** — до 20 Гбіт/с на одного користувача або пристрій, що дозволяє передавати великі обсяги даних за лічені секунди.
- **Стабільна швидкість передачі** в межах зони покриття — не менше 100 Мбіт/с для кожного користувача, незалежно від його місцезнаходження.
- **Оптимізація спектра** — ефективність використання радіочастотного ресурсу зросла утричі в порівнянні з LTE-Advanced, що забезпечує вищу продуктивність на одиницю частоти.
- **Підтримка високої мобільності** — стабільний зв’язок зберігається навіть при швидкості руху до 500 км/год, що важливо для транспортного сектору.
- **Низька затримка** — час реакції мережі скорочено до 1 мілісекунди, що критично для застосунків реального часу, таких як віддалене керування чи телемедицина.
- **Підвищена щільність підключень** — можливість підтримувати до мільйона пристроїв на квадратний кілометр, що відкриває перспективи для масового впровадження IoT.
- **Висока енергоефективність** — 5G передбачає передачу значно більшого обсягу даних при суттєво меншому споживанні енергії як мережею, так і кінцевими пристроями.
- **Трафікова щільність** — 10 Мбіт/с на квадратний метр, що дозволяє обслуговувати значну кількість одночасних з’єднань навіть у перенасичених зонах.

Очікується, що технологія 5G значно перевершить 4G за швидкістю передачі даних, дозволить підключати більшу кількість пристроїв на обмеженій території, а

також забезпечить ефективну взаємодію між пристроями без участі центральної мережі. У таблиці 1.1 наведено зіставлення ключових характеристик мереж четвертого та п’ятого покоління.

Таблиця 1.1

Зіставлення ключових характеристик мереж четвертого та п’ятого покоління

	Пікова пропускна здатність		**Щільність з'єднання прист./км^2**	**Затримка мережі, мс**	**Спектральна ефективність, біт/Гц**	
	Downlink	**Uplink**			**Downlink**	**Uplink**
4G	3	1,5		5	15	6,75
5G	20	10	1 млн	0,5 - 4	30	15

1.3 Аналіз сучасних технічних рішень, які використовуються в мережах 5G

Для реалізації основних вимог мереж п’ятого покоління необхідне впровадження новітніх технологічних рішень на рівні радіодоступу, базової та транспортної інфраструктури, абонентського обладнання, а також розвиток суміжних технологій. Вже зараз багато компаній і наукових центрів активно пропонують відповідні інноваційні підходи.

З метою задоволення зростаючих потреб користувачів у сфері мобільного зв’язку було створено нову технологічну платформу під назвою 5G New Radio (5G NR). У порівнянні з радіоінтерфейсами, що використовуються в мережах четвертого покоління, 5G NR має низку вагомих переваг.

5G NR — це уніфікований глобальний стандарт бездротового зв’язку п’ятого покоління, що пропонує більш гнучкий, високошвидкісний і функціонально насичений мобільний широкосмуговий доступ. Він відкриває можливості для масштабного підключення нових галузей та переосмислення способів взаємодії через мобільні мережі [7].

Створення стандарту 5G New Radio (NR) починалося забсолютно нових принципів, орієнтуючись виключно на вимоги, притаманні мережам п’ятого покоління. Під час розробки були враховані перспективні технології, які очікується використовувати до моменту повного впровадження 5G. У 5G NR інтегровано сучасні методи модуляції, передові форми сигналів та новітні технології радіодоступу. Усе це забезпечує не лише надвисокі швидкості передавання даних, але й покращену енергоефективність, що дозволяє продовжити час автономної роботи пристроїв користувачів у мережах нового покоління.

Рис. 1.8. Актуальність технології 5G NR у сучасних умовах

Технологія 5G NR має відповідати дедалі ширшому спектру вимог до підключення, а також різним сценаріям впровадження. Для досягнення цього вона повинна ефективно використовувати наявний радіочастотний ресурс у різних діапазонах — від низьких частот нижче 1 ГГц до середнього діапазону (1–10 ГГц) і до високочастотного спектра понад 24 ГГц, відомого як міліметрові хвилі (mmWave). У зв’язку з цим, не існує єдиного технічного рішення, яке б повністю визначало стандарт 5G NR — натомість він формується на основі низки інноваційних технологічних розробок. [8].

Залежна версія 5G NR (так звана NSA) є початковим етапом розвитку автономної 5G-мережі і переважно використовується для забезпечення розширеного мобільного широкосмугового доступу. У цьому варіанті використовуються наявна інфраструктура 4G (радіомережа та ядро) у поєднанні з доданими 5G-компонентами. Сьогодні такі рішення проходять активне тестування в багатьох країнах. Основна мета першого етапу впровадження NSA — підвищення швидкості та надійності мобільного Інтернету за допомогою використання міліметрових хвиль. Це дозволить операторам вийти на ринок з новими послугами ще до повного запуску 5G у 2020 році. Однак у високочастотному діапазоні (mmWave) охоплення буде значно меншим, а сигнал — більш чутливим до перешкод, що потребує детального вивчення та вирішення технічних викликів.

Значне зростання швидкості передачі даних у мережах 5G в основному забезпечується завдяки застосуванню технології Massive MIMO — багатоелементних антенних систем із великою кількістю елементів, що працюють у діапазоні частот від 30 до 300 ГГц (mmWave). Разом із цим застосовуються нові алгоритми радіодоступу, які підвищують ефективність використання спектра. Ці зміни охоплюють усі компоненти архітектури 5G — від антен і радіочастотних модулів до обробки сигналів у цифровому ядрі. Через тісну взаємозалежність усіх елементів системи, їх потрібно проектувати й оптимізувати комплексно.

1.3.1. Діапазони частот у мережах 5G

У державах Європейського Союзу активно відбувається розподіл частот для створення урядових сегментів мереж 5G. Зокрема, частотний діапазон 700 МГц (Band 68) зарезервовано для потреб служб громадської безпеки. [9].

Для забезпечення необхідних швидкостей передачі даних, збільшення кількості надісланих мого трафіку і кількості абонентських пристроїв в мережах 5G потрібно використання широких смуг частотних каналів як в лінії вниз, так і в лінії вгору, з безперервним спектром шириною від 500 до 1000 МГц.

Виділення таких смуг для каналів 5G можливо тільки в верхній межі сантиметрового і в міліметровому діапазонах частот. В якості перспективних смуг

частот для мереж 5G розглядаються смуги в діапазоні від 24,25 ГГц до 86 ГГц [8, 10].

Застосування міліметрових частот у мережах 5G суттєво зменшить радіус покриття базових станцій — до 50–100 метрів. Такі станції будуть розміщуватись у зонах з високим попитом на послуги типу xMBB, що дозволить формувати ультрощільні структури радіодоступу. Розгортання таких мереж сприятиме збільшенню пропускної здатності 5G-систем і покращенню їх енергоефективності.

У зв’язку з обмеженим частотним ресурсом для впровадження мереж 5G активно впроваджуються механізми спільного використання як ліцензованого, так і неліцензованого спектра із загальнодоступним доступом. Для реалізації ефективного статичного та динамічного управління спектром у таких умовах необхідне оновлення регуляторних норм як на національному, так і міжнародному рівнях.

Мережі п’ятого покоління мають максимально використовувати переваги високочастотного ліцензованого спектра з метою підвищення пропускної здатності, а також бути здатними ефективно функціонувати в неліцензованому діапазоні за умов перевантаженого трафіку. Оскільки покриття напряму залежить від доступних частотних смуг, технології 5G повинні впроваджувати нові частоти в межах сантиметрового та міліметрового діапазонів для підтримки надщільного розгортання мереж.

Крім того, для забезпечення стабільної якості сервісів у таких мережах необхідно використовувати інтелектуальні алгоритми управління радіоресурсами, які базуються на аналізі трафіку в реальному часі, прогнозуванні навантаження та адаптації параметрів доступу до спектра. Поєднання адаптивних технологій доступу, антенних рішень типу Massive MIMO та гнучкого планування топології дозволить досягти високої ефективності використання спектра та підтримки нових сценаріїв використання, включаючи автономний транспорт, індустрію 4.0 та масові IoT-комунікації.

Таблиця 1.2 демонструє частоти, заплановані для впровадження 5G-технологій у різних регіонах світу [11]:

Таблиця 1.2.

	Sub-1 GHz	Sub-6 GHz		Above 6 GHz			
Australia	n/a	3.40-3.70 GHz		24.25-27.50 GHz		39 GHz	
Canada	600 MHz	3.55-3.70 GHz		27.50-28.35 GHz	37-40 GHz	64-71 GHz	
China	n/a	3.30-3.60 GHz	4.8-5.0 GHz	24.5-27.5 GHz			
Germany	700 MHz	3.40-3.80 GHz		26 GHz			
Great Britain	700 MHz	3.40-3.80 GHz		26 GHz			
France	700 MHz	3.46-3.80 GHz		26 GHz			
Italy	700 MHz	3.60-3.80 GHz		26.5-28.9 GHz			
Japan	n/a	3.60-4.20 GHz	4.4-4.9 GHz	27.0-29.5 GHz			
Russia	n/a	4.80-4.99 GHz		25.25-29.50 GHz			
South Korea	n/a	3.42-3.70 GHz		26.5-28.9 GHz			
USA	600 MHz	3.45-4.20 GHz	5.9-7.1 GHz	24.25-28.35 GHz	37-40 GHz	47.2-48.2 GHz	64-71 GHz

1.3.2. Антенні системи MIMO

Одним із важливих напрямів розвитку технологій для мереж 5G є впровадження масивних антенних систем типу Massive MIMO. Ці системи складаються з великої кількості антенних елементів (десятки або навіть сотні), які працюють узгоджено та динамічно адаптуються до умов середовища.

Технологія MIMO (Multiple Input Multiple Output) передбачає використання кількох антен як на стороні передавача, так і на стороні приймача. Це дозволяє значно підвищити пропускну здатність мережі без потреби у збільшенні ширини частотного спектра або потужності сигналу. Завдяки такому підходу, швидкість передавання даних зростає майже пропорційно кількості антен, а якість зв’язку покращується за рахунок одночасного прийому сигналу декількома антенами [12].

Серед сучасних технологій особливе значення для мобільних мереж має MU-MIMO (Multi-User Multiple Input Multiple Output), яка дозволяє передавати окремі потоки даних кільком користувачам одночасно. MU-MIMO можна уявити як розширення традиційної MIMO-системи, де група користувачів виконує роль спільного антенного масиву. Однак на відміну від одноабонентських систем, тут

існує важливе обмеження: оскільки користувачі не взаємодіють між собою напряму, обробка просторових сигналів розподіляється нерівномірно між базовою станцією та абонентами.

У висхідному напрямку передавання базова станція приймає сигнали від кількох користувачів одночасно та має (в ідеальному випадку) повне уявлення про матрицю каналів. Це дає змогу формувати вузькі промені в бік кожного з користувачів, знижуючи рівень перешкод від інших. У низхідному каналі передавання ситуація аналогічна: базова станція, маючи повну інформацію про канали, формує просторові пучки для кожного користувача так, щоб уникнути взаємних завад. У результаті кожен користувач отримує лише свій сигнал, не маючи доступу до інформації інших активних абонентів.

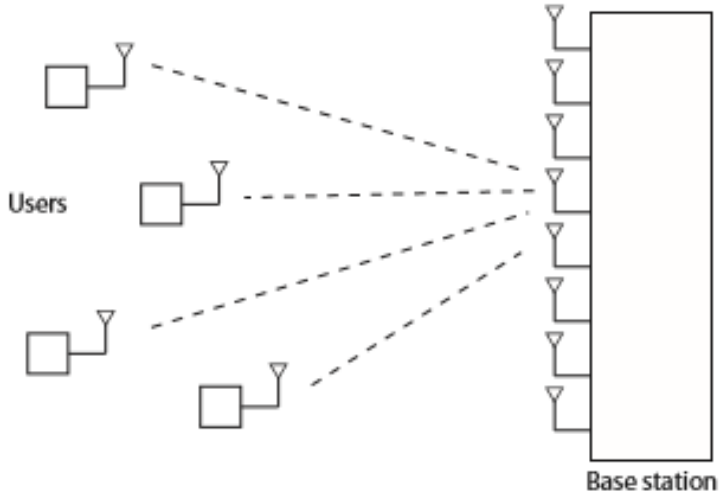

Рис.1.9 Структурна модель системи MU-MIMO

Використання технології масивних антенних решіток MIMO дає змогу динамічно формувати вузькі промені спрямованості сигналу до кожного окремого користувача. Завдяки цьому кілька абонентів, що перебувають у межах однієї зони обслуговування, можуть одночасно отримувати індивідуальні просторово-часові сигнали від базової станції. Такий підхід зменшує рівень внутрішньоканальних завад, збільшує пропускну здатність радіодоступу та ємність стільникової мережі, а також підвищує енергоефективність роботи передавального обладнання.

Окрім цього, адаптивні MIMO-системи дають змогу ефективно пригнічувати сигнали з небажаних напрямків, що суттєво підвищує захищеність мережі 5G від перешкод і покращує якість зв’язку.

Отже, технологію Massive MIMO можна розглядати як ефективну альтернативу збільшенню пропускної здатності мобільної мережі без необхідності надмірного розгортання дрібних стільників [13]. Зокрема, технологія спрямованого формування променів (Beamforming) вважається перспективним методом для оптимізації енергетичного розподілу в межах визначеної зони покриття. Завдяки використанню великої кількості антенних елементів до кількох сотень, базова станція здатна створювати та керувати кількома спрямованими променями одночасно. Це, своєю чергою, дає можливість багаторазового використання одного й того ж частотного ресурсу для різних напрямків, підвищуючи ефективність спектра.

Головною перевагою технології Massive MIMO над традиційними MIMO-системами є значно більша кількість ступенів свободи, доступних базовій станції [14]. Це відкриває можливості для підвищення просторової роздільної здатності антен, що, у свою чергу, сприяє зростанню пропускної здатності мережі завдяки використанню просторового мультиплексування або більш точному спрямуванню сигналу за допомогою формування променів.

У роботі [13] автори показали, що технологія Massive MIMO забезпечує вищу ефективність у середовищах з низькою щільністю користувачів, тоді як у районах з великою кількістю абонентів набагато кращі результати демонструють малі стільники. Це свідчить про те, що через змінну щільність користувачів неможливо визначити єдину конфігурацію мережі, яка б забезпечувала оптимальний баланс між продуктивністю Massive MIMO та ефективністю дрібностільникових рішень.

Таким чином, поєднання технології Massive MIMO з малими стільниками слід розглядати як стратегічно важливий підхід до проєктування мереж 5G, що ілюструється на рис. 1.10.

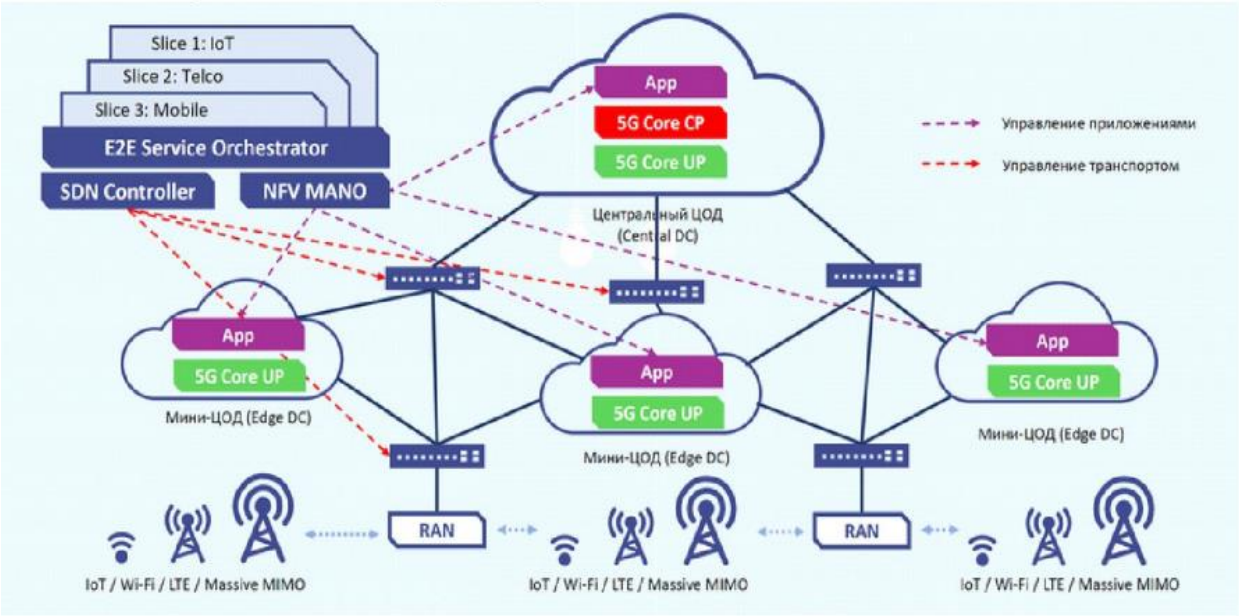

Рис.1.10 Архітектурна модель мережі 5G

Massive MIMO-системи характеризуються наявністю великої кількості антенних елементів як на базовій станції, так і на абонентських пристроях. У таких системах сотні або навіть тисячі антен, інтегрованих на БС, обслуговують відносно меншу кількість терміналів, використовуючи однакові часові та частотні ресурси. Завдяки цим властивостям, технологія Massive MIMO дозволяє суттєво — у 10 і більше разів — збільшити пропускну здатність бездротових мереж, а також забезпечити приблизно стократне підвищення енергоефективності.

Основне завдання технології формування променя полягає у створенні сигналу з заданою формою променя, спрямованого у потрібну зону простору в режимі реального часу, з одночасним пригніченням завад [15, 16]. Для досягнення такої динамічної спрямованості необхідна складна обробка сигналів, що вимагає розширених алгоритмів формування променя [16].

Залежно від принципу реалізації, формування променя поділяється на два основні підходи: комутовані промені та адаптивні масиви. У першому випадку використовується набір заздалегідь визначених напрямків (пелюсток) в діаграмі спрямованості, між якими система перемикається під час роботи. У другому випадку – система адаптивно формує форму та напрямок сигналу до конкретного

користувача (UE), забезпечуючи гнучке керування з більшою кількістю ступенів свободи.

Ще одна класифікація формування променя базується на розташуванні цифро-аналогових перетворювачів (ЦАП). Якщо всі антени підключені до одного ЦАП, маємо справу з аналоговим формуванням променя. Якщо ж кожен антенний елемент має свій ЦАП і сигнали з усіх антен обробляються окремо та синхронно — така система називається цифровою. Обидва підходи мають свої переваги та обмеження в контексті вартості, складності й продуктивності.

Аналогове формування променя характеризується нижчим енергоспоживанням і меншою обчислювальною складністю порівняно з цифровим. Проте через те, що в аналоговій схемі лише один радіочастотний тракт обслуговує всі антенні елементи, така система здатна формувати промінь лише в одному напрямку в конкретний момент часу [14]. У свою чергу, цифрове формування забезпечує значно більшу гнучкість, дозволяючи одночасно створювати декілька спрямованих променів. Однак це вимагає окремого РЧ-тракту для кожного антенного елемента, що збільшує загальне енергоспоживання.

Для досягнення балансу між енергоефективністю та багатонаправленістю було розроблено гібридну технологію формування променя. Вона поєднує переваги аналогової та цифрової схем, і є рекомендованою до використання в мережах 5G.

Ще один аспект класифікації методів формування променів стосується просторового розташування антенних елементів. Вони можуть бути організовані у різних геометричних структурах: лінійній, круговій або площинній [17].

Застосування технології формування променів у масивних MIMO-системах дає низку переваг: підвищену енергоефективність, покращену спектральну продуктивність, посилення захищеності передачі даних, а також ефективну роботу у міліметровому частотному діапазоні.

Подальшим розвитком цієї технології є 3D MIMO (також відома як Full-Dimension MIMO), яка дозволяє адаптивно спрямовувати сигнали не лише в горизонтальній, а й у вертикальній площинах. Це дає змогу розділяти сигнали між

абонентами, що знаходяться під різними кутами не тільки в горизонтальному, але й у вертикальному напрямку щодо базової станції (рис. 1.11).

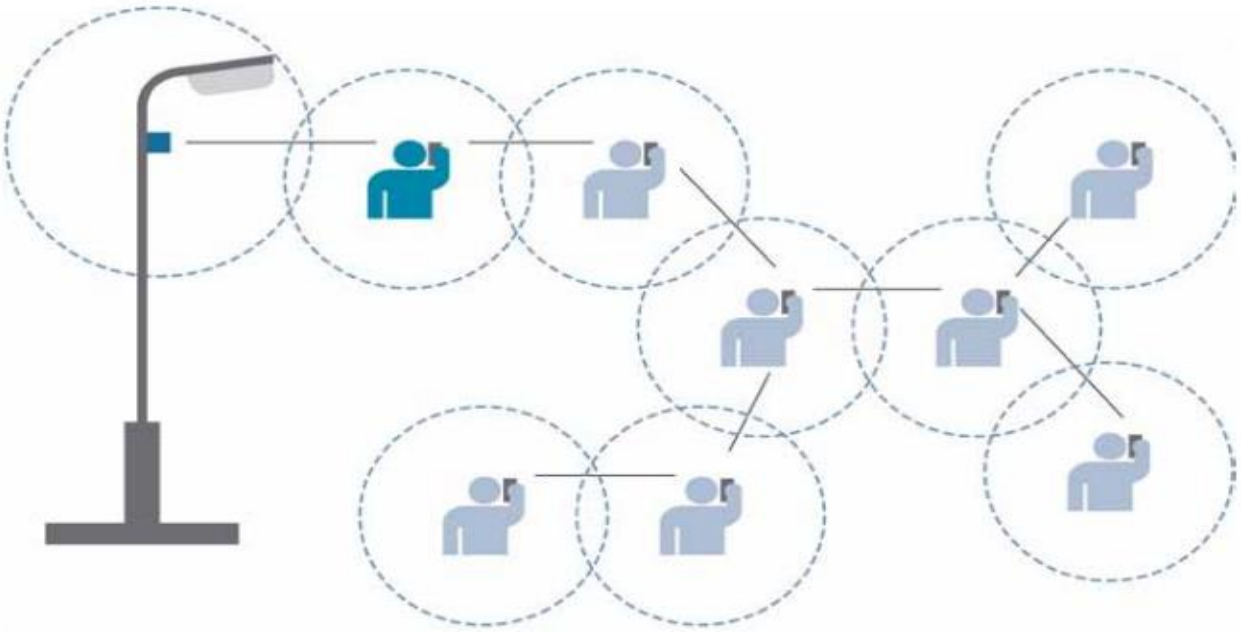

Рис.1.11 Застосування MESH-топології в архітектурі 5G-мереж

1.3.3. Нові технології формування широкосмугового сигналу

Для підвищення спектральної ефективності в мережах п’ятого покоління пропонується впровадження нових методів формування широкосмугових сигналів, таких як Fast OFDM, FTN, FBMC, UFMC, GFDM та BFDM. Частина з цих технологій орієнтована на зменшення міжчастотного інтервалу між піднесущими порівняно з традиційною схемою OFDM, яка використовується в мережах LTE. Інші рішення дозволяють відмовитися від використання циклічного префікса, що підвищує ефективність передачі.

OFDM (Orthogonal Frequency Division Multiplexing) — це цифрова модуляційна технологія, яка передбачає використання великої кількості піднесучих частот, розміщених дуже близько одна до одної, при цьому зберігається їх ортогональність. Кожна з піднесущих модулюється окремо, зазвичай із застосуванням QAM, на невеликій швидкості, що дозволяє зберегти загальну

швидкість передачі на рівні одночастотних модуляцій при більш ефективному використанні спектра.

Fast OFDM (F-OFDM) базується на принципах традиційного OFDM, але застосовує щільніше розміщення піднесучих — з частотним рознесенням, вдвічі меншим за стандартне. Така технологія спирається на властивість, згідно з якою реальна частина коефіцієнта кореляції двох комплексних піднесучих дорівнює нулю за умови, що їх розділення по частоті кратне 1/2T. Незважаючи на ущільнення, сигнали залишаються ортогональними, що зберігає якість передачі.

Ключова перевага технології OFDM порівняно з одночастотною модуляцією полягає в її стійкості до складних умов передачі сигналу. Зокрема, вона ефективно протидіє високочастотним загасанням у довгих мідних лініях, вузькосмуговим завадам, а також частотно-вибірковому затуханню, спричиненому багатопроменевим поширенням сигналу. І все це — без потреби у використанні складних фільтрів чи еквалайзерів.

Еквалізація каналу значно спрощується, оскільки сигнал OFDM можна розглядати не як один широкосмуговий потік із високою швидкістю, а як набір повільно модульованих вузькосмугових піднесущих. Завдяки цьому зменшується символьна швидкість, що дозволяє застосовувати захисний інтервал між символами. Це, у свою чергу, дає змогу компенсувати часові спотворення та зменшити міжсимвольні інтерференції.

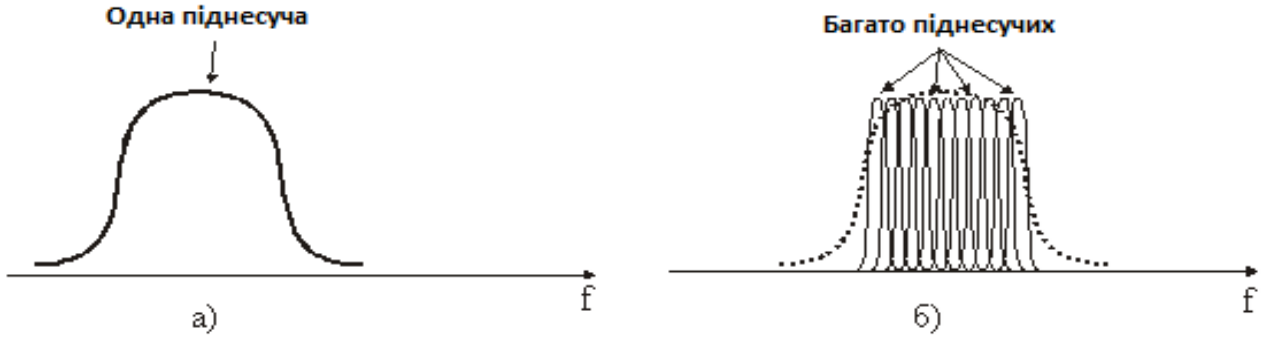

Рис.1.12 Порівняння спектрів радіосигналів: одночастотний (а) та OFDM-сигнал (б)

Однією з ключових переваг технології OFDM є її висока стійкість до багатопроменевого поширення сигналу. Щоб запобігти міжсимвольним інтерференціям, перед кожним OFDM-символом додається захисний інтервал, відомий як циклічний префікс. Цей префікс є копією частини корисного сигналу: початок символу повторює його завершення. Така структура дозволяє зберігати ортогональність піднесучих, за умови, що затримка відбитого сигналу не перевищує тривалості циклічного префікса.

Окрім збереження ортогональності, циклічний префікс надає додаткову гнучкість при обранні часової області для проведення перетворення Фур'є, що ще більше підвищує стійкість до спотворень у каналі.(рис. 1.13).

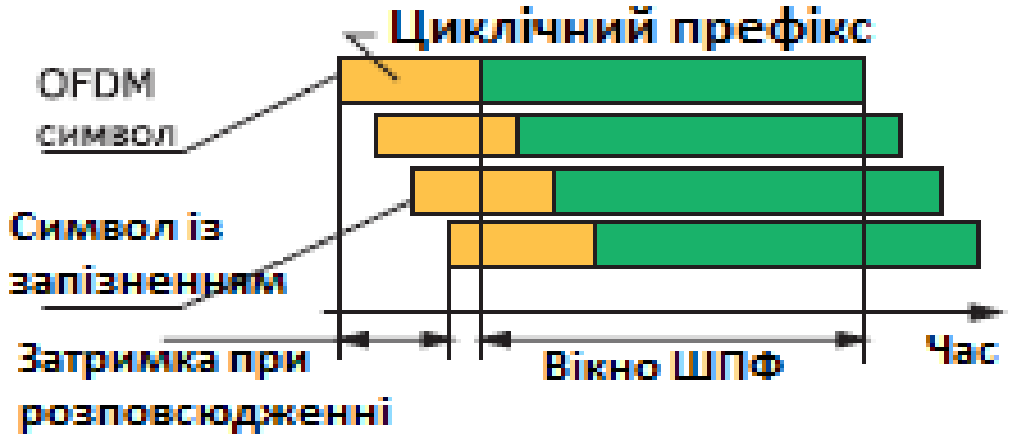

Рис.1.13. Циклічний префікс

Отже, технологія OFDM довела свою ефективність на практиці, що сприяло її широкому впровадженню в системах зв’язку. Водночас залишається актуальним питання визначення оптимальної тривалості циклічного префіксу для OFDM-символів. Від правильного вибору цього параметра залежить ефективність використання доступної пропускної здатності каналу. Відповідно, оптимізація тривалості циклічного префіксу може сприяти збільшенню загальної продуктивності каналу.

1.3.4. Використання нумерології в системах п’ятого покоління

Технологія 5G орієнтована на підтримку широкого спектра інноваційних і вдосконалених сервісів, таких як голографічна передача, автоматизоване

виробництво та автономний транспорт. Одним із ключових елементів архітектури 5G є новий радіоінтерфейс — 5G New Radio (NR). У цьому розділі розглядається OFDM-нумерологія — набір параметрів, що є визначальним для реалізації мультиплексування з ортогональним частотним розділенням каналів, що є основою радіотехнологій 5G. Ця нумерологія має тісний зв'язок із частотними діапазонами, інтервалами між піднесущими, а також із побудовою кадру.

Стандарт 5G NR передбачає можливість розгортання у широкому спектрі частот. За специфікацією 3GPP, визначено два основні робочі діапазони частот для 5G [18]:

- FR1 (Frequency Range 1) охоплює частоти в межах від 450 МГц до 6000 МГц
- FR2 (Frequency Range 2) включає частотний діапазон від 24 250 МГц до 52 600 МГц

Два частотні діапазони 5G — FR1 і FR2 — суттєво відрізняються між собою через значну різницю в частотах, тому технічні вимоги до кожного з них формуються окремо в межах відповідних стандартів. Для порівняння, у системах 4G LTE підтримувалося лише функціонування в межах діапазону FR1 — до 6000 МГц.

У рамках технології 5G NR визначено п'ять варіантів OFDM-нумерології (тобто конфігурацій параметрів модуляції), які використовуються для забезпечення ефективної роботи радіозв'язку як у FR1, так і в FR2.

μ	$\Delta f = 2^{\mu} \cdot 15$ [kHz]	Cyclic prefix
0	15	Normal
1	30	Normal
2	60	Normal, Extended
3	120	Normal
4	240	Normal

Рис. 1.14. Типові OFDM-конфігурацій у стандарті 5G

Більш детально, параметр *Subcarrier Spacing Index* — індекс інтервалу між піднесущими (μ) у мережах 5G може набувати одного з п’яти значень, відповідно до специфікації 3GPP TS 38.211 [19]. Для кожного значення μ використовується формула розрахунку рознесення між піднесущими: 2^μ × 15 кГц. Таким чином, значення μ від 0 до 4 відповідають частотному рознесенню 15, 30, 60, 120 та 240 кГц відповідно. Для порівняння, технологія 4G LTE передбачає лише один варіант — 15 кГц.

У системі 5G NR підтримується стандартний циклічний префікс для всіх вищезазначених варіантів, тоді як розширений циклічний префікс застосовується виключно при μ = 2, тобто для піднесущих із рознесенням 60 кГц. Піднесущі з інтервалами 15–120 кГц використовуються в основному для загальнодоступних каналів, які передають користувацький трафік. Рознесення в 240 кГц призначено для синхронізаційних сигналів. Вибір конкретного інтервалу між піднесущими залежить від частотної смуги — наприклад, у діапазонах 28 ГГц і 39 ГГц (міліметровий спектр) використовуються 60 кГц і 120 кГц.

Технологія OFDM є основною в архітектурі 5G. Проте, з огляду на велику кількість сценаріїв застосування та широкий діапазон частот, одного варіанту нумерології недостатньо для забезпечення всіх вимог до продуктивності. Саме тому виникає потреба у масштабованій багатонумерологічній структурі, яка дозволяє адаптуватися до конкретних умов розгортання та типів послуг. У цьому розділі розглядаються приклади багатонумерологічних алгоритмів, які впроваджуються в мережах п’ятого покоління.

Вибір нумерології для користувацького обладнання не може здійснюватися довільно. Необхідно впроваджувати спеціалізовані механізми для визначення відповідної нумерології, особливо у багатовимірних системах, які обслуговують велику кількість користувачів. Активні смуги ширини пропускання та відповідні їм нумерології можуть призначатися за допомогою різноманітних підходів. При цьому важливо враховувати компроміси між різними показниками ефективності — зокрема, спектральною ефективністю, гнучкістю налаштувань та складністю реалізації. Це дозволяє обирати оптимальні параметри, відповідно нумерології.

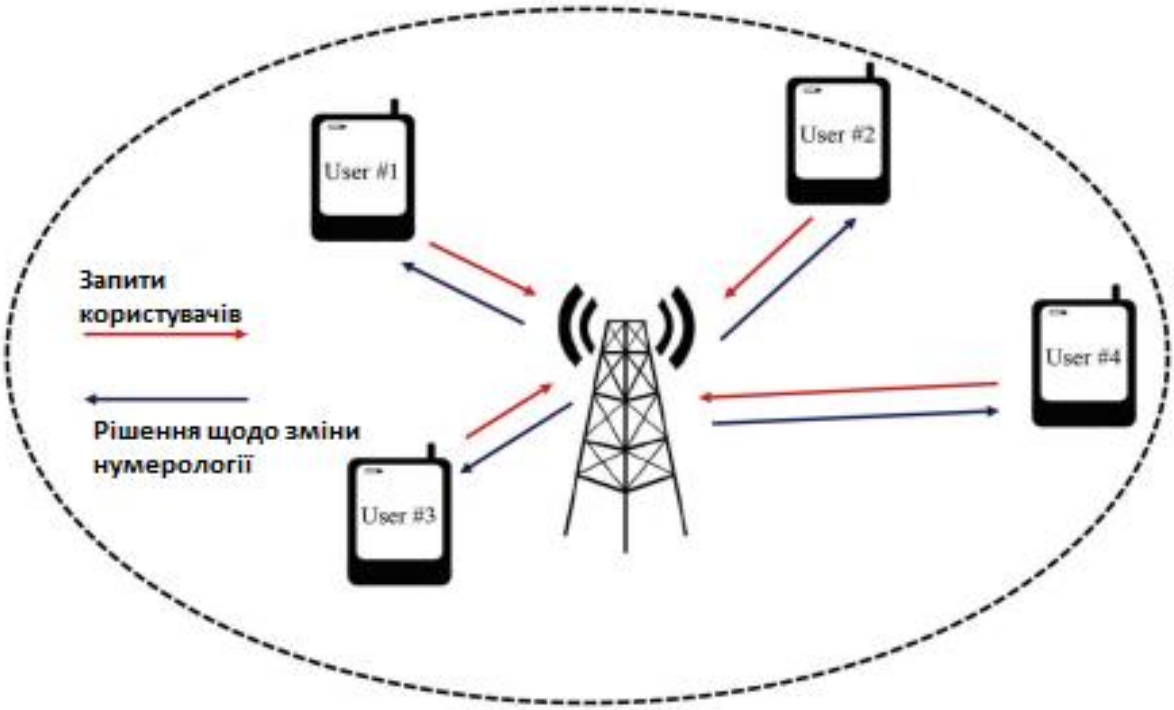

Рис. 1.15. Система оптимізації використання ресурсів

Представлена схема на Рис. 1.15 ілюструє підхід до оптимізації розподілу ресурсів. Запропонований алгоритм також включає активний механізм перемикання смуг ширини пропускання (BWP). Як вхідні параметри для алгоритму використовуються інтервал між піднесущими (Δf), тривалість циклічного префікса (TCP), а також вимоги до спектральної ефективності для всіх користувачів у межах однієї стільники.

Розширення кількості нумерологій понад стандартні п’ять, визначені в 5G, може допомогти повніше задовольнити вимоги різних користувачів і сервісів. Водночас таке розширення потребує більш складних механізмів для вибору відповідної нумерології. Щоб зменшити навантаження на обчислювальні ресурси, у майбутньому базові станції можуть застосовувати дворівневі підходи до відбору нумерологій. На першому етапі здійснюється вибір найбільш релевантного набору параметрів, а на другому — визначається оптимальна нумерологія з-поміж варіантів, обраних на попередньому етапі.

1.3.5. Використання машинного навчання в мережах п’ятого покоління

Упродовж останніх років спостерігається суттєве зростання попиту на передачу даних у бездротових мережах, що супроводжується високими вимогами до якості обслуговування користувачів (QoE — Quality of Experience). Згідно з прогнозом Cisco Visual Index, до 2021 року обсяг глобального інтернет-трафіку сягне 30 ГБ на одну особу, причому понад 63% трафіку припадатиме на бездротові й мобільні пристрої. Це зростання тісно пов’язане зі світовими тенденціями розвитку хмарних технологій та Інтернету речей, які активно сприяють цифровізації нашого повсякденного життя.

Очікується, що технології віртуалізації та роботизації стануть невід’ємною частиною майбутнього, що вимагатиме високорівневого інтелектуального контролю якості користувацького досвіду. Сучасні застосунки — такі як доповнена реальність, автономний транспорт, електронна медицина, цифрове врядування тощо — вимагають надвисокої пропускної здатності, мінімальних затримок та гарантованої надійності передачі даних. У добу великих даних, машинного навчання та штучного інтелекту зростає потреба у масштабованих методах обробки інформації, здатних реагувати на запити з мільярдів пристроїв протягом кількох мілісекунд [20].

Стрімке зростання обсягів трафіку в мобільних мережах змушує операторів впроваджувати нові рішення для підвищення пропускної здатності. Внаслідок цього мережі 5G стають дедалі складнішими з точки зору розгортання, керування та масштабування. Це, своєю чергою, зумовлює потребу у впровадженні інноваційних підходів до самонавчального проектування та автономного управління мережевою інфраструктурою.

У цьому розділі розглядається концепція інтелектуального формування променя з використанням технології Massive MIMO (Multiple Input Multiple Output). Основна ідея полягає у застосуванні методів глибинного навчання для оптимального налаштування фазових зсувів і амплітудних коефіцієнтів кожного антенного елемента. Запропоноване рішення дає змогу системі самостійно

адаптуватися до умов середовища, що суттєво підвищує продуктивність і потужність мереж 5G.

Машинне навчання — це набір алгоритмів, здатних навчатися на основі даних та приймати рішення або робити прогнози без необхідності чіткого програмного керування. Такі алгоритми вже активно застосовуються у сфері кібербезпеки, біоінформатики, медичної діагностики, пошукових систем тощо, де є потреба в автоматичній обробці великих обсягів інформації для отримання релевантних результатів.

Мобільні мережі мають складну архітектуру, а майбутні системи 5G будуть ще складнішими через різноманітність сценаріїв використання — таких як широкомасштабне впровадження енергоефективних сенсорів, інтелектуальні транспортні системи, наднадійні комунікації з низькою затримкою, корпоративні мережі тощо. Для ефективного управління цими складними умовами необхідна інтеграція інтелектуальних аналітичних рішень у структуру мереж наступного покоління.

Машинне навчання є ефективним інструментом для вирішення складних задач, які важко або навіть неможливо реалізувати традиційними методами. Зокрема, воно ідеально підходить для випадків, коли існуючі рішення потребують значної ручної настройки, або коли чітких алгоритмічних підходів взагалі не існує. Замість звичних програм із великою кількістю умов і правил, тут використовуються алгоритми, які самостійно навчаються на основі історичних даних.

Завдяки цьому, методи машинного навчання дозволяють виявляти аномальні ситуації, прогнозувати розвиток подій, адаптуватися до змін середовища, аналізувати великі обсяги інформації для отримання цінних висновків та знаходити приховані закономірності, які важко виявити традиційними способами [21]. На рис. 1.16 показано, як співвідносяться між собою глибоке навчання, машинне навчання та штучний інтелект.

Алгоритми машинного навчання аналізують вхідні дані, навчаються на них і згодом застосовують набуті знання для прийняття рішень. Глибоке навчання є

одним з напрямів машинного навчання, який працює за подібним принципом, але відрізняється за потужністю. Його моделі побудовані для багаторівневого аналізу інформації, що структуровано подібно до того, як люди обробляють дані. У додатках глибокого навчання використовується архітектура штучної нейронної мережі — багатошарової системи, натхненної біологічною нейронною мережею людського мозку. Це забезпечує ефективніший процес навчання порівняно зі звичайними підходами машинного навчання.

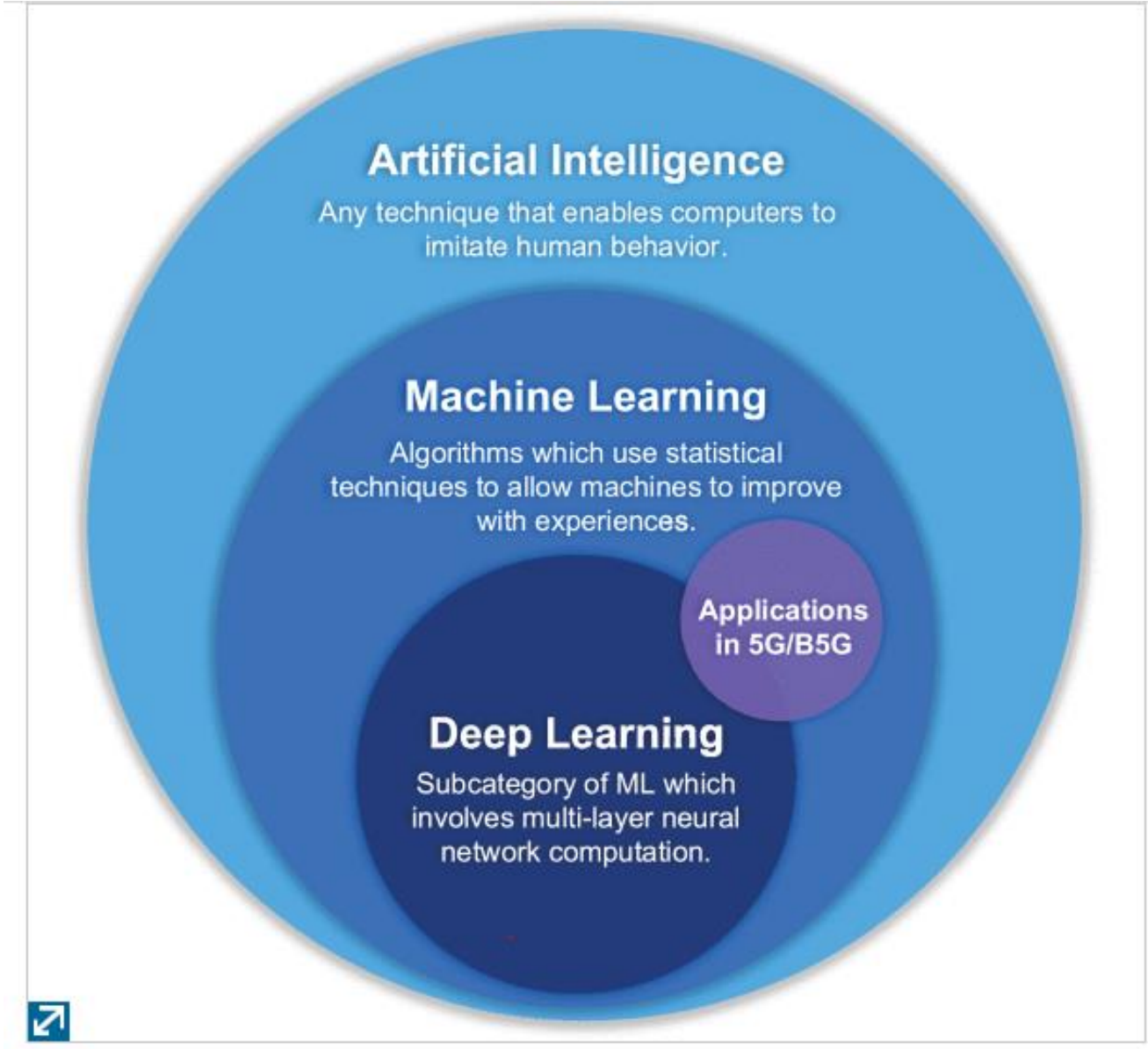

Рис.1.16. Структурна взаємозалежність штучного інтелекту, машинного та глибокого навчання

Таким чином, головна перевага глибокого навчання над традиційним машинним навчанням полягає в тому, що воно організовує алгоритми у вигляді

багаторівневої структури — штучної нейронної мережі, яка здатна до самостійного навчання та прийняття рішень.

Хоча використання глибинного навчання на фізичному рівні бездротового зв’язку — явище досить нове, вже сьогодні ця технологія може застосовуватися для задач розпізнавання типу модуляції, канального декодування, а також детектування сигналів, що сприяє покращенню ефективності існуючих бездротових систем. Окрім цього, глибоке навчання відкриває перспективи для розробки нових архітектур зв’язку, а також для розширення наявних експертних підходів у багаторежимних системах та системах з множинними антенами (MIMO).

1.3.6. Технології SDN та NFV

Інтеграція програмно-конфігурованих мереж (SDN) і віртуалізації мережевих функцій (NFV) відкриває нові можливості для створення гнучкої та масштабованої архітектури зв’язку, що особливо актуально для державного сектору [22].

Сучасна телекомунікаційна інфраструктура операторів базується на великій кількості спеціалізованих апаратних засобів. Впровадження нових послуг зазвичай потребує розширення фізичної інфраструктури шляхом додавання нового обладнання для забезпечення функціонування сервісів. При цьому необхідно враховувати низку технічних аспектів:

- наявність необхідних компонентів для стабільної роботи системи;
- відповідні площі для розміщення обладнання;
- забезпечення додаткових джерел живлення;
- створення відповідного мікроклімату в технічних приміщеннях.

Хоча впровадження нових рішень сприяє покращенню якості послуг, розширенню функціональних можливостей операторів і збільшенню користувацького потенціалу, воно також супроводжується певними недоліками: підвищене енергоспоживання, значні капітальні та операційні витрати, потреба у кваліфікованому персоналі для обслуговування.

Додатково, стрімке моральне старіння мережевого обладнання — навіть за відсутності фізичного зносу — змушує операторів частіше повторювати цикл "закупівля – проєктування – інтеграція – впровадження". З розвитком технологій цей цикл стає дедалі коротшим, що призводить до ситуації, коли витрати на підтримку й розвиток мереж перевищують доходи. Це доводить, що розширення інфраструктури шляхом нарощування спеціалізованого обладнання є неефективним у довгостроковій перспективі. Тому постає нагальна потреба в нових підходах до розвитку телекомунікаційного бізнесу та сервісної моделі провайдерів.

Програмно-конфігуровану мережу (SDN) визначають як підхід до адміністрування комп’ютерних мереж, що передбачає відокремлення функцій керування мережею (control plane) від рівня передачі даних (data plane). Завдяки цьому мережевими сервісами можна управляти за допомогою програмного забезпечення. Для додатків вищого рівня передбачено використання прикладних програмних інтерфейсів (API), що спрощує і пришвидшує впровадження нових сервісів.

Віртуалізація мережевих функцій (NFV) — це технологія, яка дозволяє виконувати традиційні функції мережевих пристроїв у вигляді програмного забезпечення, що працює на звичайних серверах, найчастіше на базі архітектури x86, у середовищі віртуальних машин (VM). Такі програмні компоненти можуть взаємодіяти один з одним для забезпечення телекомунікаційних послуг, замінюючи при цьому традиційні апаратні рішення.

Незважаючи на те, що SDN і NFV є самостійними технологіями, вони можуть ефективно доповнювати одна одну в процесі оптимізації мережевої інфраструктури.

У контексті цифрової трансформації державного сектору, поєднання SDN і NFV дозволяє оперативно адаптувати мережеву інфраструктуру до змінних умов, пришвидшує впровадження нових послуг, а також підвищує рівень безпеки завдяки централізованому управлінню трафіком і автоматизації захисних механізмів. Такий підхід є ключовим для побудови сучасної національної цифрової екосистеми, здатної швидко масштабуватись та реагувати на виклики кібербезпеки.

Архітектурна модель SDN та NFV зображена нижче на рис. 1.17.

Рис.1.17. Архітектурна модель SDN та NFV

SDN (Software Defined Networking) — це архітектурна концепція, яка створює основу для формування «мережі в мережі» з чітко визначеними параметрами та конфігурацією. Завдяки цьому мережа набуває ознак програмованості — її структуру можна адаптувати під потреби конкретних застосунків, використовуючи наявні ресурси. SDN також забезпечує відкритість і гнучкість у керуванні мережевими сервісами.

Ця технологія дозволяє автоматично налаштовувати мережу відповідно до вимог певних додатків або класів сервісів (наприклад, «business», «smart», «play») [23]. Додатки можуть звертатися до мережі для підключення до потрібних послуг і керування ними, а натомість отримувати інформацію про поточну топологію та стан мережі.

Ключова особливість SDN — логічне розділення площини передачі даних (data plane) і площини управління (control plane). Це розділення реалізується за допомогою стандартних протоколів, які забезпечують взаємодію між цими рівнями.

Отже, SDN — це не черговий мережевий протокол, а принципово нова архітектура управління мережею, яка забезпечує абстракцію та централізований контроль. Важливо, що для впровадження SDN не обов’язково повністю

оновлювати інфраструктуру — архітектура може працювати на базі існуючого обладнання, водночас докорінно змінюючи підхід до управління мережею.

Інтеграція SDN дає змогу значно пришвидшити впровадження нових сервісів, мінімізувати час реакції на мережеві інциденти та оптимізувати розподіл трафіку між сервісами залежно від їхніх пріоритетів. Завдяки централізованому контролю адміністратор може швидко реагувати на зміну навантаження, автоматично масштабувати ресурси або перенаправляти потоки даних у разі виявлення збоїв або атак.

Крім того, SDN відкриває нові можливості у сфері кібербезпеки. Завдяки централізованому управлінню та глобальному баченню мережі, система може впроваджувати динамічні політики доступу, виявляти аномальну поведінку в реальному часі та оперативно локалізовувати загрози. Це особливо важливо для критичних інфраструктур, органів державної влади та корпоративного сектору, де безперервність і захищеність комунікацій є пріоритетом.

Рис. 1.18. Порівняльна схема управління мережею без SDN і з SDN

NFV (Network Functions Virtualization) — це підхід до віртуалізації функціональності мережевих елементів, що використовуються операторами зв’язку. Основна ідея NFV полягає в тому, щоб виконувати функції керування мережею та надання сервісів за допомогою програмного забезпечення замість застосування спеціалізованого апаратного обладнання.

Архітектура NFV була розроблена Європейським інститутом телекомунікаційних стандартів (ETSI) і описана у документі ETSI GS NFV-0010 V0.1.7.показана на рис. 1.19.

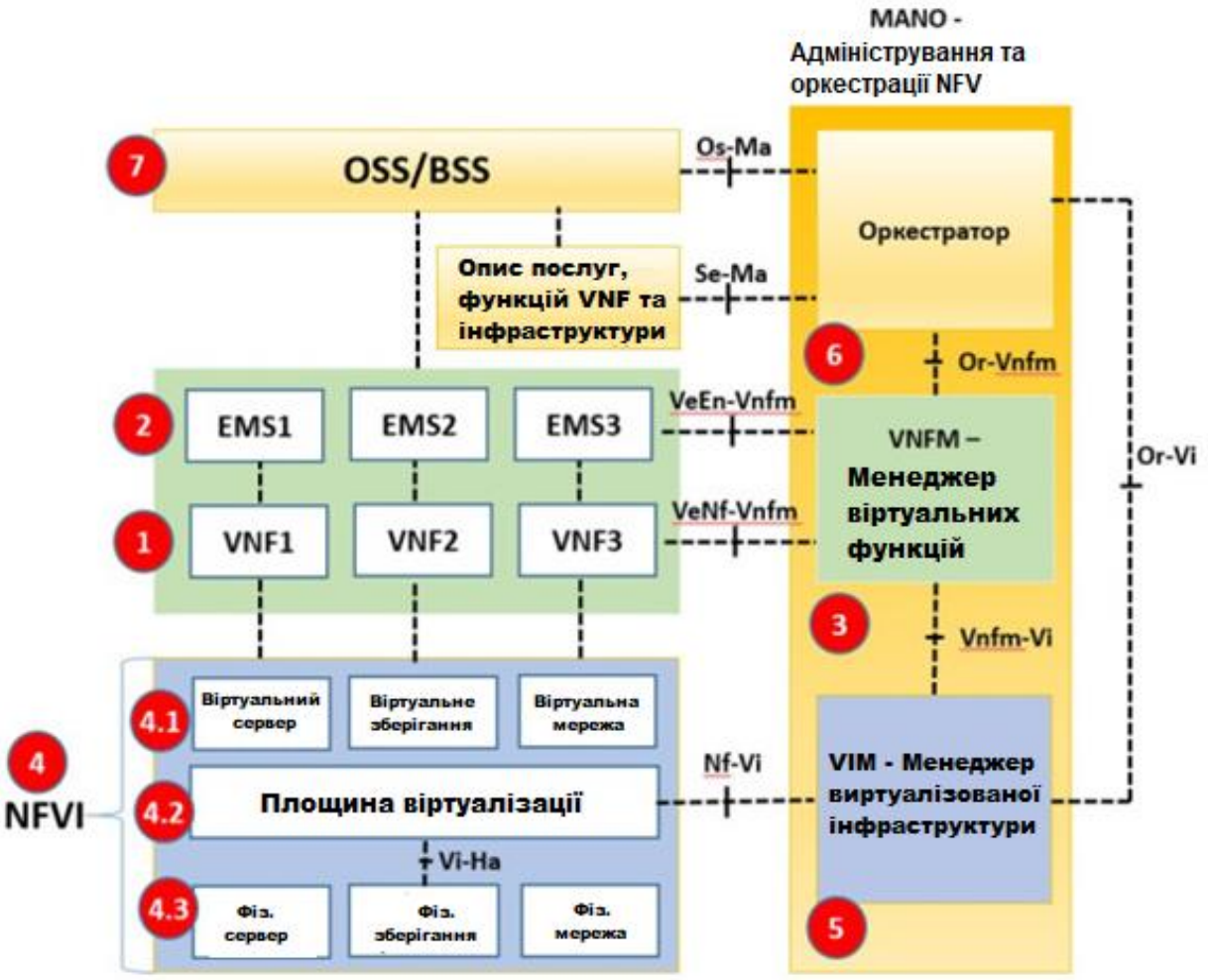

Рис. 1.19. Модель архітектури NFV у телекомунікаційного провайдера

Однією з ключових переваг архітектури NFV є можливість реалізації концепції «оркестрації послуг», що полягає у динамічному виділенні віртуалізованих ресурсів для виконання конкретних мережевих функцій за запитом. Це забезпечує максимально ефективне використання апаратних ресурсів, таких як сервери, сховища та мережеві компоненти. Центральну роль у цій архітектурі відіграє компонент MANO (Management and Orchestration) — система керування та оркестрації, яка забезпечує повноцінне функціонування NFV-середовища.

Детальніше розглянемо основні складові архітектури NFV:

1. Віртуальні мережеві функції (VNF — Virtual Network Functions). VNF є базовими будівельними блоками NFV-архітектури. Це програмні реалізації функцій мережевих елементів, таких як маршрутизатори (Router VNF), базові станції (BS VNF) тощо. Крім того, одна VNF може відповідати лише окремій функції апаратного елемента, наприклад, лише пересиланню пакетів, тоді як сукупність таких VNF реалізує повноцінний функціонал фізичного пристрою. До прикладу, такі компоненти як IMS, GGSN або SGSN також можуть бути реалізовані у вигляді VNF. Варто розрізняти поняття: NFV — це технологічна концепція, а VNF — окрема функціональна одиниця в межах цієї концепції.

2. Система управління елементами (EMS — Element Management System). EMS відповідає за адміністрування VNF-компонентів, зокрема їх конфігурацію, моніторинг, управління відмовами (fault management), продуктивністю (performance management) тощо. Аналогічно до того, як у традиційних мережах використовується NMS (Network Management System), у віртуалізованих середовищах ця роль покладається на EMS. Керування між EMS і VNF здійснюється через закриті (пропрієтарні) інтерфейси, і наразі у специфікаціях NFV не передбачено конкретного стандартного позначення цієї взаємодії. Очікується, що майбутні редакції стандарту деталізують цю точку. Одну VNF може обслуговувати окрема EMS, або ж одна EMS може керувати кількома VNF. До того ж, EMS може бути реалізована як віртуальна функція, яка сама потребує управління від вищого рівня EMS.

3. Менеджер віртуальних мережевих функцій (VNFM — VNF Manager) VNFM відповідає за керування однією або декількома VNF та забезпечує повний життєвий цикл цих функцій: від ініціалізації та обслуговування — до завершення роботи. На відміну від EMS, VNFM діє через визначену стандартом ETSI референсну точку Ve-Vnfm. Це дає змогу реалізовувати керування в рамках архітектури NFV більш узгоджено. Поняття «референсна точка» (reference point) у цьому контексті відрізняється від «інтерфейсу», оскільки вона визначає логічний зв’язок або взаємодію між функціональними блоками, незалежно від конкретного способу реалізації або протоколу.

4. Інфраструктура віртуалізації мережевих функцій (NFVI — Network Functions Virtualization Infrastructure). NFVI — це середовище, в якому працюють VNF. Вона включає фізичні ресурси, рівень віртуалізації та віртуалізовані ресурси, які подані нижче.

- 4.1 Віртуальні ресурси — це логічно абстраговані компоненти, що включають обчислювальні ресурси, мережу та сховища. Саме вони використовуються для роботи VNF, при цьому фізичні ресурси залишаються прихованими від рівня додатків.
- 4.2 Рівень віртуалізації (Virtualization Layer) — відповідає за створення абстракції фізичних ресурсів. Тут використовується гіпервізор — спеціальне програмне забезпечення, яке дозволяє запускати віртуальні машини незалежно від конкретного апаратного забезпечення. Завдяки цьому програми та операційні системи можуть бути розгорнуті на будь-якому доступному сервері.
- 4.3 Фізичні ресурси — це «залізна» частина інфраструктури, яка включає сервери, комутатори, системи зберігання даних тощо. Саме на цій базі функціонують усі віртуалізовані компоненти NFV.

5. Менеджер інфраструктури віртуалізації (VIM — Virtualized Infrastructure Manager). VIM здійснює управління всією інфраструктурою NFVI в межах одного адміністративного домену. Він відповідає за моніторинг та керування ресурсами — як фізичними, так і віртуальними. Крім того, VIM виконує збір телеметрії, аналітики продуктивності та подій, що виникають у межах інфраструктури.

6. Оркестратор NFV (NFV Orchestrator). NFV-оркестратор виконує завдання координації, керування життєвим циклом мережевих сервісів, що базуються на віртуальних функціях (VNF). Він здійснює створення та об’єднання кількох VNF у повноцінну мережеву послугу, а також відповідає за глобальне керування ресурсами інфраструктури NFVI. Зокрема, оркестратор адмініструє обчислювальні, мережеві та сховищні ресурси, розподілені між кількома VIM (менеджерами віртуалізованої інфраструктури). Варто зазначити, що взаємодія оркестратора з VNF здійснюється опосередковано — через VNFM та VIM.

7. Системи підтримки операцій і бізнесу (OSS / BSS — Operations Support System / Business Support System) OSS/BSS — це функціональні системи оператора, які забезпечують підтримку операційної діяльності та управління бізнес-процесами.

- OSS (Operation Support System) охоплює задачі керування мережею, включаючи управління конфігураціями, обробку збоїв та надання сервісів.
- BSS (Business Support System) відповідає за взаємодію з абонентами, включаючи управління клієнтськими даними, продуктами, замовленнями та білінгом.

У рамках архітектури NFV ці системи можуть бути інтегровані з MANO (Management and Orchestration) через стандартні інтерфейси, що забезпечує узгоджену взаємодію між бізнес-рівнем і технічною платформою.

1.3.7. Технологія MEC

Технологія Multi-Access Edge Computing (MEC) створює можливості для розробників додатків та постачальників контенту завдяки наданню хмарних обчислювальних ресурсів і IT-сервісів безпосередньо на межі телекомунікаційної мережі [24]. Це середовище забезпечує мінімальні затримки, високу пропускну здатність та прямий доступ до радіомережевої інформації в режимі реального часу, що дозволяє створювати адаптивні та продуктивні застосунки.

MEC формує нову екосистему та ціннісний ланцюг, відкриваючи радіомережі операторів мобільного зв’язку для сертифікованих третіх сторін. Такий підхід дозволяє швидко впроваджувати інноваційні сервіси, орієнтовані на споживачів, підприємства та галузеві рішення.

Ця технологія є еволюційним етапом розвитку мобільної інфраструктури, де поєднуються IT-можливості та телекомунікації. MEC дозволяє операторам залучати нові вертикальні сегменти та пропонувати сучасні сервіси для бізнесу й кінцевих користувачів. Серед них:

- аналітика відеоданих

- сервіси геолокації
- рішення для Інтернету речей (IoT)
- доповнена реальність
- локалізоване розповсюдження контенту
- кешування даних на мережевому краї

Завдяки MEC додатки можуть взаємодіяти з локальними даними в режимі реального часу, за умови наявності доступу до крайової інфраструктури. Це дозволяє зменшити навантаження на основну мобільну мережу, зберігаючи її ресурси для глобального трафіку та масштабних завдань.

Оператори отримують можливість стандартизовано відкривати інтерфейси радіодоступу (RAN) для партнерів, які можуть розгортати власні застосунки з низькими затримками та з доступом до оперативної мережевої інформації. MEC забезпечує гнучке середовище для реалізації рішень з максимальною ефективністю й мінімальною затримкою. (рис. 1.20) [25].

Рис.1.20. Концептуальна побудова MEC-інфраструктури

Нещодавно робоча група ETSI, яка відповідає за розвиток MEC, розширила сферу своєї діяльності, включивши підтримку різноманітних мережевих

технологій. У зв’язку з цим офіційно було введено термін Multi-Access Edge Computing.

Завдяки архітектурі MEC оператори отримують можливість розгортати сервіси на мережевому краї, що відкриває нові горизонти для CDN, DNS, 5G, IoT та мобільного трафіку, включаючи телеметричні рішення. Вони зможуть запропонувати геолокаційні послуги, відеоаналітику, доповнену реальність, а також сервіси для підключених транспортних засобів.

Крім того, MEC дозволяє операторам надавати свою інфраструктуру у вигляді сервісу третім сторонам. Це надзвичайно корисно для малого та середнього бізнесу, що прагне впроваджувати передові технології.

Технологія Multi-Access Edge Computing ідеально підходить для підготовки інфраструктури до роботи з додатками, що потребують високої пропускної здатності та мінімальних затримок. Вона також створює підґрунтя для плавного переходу до повноцінних 5G-мереж.

Однією з ключових переваг MEC є здатність обробляти критичні дані локально, без потреби передавання їх до віддалених дата-центрів. Це особливо важливо для додатків, де затримка в мілісекундах може мати вирішальне значення — наприклад, у сфері охорони здоров’я, автономного транспорту або промислового контролю.

Крім того, MEC сприяє підвищенню рівня безпеки, оскільки чутлива інформація обробляється ближче до джерела її генерації. Це зменшує ризик перехоплення або втрати даних у процесі передачі, а також дозволяє реалізовувати адаптивні механізми авторизації, автентифікації та реагування на загрози безпосередньо на мережевому краї. Таким чином, MEC стає ключовим елементом у побудові надійних, розподілених і масштабованих цифрових екосистем.

Крім суто технічних переваг, впровадження MEC створює сприятливі умови для розвитку нових бізнес-моделей у сфері цифрових послуг. Провайдери можуть монетизувати інфраструктуру, пропонуючи **Edge-as-a-Service (EaaS)** для стартапів, муніципалітетів, агросектору або освітніх установ. Такий підхід дозволяє ефективно використовувати локальні ресурси, зменшуючи залежність від

централізованих хмарних сервісів, і водночас стимулює розвиток інноваційних продуктів, орієнтованих на потреби конкретних регіонів або спільнот.

1.3.8. Хмарна інфраструктура Cloud RAN

Представлено інфраструктуру Cloud RAN для організації радіодоступу на Рис. 1.21.

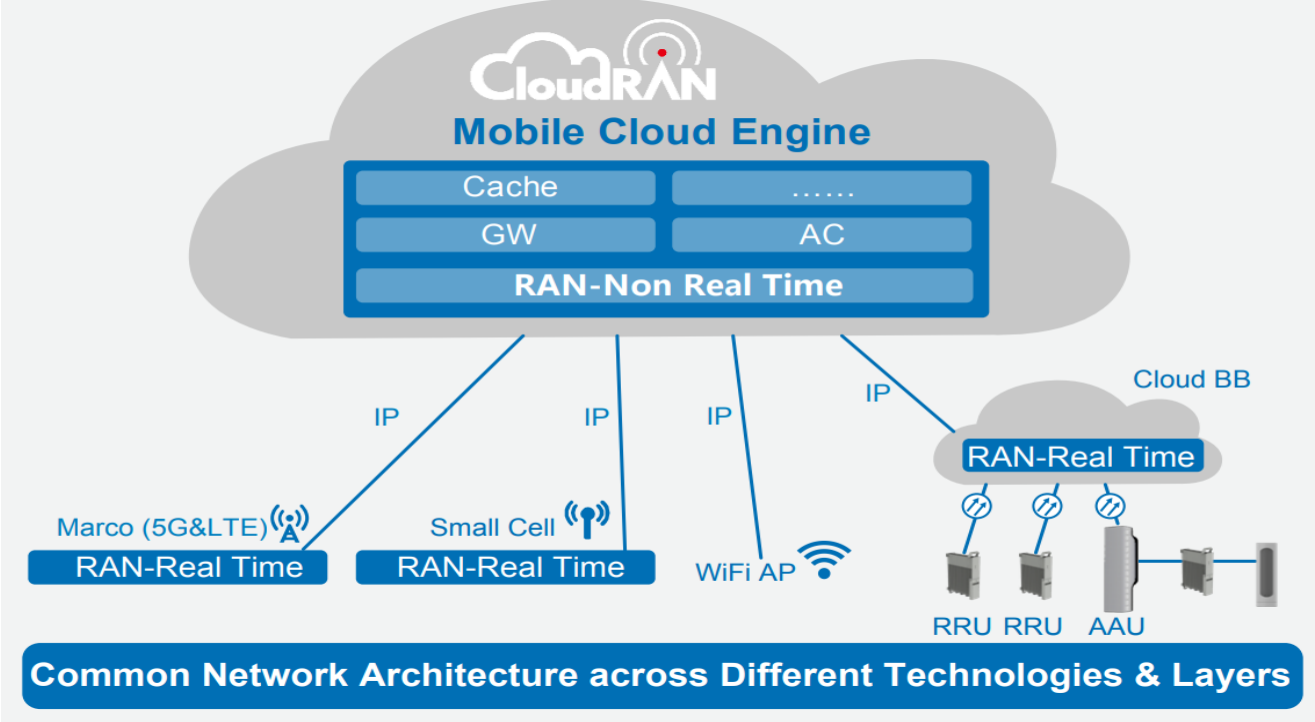

Рис. 1.21. Інфраструктура Cloud RAN для організації радіодоступу

Функціональні завдання RAN у режимі реального часу включають планування доступу до мережі, регулювання потужності сигналу, керування інтерференцією, організацію повторних передач, а також модуляцію та кодування. Усі ці процеси вимагають високої обчислювальної продуктивності та забезпечення миттєвої обробки даних. Саме тому впровадження хмарного підходу до RAN має низку суттєвих переваг:

- Можливість реалізації програмно-керованих базових станцій, які підтримують мультистандартні режими роботи (NR/E-UTRA), а також гнучкість і масштабованість віртуалізованих рішень.

- Розміщення обладнання базових станцій у захищених дата-центрах, що відповідають високим стандартам надійності та безпеки.
- Єдина хмарна інфраструктура Cloud RAN забезпечує централізоване управління великою кількістю радіомодулів на великих територіях покриття. Це дозволяє ефективніше використовувати частотний ресурс, покращує алгоритми придушення перешкод, оптимізує багатоточкову передачу (CoMP) та внутрішньомережеві хендовери (Intra-RAT).[26].

1.3.9. Технологічні розробки для забезпечення додаткового функціоналу мереж 5G

Для зменшення енергоспоживання IoT- та M2M-пристроїв розробляються вузькосмугові радіомодулі з покращеною енергоефективністю. Вони підтримують розширені режими сну, подовжений інтервал пейджингу та можливість підключення до мережі згідно із заздалегідь визначеним графіком для передачі даних. Окрім цього, зниження вартості таких пристроїв досягається завдяки використанню хмарних технологій, які дозволяють передавати частину обчислювального навантаження з пристрою на прикладні сервіси в мережі.

Для розширення покриття мережі 5G активно впроваджується концепція мобільних базових станцій, що можуть бути розміщені на рухомих об’єктах, таких як транспортні засоби. Ці мобільні вузли формують динамічні мережі радіодоступу, які здатні не лише взаємодіяти між собою, а й підключатися до стаціонарної інфраструктури. Їх робота організована за принципом MESH-мереж [17], де кожен елемент одночасно виконує роль ретранслятора, тим самим забезпечуючи розширення зони покриття.

Впровадження таких рішень відкриває нові можливості для розвитку автономного транспорту та інтелектуальних систем управління дорожнім рухом. Крім того, передбачається активне поширення технології прямої взаємодії між пристроями — Device-to-Device (D2D). Цей підхід дозволяє здійснювати обмін даними між абонентами без залучення центральної мережевої інфраструктури, що сприяє підвищенню спектральної ефективності, зниженню затримок та

енергоспоживання. Особливе значення D2D-зв’язок має для реалізації рішень у сфері професійної та технологічної комунікації.

1.4 Аналіз багатошарової структури мереж 5G

Впровадження ієрархічної багатошарової архітектури мережі дає змогу ефективно розподіляти навантаження між макро-, мікро- та пікосотами, що позитивно впливає на загальну масштабованість і надійність системи [27]. Швидке зростання споживання мультимедійного контенту та запити користувачів на якісні сервіси стимулювали радикальні зміни в управлінні телекомунікаційною інфраструктурою, зокрема в аспектах маршрутизації, контролю та надання послуг.

5G вважається технологічною платформою майбутнього, здатною підтримувати широкий спектр вертикальних додатків із різноманітними вимогами до продуктивності та обслуговування. Для реалізації цього бачення фізичну інфраструктуру мережі необхідно логічно розділити на кілька ізольованих сегментів — так званих мережевих зрізів (network slices). Кожен такий сегмент має специфічну конфігурацію, адаптовану під вимоги певного типу трафіку, наприклад, масовий IoT, мобільні пристрої або автономні транспортні системи.

Оскільки різні сценарії використання в межах 5G вимагають різних характеристик обслуговування, таких як швидкість передачі, затримки, надійність чи зона покриття, виникає потреба в інноваційних механізмах — зокрема, у розгортанні малих сот, інтелектуальному керуванні трафіком та автоматизованому контролі ресурсів.

Network slicing — це технологія поділу фізичної інфраструктури на декілька логічних віртуальних мереж, кожна з яких орієнтована на окремий набір послуг, додатків або клієнтів. Вона об'єднує можливості SDN (програмно-керованих мереж) і NFV (віртуалізації функцій) для створення гнучкої та адаптивної архітектури.

Цей підхід також передбачає відокремлення площини управління (Control Plane) від площини користувача (User Plane), переміщуючи функції користувача

ближче до краю мережі (edge). Кожен зріз може мати власну унікальну архітектуру, політику керування та захисту, орієнтовану на конкретний випадок використання. Такий підхід дозволяє індивідуально розподіляти ресурси — пропускну здатність, щільність підключень, зону покриття — відповідно до потреб кожного сервісу.

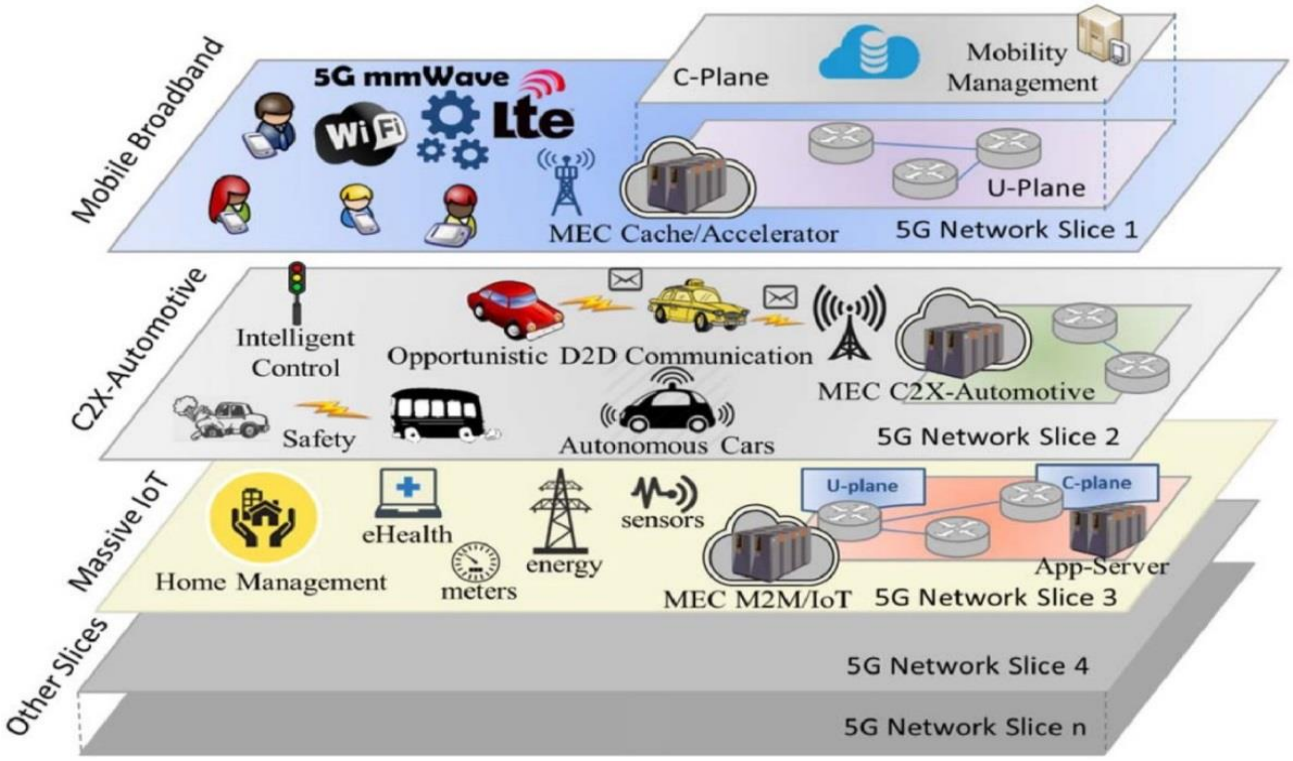

Рис. 1.22. Фундаментальна ідея технології Network Slicing

Якщо мережеве з'єднання забезпечує низьку затримку та достатню пропускну здатність, пріоритетність обробки даних може реалізовуватись на рівні програмного управління мережею. У межах network slicing логічні зрізи, що функціонують на спільній фізичній інфраструктурі, ізольовані один від одного. Це означає, що проблеми безпеки або перевантаження в одному зрізі не впливають на інші.

Програмно-керована мережа (SDN)

SDN (Software-Defined Networking) — це концепція, що дозволяє створювати інтелектуальні, адаптивні мережі, які є повністю програмованими. Такий підхід дає змогу керувати додатками та сервісами з високим рівнем деталізації на всьому протязі мережевої інфраструктури. За визначенням Open Network Foundation

(ONF), SDN передбачає фізичне відокремлення площини керування (control plane) від площини передачі даних (data plane), при якому одна система управління може централізовано контролювати численні мережеві пристрої.

Це розділення забезпечує гнучкість, централізований контроль і цілісне уявлення про мережу, дозволяючи швидко адаптуватися до змін ринку, вимог користувачів або мережевих умов. SDN створює віртуалізоване середовище керування, яке усуває розрив між рівнем управління інфраструктурою та рівнем надання сервісів, забезпечуючи автоматизацію й інтелектуальні функції керування.

Керування SDN-мережею реалізується за допомогою стандартизованих southbound-інтерфейсів (SBI), таких як OpenFlow, FoRCES або OpFlex. Вони визначають спосіб комунікації між мережевими елементами передачі даних і контролерами керування.

Площина передачі даних SDN може бути реалізована на базі загальнодоступного апаратного забезпечення, зокрема з використанням платформ, як-от VMware NSX, що складається з централізованого контролера та віртуального комутатора (vSwitch), забезпечуючи повну віртуалізацію мережевого середовища.

Разом з тим, ефективність реалізації SDN-рішень значною мірою залежить від вимог до продуктивності та масштабованості середовища, у якому вони застосовуються. Наукові кола, галузеві експерти та провідні організації зі стандартизації, зокрема ONF (Open Networking Foundation), SDNRG (Software Defined Networking Research Group) Інтернет-дослідницького фонду (IRTF) та Інженерна робоча група Інтернету (IETF), вже давно визнають значний потенціал SDN і активно формують його архітектуру, ключові інтерфейси та функціональні вимоги, орієнтовані на мережі п’ятого покоління.

SDN спрямований на подолання обмежень традиційних мережевих архітектур, які не відповідають вимогам до гнучкості, масштабованості, централізованого управління та динамічної конфігурації. Це особливо актуально для сучасних центрів обробки даних, кампусів та гетерогенних мережевих середовищ.

Концепція SDN у контексті аналізу і підтримки network slicing для 5G була глибоко розроблена ONF. У цьому підході кожен контекст клієнта розглядається як окремий логічний зріз мережі. Контролер SDN використовується для керування цими зрізами шляхом застосування набору політик або правил, що визначають поведінку мережі.

Контролер SDN створює й підтримує окремі контексти для клієнта і сервера, керуючи відповідними ресурсами, необхідними для обслуговування запитів користувачів. Зокрема, він підтримує логіку клієнтського контексту кожного зрізу, а також виконує оркестрацію ресурсів у серверному контексті.

Це дозволяє групувати логічні зрізи, які належать до одного контексту, і динамічно ними управляти в межах віртуалізованої мережі. Такий підхід забезпечує гнучке, адаптивне і масштабоване управління сервісами у середовищі 5G.На рис. 1.23. представлена архітектура SDN:

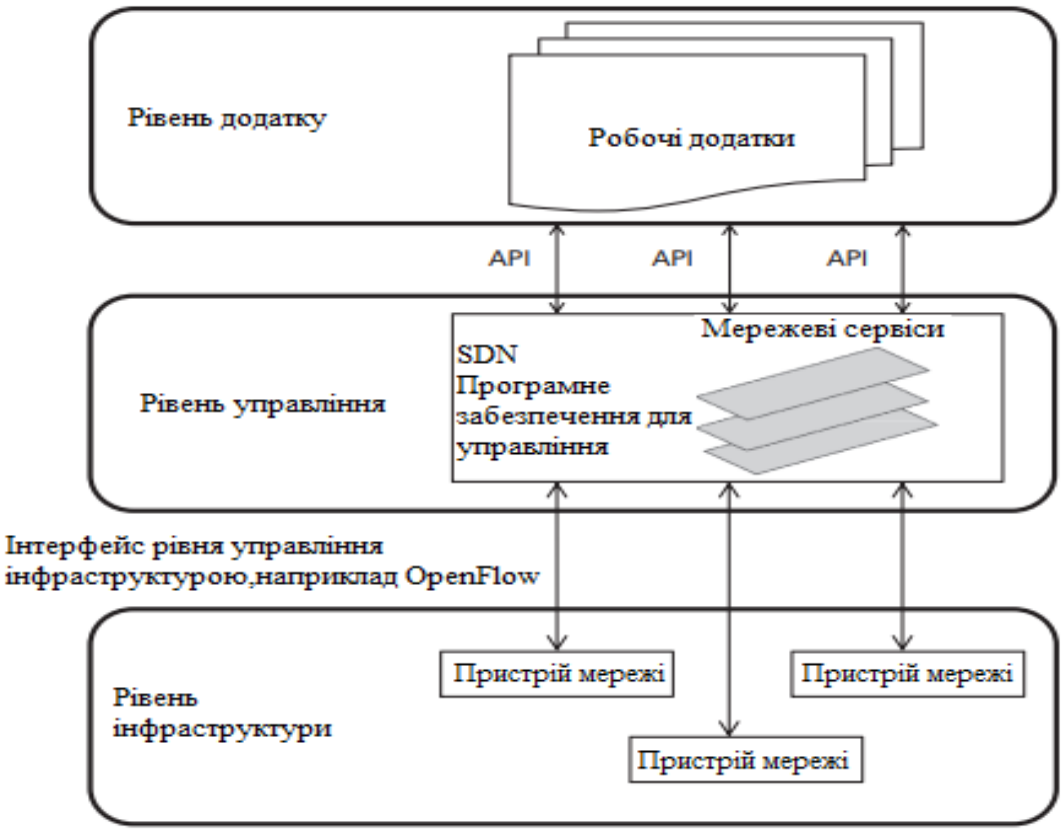

Рис. 1.23. Архітектура SDN

NFV — віртуалізація мережевих функцій

NFV (Network Functions Virtualization) — це концепція віртуалізації функцій мережевої інфраструктури, таких як міжмережеві екрани, VPN, TCP-оптимізатори, NAT64, DPI, які зазвичай реалізуються на спеціалізованому обладнанні. У підході NFV ці функції розгортаються як віртуальні мережеві функції (VNF) на стандартних, недорогих апаратних платформах.

Такий підхід руйнує традиційну модель «програмне забезпечення + апаратне забезпечення», характерну для постачальників мережевих рішень, і натомість дозволяє динамічно масштабувати й гнучко розгортати VNF у межах єдиної інфраструктури. NFV дає змогу ефективно розподіляти ресурси між віртуальними функціями, організовувати логічні ланцюжки сервісів (Service Function Chaining — SFC) і знижувати залежність від фізичних обмежень.

Завдяки віртуалізації, частина мережевих функцій може розгортатися безпосередньо в інфраструктурі постачальника послуг (SP), а не на стороні клієнта. Це суттєво спрощує оновлення, масштабування або видалення функцій — достатньо внести зміни на стороні провайдера, не втручаючись у клієнтське обладнання.

Для операторів зв’язку NFV відкриває нові можливості:

- Зменшення капітальних (CAPEX) та операційних витрат (OPEX) завдяки використанню універсального обладнання.
- Гнучке масштабування послуг під актуальні потреби клієнтів.
- Прискорене виведення нових сервісів на ринок завдяки скороченню часу розгортання.

У контексті 5G, технологія NFV забезпечує ефективний розподіл ресурсів із урахуванням QoS, підтримує низькі затримки, стабільну продуктивність і сумісність з традиційними (не-VNF) рішеннями.

Ключові переваги NFV у порівнянні з класичними мережами:

1. Розділення програмного забезпечення та апаратної платформи. Програмне забезпечення виконується незалежно від апаратної інфраструктури, що дає змогу легко адаптувати і масштабувати рішення.

2. Гнучкість у розгортанні мережевих функцій. Один і той самий апаратний ресурс може використовуватись для реалізації різних VNF у залежності від ситуації.

3. Динамічне керування послугами**.** Оператори можуть швидко впроваджувати індивідуальні сервіси на основі потреб клієнтів, адаптуючи навантаження та продуктивність VNF у режимі реального часу.

На рис. 1.24 представлена модель побудови NFV-середовища:

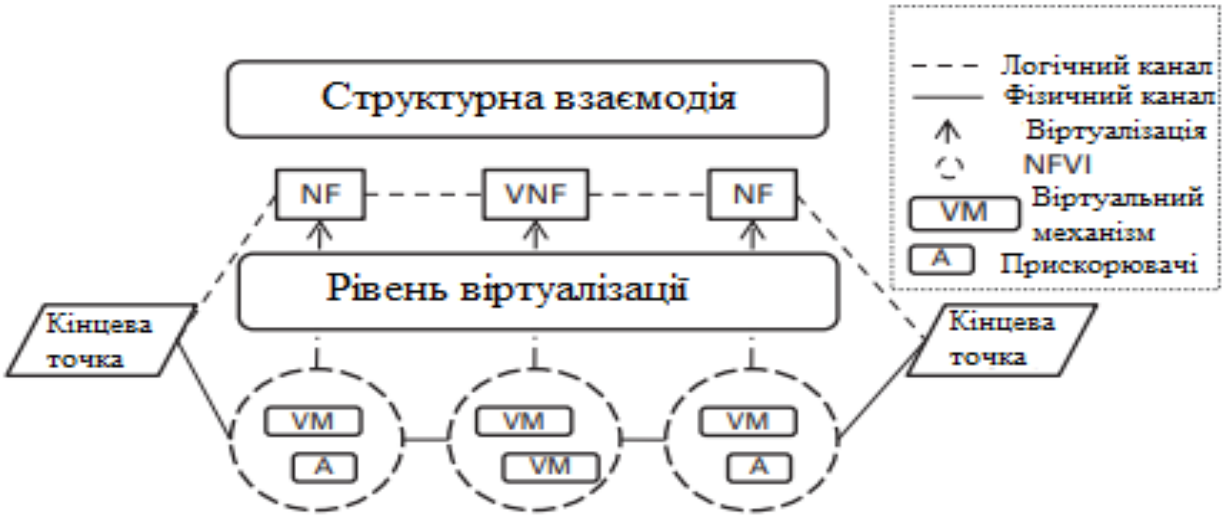

Рис. 1.24. Модель побудови NFV-середовища

Граничні обчислення з множинним доступом (MEC)

MEC (Multi-access Edge Computing) — це концепція, яка надає розробникам програмного забезпечення та постачальникам контенту обчислювальні ресурси і IT-сервіси безпосередньо на межі мобільної мережі. Обробка даних здійснюється максимально близько до місця їх генерації та використання, що забезпечує мінімальні затримки — ключовий фактор для критично важливих бізнес-додатків та інтерактивних сервісів у середовищах з високою концентрацією користувачів (наприклад, вокзали, аеропорти, торгові центри).

Локальне опрацювання даних дозволяє знизити навантаження на ядро мережі і суттєво скоротити витрати на передачу трафіку. Крім цього, MEC впроваджує такі переваги в архітектуру 5G:

1. Покращення показників якості обслуговування (QoS) та досвіду користувача (QoE), зокрема під час відеостримінгу, який інтегровано через network slicing.

2. Оптимізація використання мобільних ресурсів, завдяки розміщенню ресурсомістких компонентів додатків безпосередньо на краю мережі.

3. Трансформація вузлів доступу в інтелектуальні хаби, які можуть надавати контекстно-залежні послуги, використовуючи дані з радіомережі (наприклад, інформацію про геолокацію, завантаженість соти або виділену пропускну здатність).

Роль MEC у контексті нарізки мережі (network slicing) в архітектурі 5G

Ключовим компонентом MEC є сервер додатків, який функціонує поверх хмарної інфраструктури MEC NFVI. Цей сервер виконує хостинг MEC-додатків (MEC Apps), які взаємодіють із платформою MEC через спільні комунікаційні інтерфейси.

Платформа MEC надає необхідні сервіси для додатків і виконує роль посередника, реалізуючи API для взаємодії між додатками MEC та внутрішніми сервісами.

Обчислювальні вузли MEC можуть бути розміщені локально (у ЦОД) або віддалено — в хмарному середовищі.

Важливою функцією є розвантаження трафіку (Traffic Offloading Function — TOF), яка реалізується на рівні data plane. Вона забезпечує:

- моніторинг трафіку в реальному часі
- пріоритизацію пакетів
- гнучке перенаправлення згідно з визначеними політиками

Це робить MEC незамінним компонентом для забезпечення динамічної якості сервісів та адаптивного керування мережею в умовах 5G.

1.5 Аналіз ефективності використання наявних рішень

1. Граничні обчислення з множинним доступом (MEC)

Технологія MEC дозволяє обробляти дані безпосередньо на межі мережі, тобто максимально близько до кінцевого користувача. Це значно знижує затримки, підвищує швидкість реакції сервісів і зменшує навантаження на центральні дата-центри. Основні переваги MEC полягають у забезпеченні критичних показників QoS/QoE, оптимізації мобільних ресурсів, а також у можливості реалізації контекстно-залежних сервісів (наприклад, визначення локації користувача або адаптивне розподілення трафіку в реальному часі) [28]. Разом із тим, MEC має обмеження: це складність інтеграції в наявну інфраструктуру, менша обчислювальна потужність у порівнянні з хмарними ЦОД, а також підвищені вимоги до координації з технологіями SDN і NFV. Підвищити ефективність MEC можливо через впровадження штучного інтелекту, машинного навчання, контейнеризації (Docker, Kubernetes), Zero Trust архітектури та інтеграцію з network slicing.

2. Хмарна радіомережа доступу (Cloud RAN)

Cloud RAN дозволяє централізувати обробку даних радіомережі, використовуючи хмарні ресурси, що дає змогу знизити вартість обладнання, спростити управління мережею та оптимізувати використання частотного спектра. Ця технологія також дозволяє швидко впроваджувати нові послуги через віртуалізацію функцій і тісну інтеграцію з SDN/NFV. Серед недоліків — високі вимоги до пропускної здатності транспортної мережі, можливі затримки через централізовану обробку, складність адаптації до існуючих мобільних систем, а також виклики у сфері безпеки. Методами покращення ефективності Cloud RAN є: поєднання з MEC для зменшення затримок, застосування AI для управління ресурсами, сегментація мережі за допомогою network slicing, а також підвищення рівня безпеки за рахунок шифрування та моделі Zero Trust.

3. Антенні системи Massive MIMO

Massive MIMO — це технологія, яка забезпечує значне збільшення пропускної здатності мережі завдяки великій кількості антенних елементів, що працюють паралельно. Серед її ключових переваг — високошвидкісні з'єднання, покращене покриття мережі за рахунок формування вузьких променів (beamforming), зниження завад, а також ефективніше використання енергії. Втім, система вимагає складного управління, значних обчислювальних ресурсів і складної інтеграції. Також існують проблеми з енергоспоживанням на передавальній стороні. Підвищення ефективності Massive MIMO можливе через оптимізацію алгоритмів формування променів, інтеграцію з системами штучного інтелекту, а також розумне керування просторовими ресурсами.

Висновки

MEC, Cloud RAN і Massive MIMO є фундаментальними технологіями для розвитку мереж 5G, оскільки вони дозволяють досягти нових рівнів продуктивності, адаптивності та ефективності. Проте кожна з них вимагає вирішення низки викликів — від технічної інтеграції до питань безпеки і керування ресурсами. Їх поєднання, з використанням AI, контейнеризації та мережевої сегментації, дозволяє створювати дійсно гнучкі, масштабовані і ефективні архітектури зв'язку майбутнього.[29].

Особливо актуальною задачою є розвиток стільникових мереж зв’язку для нашої країни. Існуючі мережі зв’язку вже не можуть задовольнити потреби ринку за якістю та ефективністю обміну інформацією.

Тому в даному розділі було проведено дослідження ефективності функціонування стільникових мереж як в Україні зокрема, так і в світі.

Зокрема, спочатку було проведено змістовний аналіз сучасних стільникових мереж, які діють по всьому світу, з метою визначення їхніх недоліків та потенційних шляхів їх покращення. Були досліджені мережі 4G, їх архітектура та якість обслуговування на сьогоднішній день. За результатами досліджень було встановлено не досить задовільну якість обслуговування абонентів та відповідно

ефективність функціонування стільникових мереж. Тому було проаналізовано, які проблеми є причиною цього.

Після цього було проаналізовано вимоги до стільникових мереж нового покоління та технологічні рішення, які можуть допомогти їх досягти. Було встановлено ряд їх недоліків та були встановлені шляхи їх усунення.

Постановка задач дисертаційного дослідження

Основні принципи побудови та функціонування ССЗ Держспецзв'язку

Розробка системи стільникового зв'язку Держспецзв'язку передбачає формування організаційно-технічних рішень, що забезпечать захищений, надійний та стійкий мобільний зв'язок для потреб військових, державних органів, критичної інфраструктури тощо.

Основні принципи роботи та побудови ССЗ включають:

1. Модульна архітектура та сегментація мережі – побудова системи на основі захищених автономних зон зв'язку з можливістю інтеграції з існуючими державними та військовими комунікаційними платформами.

2. Використання сучасних стандартів мобільного зв'язку – впровадження технологій 4G/5G із перспективою розвитку 6G, що дозволяє реалізувати захищений голосовий зв'язок, передачу даних і мультимедійний трафік.

3. Криптографічний захист зв'язку – інтеграція національних криптографічних стандартів для забезпечення конфіденційності, цілісності та автентифікації користувачів.

4. Резервування та стійкість до атак – розробка автономних резервних каналів, що гарантують стійкість до кібератак, електронних перешкод та фізичних пошкоджень мережевої інфраструктури.

5. Інтеграція з системами екстреного зв'язку – підтримка міжвідомчої взаємодії між органами державної влади, військовими структурами та службами безпеки в умовах надзвичайних ситуацій.

6. Гнучкість розгортання – можливість використання стаціонарних, мобільних та супутникових рішень, що забезпечують покриття в будь-яких умовах, включаючи зони бойових дій та віддалені регіони.

Висновки до 1 розділу

У першому розділі дисертації проаналізовано сучасний стан і особливості функціонування мобільних мереж зв’язку спеціального призначення, а також досліджено технічні рішення, що використовуються в мережах стільникового зв’язку п’ятого покоління (5G). Проведено порівняльну характеристику традиційних технологій, таких як TETRA, P25, LTE для потреб урядового зв’язку, та виявлено їх ключові обмеження в умовах зростаючих вимог до швидкості, масштабованості, надійності та інформаційної безпеки.

Розглянуто основні функціональні та технічні вимоги до мереж 5G, зокрема підтримку широкосмугового доступу, критичного зв’язку з низькими затримками, високої щільності пристроїв, енергоефективності та адаптивного управління ресурсами. Проведено огляд перспективних технологій, включаючи Massive MIMO, beamforming, нумерологію, MEC, Cloud RAN, SDN/NFV, а також можливості інтеграції штучного інтелекту та машинного навчання для управління мережею.

У результаті зроблено висновок, що архітектура 5G забезпечує потужний інструментарій для створення високонадійних, захищених та масштабованих мереж зв’язку спеціального призначення. Подальші дослідження повинні бути спрямовані на адаптацію архітектурних рішень 5G до специфіки урядового та рятувального зв’язку, формалізацію вимог до якості обслуговування (QoS), резервування ресурсів і стійкості до надзвичайних ситуацій.

РОЗДІЛ 2
ФОРМУВАННЯ ВИМОГ ДО ПЕРСПЕКТИВНИХ МЕРЕЖ УРЯДОВОГО РАДІОЗВ'ЯЗКУ

2.1.1 Аналіз вимог до сучасних мереж урядового зв'язку

Для визначення підходів до побудови мережі урядового зв'язку було проаналізовано нормативно-правові акти, які регламентують створення та функціонування державних інформаційних систем. Одним із ключових документів є положення [30], згідно з якими такі системи мають забезпечувати облік, контроль, координацію діяльності органів державної влади, а також підвищення ефективності управлінських процесів.

Законодавство визначає, що інформаційні системи, які:

- обслуговують державні органи та створюються в межах їхньої компетенції;
- містять інформацію, отриману або надану внаслідок виконання державних функцій;
- фінансуються з державного бюджету або цільових фондів, вважаються державною власністю та підлягають управлінню з боку відповідного державного органу.

Окремо наголошується, що аналогічні вимоги застосовуються також до муніципальних систем, якщо не передбачено іншого на рівні спеціального законодавства.

Таким чином, при проєктуванні мережі урядового зв'язку необхідно дотримуватися наступних принципів:

- централізоване управління та контроль доступу;
- обов'язкове забезпечення захисту даних та безперервності функціонування;
- дотримання норм фінансування, відповідальності та прав власності на IT-інфраструктуру;

- відповідність меті – підтримка державного управління, публічних сервісів та звітності.

При розробці мережі урядового зв’язку особливу увагу слід приділяти нормам, що регулюють порядок створення, фінансування та експлуатації державних інформаційних систем.

Відповідно до національного законодавства [31], такі системи можуть бути ініційовані як на підставі закону, так і за рішенням уповноважених державних органів. У випадку фінансування за рахунок державного бюджету, витрати на створення і підтримку ІТ-систем мають відповідати нормам бюджетної класифікації та бути чітко прописаними в законодавчих документах, які регулюють розподіл бюджетних коштів.

Рішення про запуск інформаційної системи має обов’язково містити:

- опис типу та обсягу даних, які планується обробляти;
- джерела фінансування, процедури та строки створення системи;
- технічні вимоги до функціоналу, форматів зберігання, обміну та надання інформації;
- чітко визначені строки реалізації проєкту, а також відповідальних осіб.

Також підкреслюється, що реалізація подібних проєктів повинна відбуватись у межах загального порядку державних закупівель, регламентованого національним законодавством.

Після завершення етапу розробки система проходить прийняття в експлуатацію. Цей процес регулюється спеціальним положенням, розробленим її власником. Уряд, у свою чергу, має право встановлювати додаткові обов’язкові вимоги до таких процедур, особливо якщо йдеться про системи, що обробляють чутливу або спеціальну інформацію.

Ефективне функціонування державних інформаційних систем передбачає дотримання чітких нормативно встановлених вимог до форматів зберігання, передачі та обміну даними [32]. Відповідний орган виконавчої влади, відповідальний за політику у сфері інформаційних технологій, розробляє та

затверджує єдині форми представлення інформації, що мають використовуватись у державних ІТ-системах.

При проектуванні нових інформаційних платформ державного рівня обов’язковим є дотримання принципу сумісності з іншими існуючими державними системами. Це дозволяє забезпечити цілісну взаємодію між платформами без втрат інформації чи необхідності додаткових конвертацій даних.

Щодо технічних вимог, то все обладнання, задіяне у зберіганні, обробці або передачі даних у межах державних систем, повинно бути сертифікованим згідно з національними технічними регламентами. Це критично важливо для гарантування безпеки, стабільності та цілісності функціонування таких систем.

Крім того, технічне завдання на створення державної інформаційної системи має включати обов’язковий розділ щодо забезпечення інформаційної безпеки та захисту даних. Це стосується як проєктів, що виконуються за державними контрактами, так і розробок, що здійснюються внутрішніми ресурсами державних структур.

У процесі розробки, впровадження та експлуатації державних інформаційних систем особливе значення має правовий режим використання об’єктів інтелектуальної власності (ІВ).

Згідно з вимогами чинного законодавства [33], виключні права на об'єкти ІВ, які є частиною або використовуються у державних ІТ-системах, можуть належати як державі (власнику системи), так і іншим особам, відповідно до норм законодавства у сфері інтелектуальної власності.

У випадках, коли система потребує інтеграції об'єктів ІВ, власник ІТ-системи зобов'язаний заздалегідь отримати дозвіл від правовласника. Без такого дозволу використання відповідного об'єкта в державній системі вважається недопустимим, якщо інше не передбачено законом.

У разі, якщо власник об’єкта ІВ відмовляє в дозволі, а інтеграція цього об’єкта є критично необхідною, держава має право звернутися до суду з вимогою про надання примусової невиключної ліцензії. Такий запит має містити

обґрунтування, пропозиції щодо умов використання, розміру винагороди, способу та термінів оплати.

У випадку задоволення судового позову ліцензійні виплати не можуть бути нижчими за ринкову вартість аналогічних ліцензій. Оплата здійснюється з бюджетних коштів, передбачених на створення та підтримку відповідної державної інформаційної системи.

Забезпечення цілісності та надійності інформації у державних ІТ-системах є одним із ключових обов’язків їхніх власників. Саме вони несуть відповідальність за організацію зберігання даних, запобігання їх втраті, спотворенню або несанкціонованому доступу, а також мають гарантувати можливість відновлення інформації у випадку інцидентів.

Окремо законодавством [34] визначено обов’язок створення резервних копій для певних категорій державних інформаційних систем. Перелік таких систем формується на рівні уряду та охоплює ті, що мають критичне значення для державного управління, наукової, культурної, освітньої сфери, а також захисту прав громадян, юридичних осіб та функціонування органів влади.

При ухваленні рішення про включення конкретної системи до цього переліку уряд має встановити:

- періодичність створення резервних копій;
- уповноважену організацію, відповідальну за їх зберігання.

Такі організації зобов’язані дотримуватися тих самих вимог інформаційної безпеки, що застосовуються безпосередньо до державної системи, з якої створено копії. Це включає технічний та організаційний захист інформації, зберігання резервів у безпечному середовищі та контроль за доступом.

Подібний підхід до оцінки ефективності схем проєктування мобільних мереж детально обґрунтовано у [30], де запропоновано методику факторного аналізу для вибору оптимальних рішень з урахуванням багатокритеріальності та структурної складності.

Для формування вимог до перспективних мереж урядового зв’язку необхідно сформулювати групи абонентів, які будуть користуватися послугами; перелік

послуг для кожної групи абонентів та відповідно вимоги, які мають бути забезпечені мережею при наданні цих послуг.

Окрім технічних та правових аспектів, важливим елементом при створенні та експлуатації державних інформаційних систем є наявність механізмів постійного моніторингу та аудиту їх функціонування. Це передбачає як проведення регулярних технічних перевірок працездатності, так і незалежну оцінку дотримання нормативно-правових вимог, зокрема у сфері інформаційної безпеки, захисту персональних даних та відповідності стандартам взаємодії з іншими державними платформами. Такі аудити повинні виконуватись із визначеною періодичністю та фіксацією результатів у формі звітів, що надаються відповідним контролюючим органам. Це дозволяє забезпечити прозорість, відповідальність і підвищити довіру до державних ІТ-систем з боку громадян і партнерських організацій.

2.1.2. Розподіл на групи абонентів

У відповідності до діючих вимог, абонентів рухомого урядового радіозв’язку можна розділіти на наступні групи (табл. 2.1).

Таблиця 2.1.

Групи абонентів урядового радіозв’язку

№ з./п.	Назва групи абонентів	Скорочена назва	Орієнтовний перелік користувачів, що буде включений до групи
1	Група вищого рівня	ВР	Президент, Прем’єр-міністр, Віцепрем’єр-міністри, Міністри Кабінету Міністрів
2	Група першого рівня	Р1	Заступники Міністрів Кабінету Міністрів, Голови Обласних державних адміністрацій тощо
3	Група другого рівня	Р2	Начальник ДержНДІ, Керівництво Держспецзв’язку тощо

Розподіл абонентів урядового радіозв’язку на зазначені групи забезпечує ієрархічну структуру доступу до каналів зв’язку відповідно до рівня відповідальності та функціональних обов’язків посадових осіб. Такий підхід дозволяє оптимізувати маршрутизацію трафіку, гарантувати пріоритетне обслуговування критично важливих абонентів у надзвичайних ситуаціях, а також реалізувати гнучкі механізми управління навантаженням у межах обмеженого радіочастотного ресурсу.

2.1.3. Формування переліку послуг перспективних мереж урядового радіозв’язку

Для формування переліку послуг перспективних мереж урядового радіозв’язку спочатку проаналізуємо сервіси, які можуть надаватись в стільникових мережах різних поколінь.

На сьогоднішній день у сфері стільникового зв’язку відсутня уніфікована класифікація додаткових послуг, що надаються в мережах різних поколінь. Аналізуючи еволюцію мобільних технологій [35], можна зробити висновок про активний розвиток ринку value-added services (VAS) — послуг з доданою вартістю. Їх кількість постійно зростає, що створює необхідність у вдосконаленні системи класифікації.

Для ефективної розробки, просування та впровадження VAS-послуг важливо чітко визначати їх цілі, функціональне призначення та умови реалізації.

Умовно VAS-послуги можна розділити на дві основні категорії:

- Безкоштовні послуги, які зазвичай мають сервісну функцію, спрямовану на підвищення лояльності клієнтів, залучення нових користувачів або покращення досвіду існуючих абонентів;
- Платні послуги, які передбачають комерційний характер та генерують додатковий дохід для мобільного оператора [36].

Серед безкоштовних сервісів, що надаються мобільними операторами, виділяють послуги сервісного типу, які спрямовані на підвищення зручності

користування послугами зв’язку для нових і постійних абонентів. Їх можна умовно поділити на дві категорії:

1. Адміністративні послуги користувача

Ці сервіси дозволяють налаштовувати параметри послуг:

- Активація або відключення доступних сервісів.
- Редагування особистого профілю користувача.
- Керування груповими підключеннями.
- Вибір режиму дзвінків — індивідуального чи колективного.
- Встановлення рівнів пріоритету для доступу до мережевих ресурсів.

2. Інформаційно-індикативні послуги

Спрямовані на надання оперативної інформації:

- Перевірка балансу та залишку доступного трафіку.
- Автоматичні сповіщення про події в системі.
- Інформування про технічні оновлення або аварійні ситуації.
- Базова геолокація для окремих підрозділів або пристроїв.

Платні VAS-послуги технологічного спрямування

До категорії комерційних послуг входять рішення, які базуються на новітніх IT-технологіях і призначені, передусім, для підприємств, органів безпеки та спеціалізованих структур:

- **MCVideo** — передача відео в реальному часі з камер спостереження.
- **MCData** — обмін файлами, картографічними даними, інформацією з датчиків.
- **Системи шифрування** — забезпечення захисту трафіку через спеціалізоване ПЗ.
- **Диспетчерські рішення** — управління об'єктами або підрозділами через мобільні додатки.
- **Підключення до SCADA/IoT** — для моніторингу критичної інфраструктури.
- **Інтелектуальний аналіз відео** — використання ШІ для ідентифікації об’єктів.

- **Інтеграція з безпілотними літальними апаратами (БПЛА)** — відеотрансляція з дронів у реальному часі.
- **Підтримка QoS (QCI)** — для забезпечення стабільного каналу зв'язку для служб з підвищеними вимогами до якості.

До категорії додаткових сервісів мобільного зв'язку важливо віднести послуги міжнародного характеру, які дозволяють користувачам залишатися на зв'язку за межами своєї країни. До таких послуг належать, зокрема:

- **міжнародний роумінг**, що забезпечує доступ до дзвінків, мобільного Інтернету та SMS у зарубіжних мобільних мережах;
- **відправлення міжнародних SMS**, що дає змогу підтримувати комунікацію між абонентами різних країн.

Окрему категорію становлять **контент-послуги**, які формують важливу частину сучасної мобільної екосистеми. З метою впорядкування їх можна розділити на три основні підгрупи:

1. **Корпоративні сервіси** — орієнтовані на юридичних осіб, підприємства та організації. Вони призначені для групового використання і включають можливості спільного управління зв'язком, контроль витрат, формування віртуальних мереж всередині компанії тощо.
2. **Інформаційні сервіси** — забезпечують доступ до актуальних новин, прогнозу погоди, економічних показників, подій тощо.
3. **Розважальні сервіси** — охоплюють широкий спектр медіа- ігор, аудіо- та відеоконтенту, інтерактивних підписок, персоналізації сигналів виклику тощо.

Розподіл додаткових послуг мобільного зв'язку (VAS) за критеріями доступності (всередині країни чи за кордоном) та за функціональним призначенням (бізнес, інформація, розваги) дозволяє більш чітко систематизувати їх використання у сучасній телекомунікаційній екосистемі. Така структуризація допомагає операторам формувати точні пропозиції для цільових аудиторій, а споживачам — отримувати релевантні сервіси.

Серед послуг, що орієнтовані на корпоративних клієнтів, варто відзначити:

- **Груповий доступ до мобільного інтернету (Group APN/QCI)** — забезпечення пріоритетного каналу зв’язку для усіх пристроїв організації.
- **Корпоративні VPN-мережі** — створення захищеного з’єднання для доступу до внутрішньої інфраструктури компанії через мобільну мережу.
- **Мобільні платформи для керування персоналом** — можливість надсилання завдань, контролю виконання та геолокаційного моніторингу співробітників у режимі реального часу.
- **Зашифрований внутрішній зв’язок** — використання технологій для безпечного голосового та відеозв’язку в межах корпоративної мережі.
- **Інтеграція з бізнес-системами (CRM/ERP)** — функціональність для автоматизованих дзвінків чи сповіщень безпосередньо з інформаційних систем компанії.
- **Централізований запис комунікацій** — зберігання дзвінків або повідомлень у логістичних, безпекових або диспетчерських підрозділах.
- **Контроль переміщення співробітників (геозони)** — визначення місцезнаходження працівників з метою підвищення ефективності роботи на виїзді.
- **Push-оповіщення для внутрішньої комунікації** — оперативне інформування співробітників про важливі події або завдання.
- **Підвищений пріоритет доступу до мережі (QoS)** — забезпечення стабільного з’єднання навіть у моменти високого навантаження на мережу, що критично для службових задач.

Серед додаткових сервісів мобільних операторів важливе місце займають новини та розваги, які реалізуються за допомогою мультимедійних платформ. Ці послуги базуються на спеціалізованих програмно-апаратних рішеннях, що забезпечують доступ до контенту через сучасні технології передачі даних (GPRS/EDGE/3G/4G/5G).

Серед основних послуг цієї категорії можна виокремити:

- **Зображення для мобільного пристрою** – завантаження фонів, графіки, анімаційних зображень та екранних заставок.

- **Аудіоконтент** – рінгтони, уривки музичних творів, можливість інтеграції з музичними сервісами чи бібліотеками користувача.
- **Відеоматеріали** – перегляд або збереження відео у форматах, сумісних із мобільними платформами (наприклад, MP4, 3GP).
- **Мобільні ігри** – завантаження і запуск ігор на Java, HTML5, Android або iOS, що спрямовані на дозвілля або тренування реакції.
- **Інформаційні SMS-сервіси** – надсилання коротких текстових повідомлень із погодними даними, щоденними новинами, астрологічними прогнозами тощо.
- **Відео за запитом (VoD)** – користувач отримує можливість обирати та переглядати фільми, шоу чи архівні записи у зручний час.
- **Мобільне телебачення** – трансляція телеканалів онлайн у реальному часі без необхідності підключення до телевізора.
- **Інтерактивні платформи** – участь у різноманітних опитуваннях, конкурсах, телевізійних шоу або проєктах соціального спрямування через мобільний додаток.

Окремою групою послуг є захист в стільникових мережах, ця група слугує для безпечної передачі даних в мобільних мережах, та збереження конфіденційності. Зараз ці послуги не розвинені, однак в майбутньому вони будуть грати одну з провідних ролей.

Також виділено було групу фінансових послуг, які починають набирати популярності останнім часом. Оператори намагаються створювати сервіси, які би дозволяли акумулювати все життя, в тому числі й фінансове, у смартфоні.

У підсумку було розроблено оновлену та вдосконалену систему класифікації сервісів, що використовуються в урядовому зв’язку, з урахуванням сучасних технологічних вимог і функціонального призначення (Рис. 2.1).

Ще однією перспективною групою послуг, що формується в рамках урядового зв’язку, є аналітичні та ситуаційно-орієнтовані сервіси, які забезпечують збір, обробку та візуалізацію інформації в режимі реального часу для потреб управління, безпеки та реагування на надзвичайні ситуації. Такі сервіси базуються

на інтеграції з геоінформаційними системами, системами моніторингу, штучного інтелекту та прогнозування ризиків. Їхнє впровадження дозволяє органам державної влади приймати обґрунтовані рішення в умовах обмеженого часу, підвищуючи ефективність державного управління та оперативного реагування.

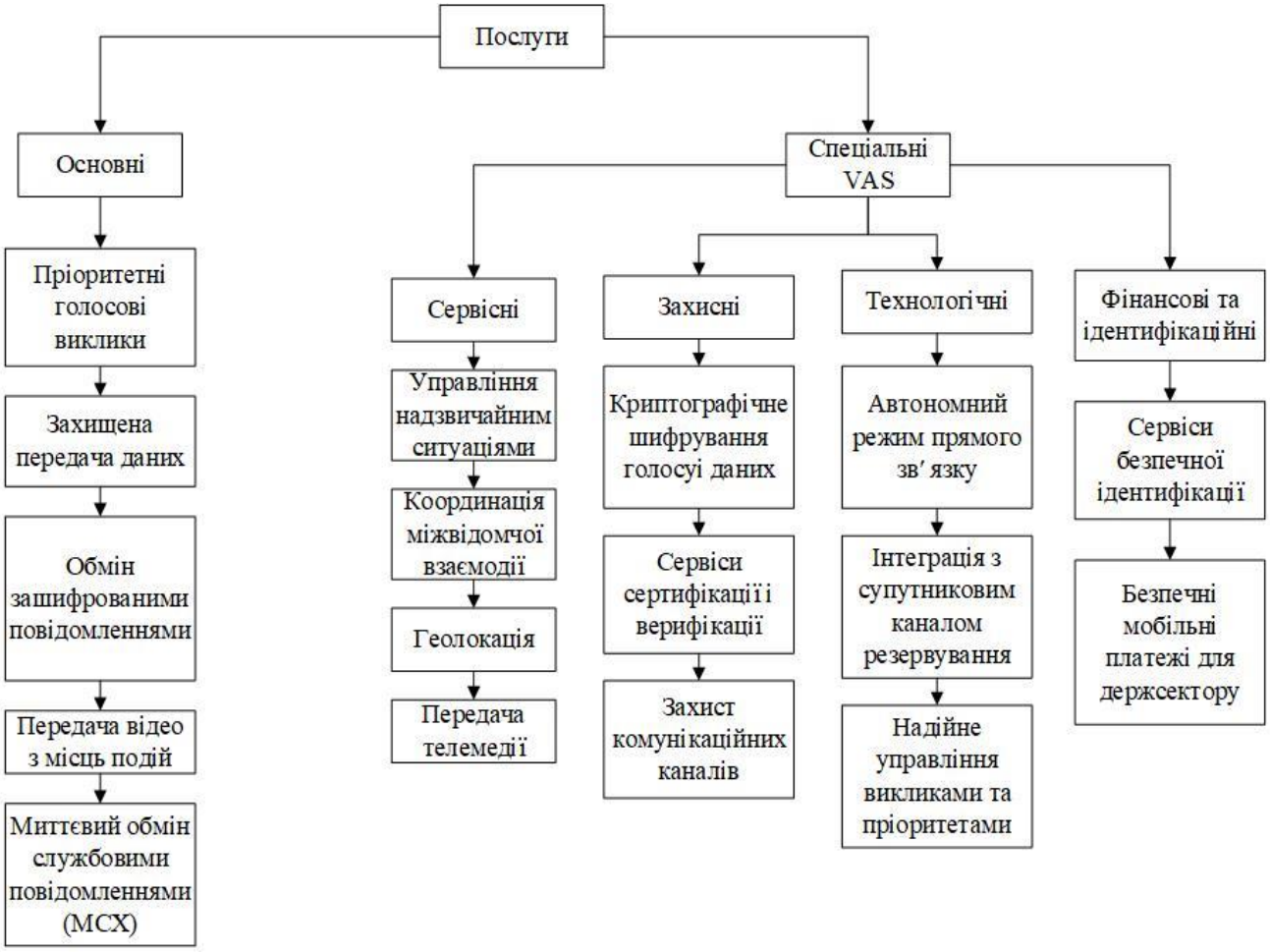

Рис. 2.1. Структурована модель класифікації послуг урядового зв'язку

На основі цієї вище наведеної класифікації послуг сучасних мереж урядового зв'язку, можна сформулювати перелік основних послуг мереж урядового радіозв'язку:

- Голосовий зв'язок;
- Відеозв'язок;
- Відеоконференцзв'язок;
- Сервіси передачі даних;
- Мобільний доступ до сервісів мережі Інтернет;

- Перспективні застосунки.

2.1.4. Вимоги до перспективних мереж урядового радіозв’язку

На основі наведеного переліку ключових послуг перспективних систем урядового радіозв’язку, можливо окреслити відповідні граничні параметри якості обслуговування, необхідні для забезпечення належного функціонування кожного із сервісів. (табл. 2.2).

Таблиця 2.2

Вимоги до мереж урядового радіозв’язку

№ п/п	Опис вимог	Метрики	Значення
1	Швидкість передавання даних (канал downlink)	Необхідно забезпечити пікову швидкість прийому даних	1 Гбіт/с
2	Швидкість передавання даних (канал uplink)	Необхідно забезпечити пікову швидкість передачі даних	100 Мбіт/с
3	Затримка	Необхідно забезпечити мінімальну затримку	5 мс
4	Мобільність	Необхідно забезпечити неперервне з’єднання як статичного об’єкту, так і рухомого (наприклад, у швидкісному потязі або гелікоптері)	600 км/год
5	Інформація про місцезнаходження	Необхідно найточніше визначення місцезнаходження абонента	Точність – до 1 м
6	Безпека/конфіденційність	Необхідно забезпечити високий рівень безпеки та	Конфіденційність – 100%

		конфіденційності абонентів оскільки інформація, яка передається є секретною і потребує особливого захисту	Цілісність – 100%
7	Надійність/доступність	Необхідно забезпечити надійне з'єднання, шифрування даних, оскільки інформація, яка передається є секретною і потребує особливого захисту	99,999%

При цьому із врахуванням класифікації із підрозділу 2.2.1, запишемо групи послуг та конкретні вимоги для кожної групи абонентів (табл. 2.3).

Таблиця 2.3

Вимоги до якості обслуговування різних груп абонентів урядового радіозв'язку на базі 5G

Вимога	**Група абонентів**		
	ВР	Р1	Р2
Швидкість передавання даних (канал downlink)	1 Гбіт/с	1 Гбіт/с	1 Гбіт/с
Швидкість передавання даних (канал uplink)	100 Мбіт/с	100 Мбіт/с	100 Мбіт/с
Затримка	До 50 мс	До 50 мс	До 50 мс
Мобільність	До 600 км/год	До 200 км/год	До 200 км/год
Безпека/конфіденційність	100%	100%	100%
Надійність	99,999%	99,999%	99,9%
Доступність	100%	100%	95%

Вимоги до самої перспективної мережі урядового рухомого радіозв’язку можна сформулювати наступним чином:

1. Призначення мережі: надання послуг телефонного зв’язку, відеозв’язку, аудіо- та відеоконференцій, електронної пошти, передачі даних, доступу до мережі Інтернет рухомим абонентам спеціальних гуп користувачів.

2. Кількість абонентів мережі: не менше 5000.

3. Кількість абонентів міської мережі у м. Київ: не менше 2000.

4. Кількість абонентів в одній мережі міського зв’язку в обласному центрі України: не менше 100.

5. Види з’єднань у мережі:

- автоматичних телефонних/відеотелефонних з’єднань між собою;
- телефонних/відеотелефонних з’єднань абонентів через оператора;
- телефонних/відеотелефонних конференцій;
- передачі даних;
- безпечного доступу до ресурсів мережі Інтернет.

6. Кількість одночасних конференцій: до 100

7. Кількість одночасних учасників конференцій: від 5 до 100.

Висновки

1. Було проаналізовано існуючі вимоги до мереж урядового радіозв’язку.

2. Для формування вимог до перспективних мереж урядового зв’язку були сформовані групи абонентів, які будуть користуватися послугами; перелік послуг для кожної групи абонентів та відповідно вимоги, які мають бути забезпечені мережею при наданні цих послуг.

3. Було проведено уточнення узагальненої класифікації послуг зв’язку, які можуть надаватись операторами стільникового зв’язку. Зокрема, були визначені та додані нові послуги, які можуть надаватись в стільникових мережах 5-го покоління. На основі цієї узагальненої класифікації були обрані послуги, які плануються до використання у перспективних мережах урядового радіозв’язку.

4. Для обраних послуг, які плануються до використання у перспективних мережах урядового радіозв’язку було визначено основні вимоги по якості обслуговування.

5. Для всієї мережі урядового радіозв’язку були також сформовані основні вимоги по призначенню, кількості абонентів, видам з’єднань, кількості сесій тощо.

Розробка особливої системи стільникового зв’язку передбачає формування організаційно-технічних рішень, що забезпечать захищений, надійний та стійкий мобільний зв’язок для потреб військових, державних органів, критичної інфраструктури тощо.

2.2.1 Модульна архітектура

Модульна архітектура (Рис. 2.2.) передбачає розподіл системи на незалежні функціональні блоки, що в свою чергу дозволяє:

- локалізувати вплив потенційних атак – компрометація одного модуля не впливає на всю систему;

- гнучко масштабувати мережу відповідно до поточних потреб, забезпечуючи швидке розгортання нових вузлів;

- розділяти зони доступу за рівнем критичності – від загальнодоступного державного зв’язку до спеціальних каналів для спеціальних комунікацій (наприклад для зв’язку з БПЛА).

Кожен модуль в ідеальних умовах має включати:

1) ядро мережі (Core Network);

2) радіомережу (RAN – Radio Access Network);

3) безпековий сегмент (Security Zone) – модулі кібербезпеки, криптографічного захисту та аутентифікації;

4) Модуль управління (Network Management & Monitoring).

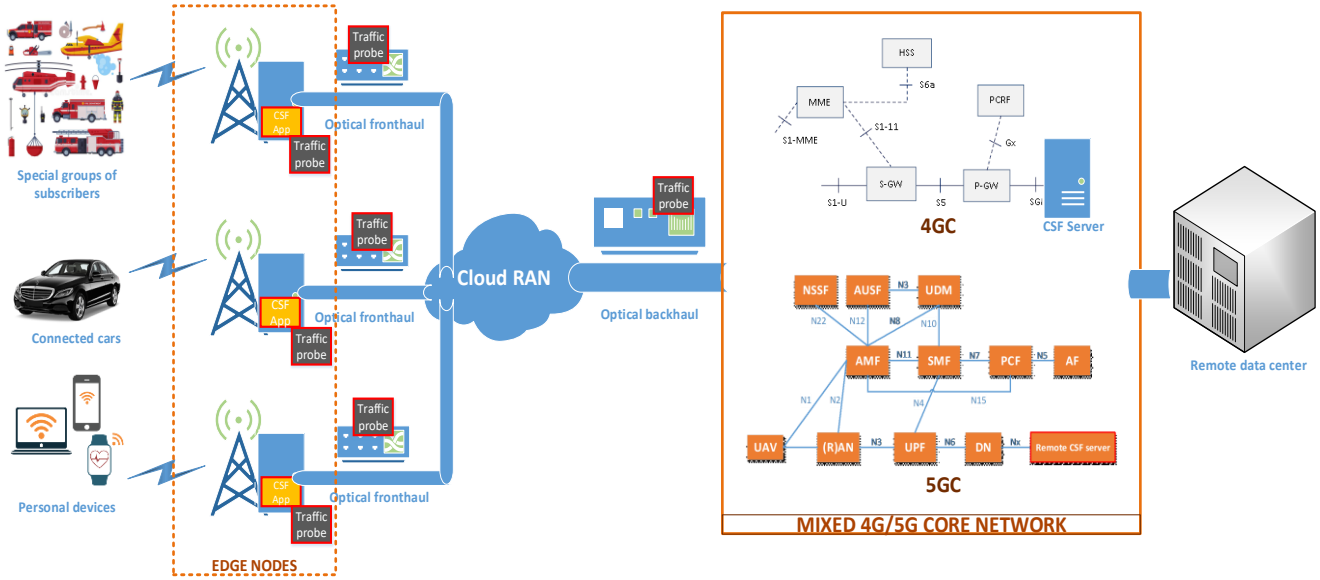

Рис. 2.2. Модуль архітектура стільникової мережі

Такий підхід відповідає міжнародним стратегічним підходам до побудови безпечних 5G-мереж, зокрема відображеним у національній стратегії уряду США [37], а також рекомендаціях CISA та NSA щодо реалізації Network Slicing у критичних комунікаціях [38].

2.2.2. Сегментація мережі та автономні зони зв’язку

Сегментація мережі дозволяє розподілити трафік між захищеними автономними зонами зв’язку залежно від рівня критичності даних.

Основні сегменти можуть включати:

1) Національний сегмент – захищена центральна інфраструктура для комунікацій державних органів, що інтегрується з іншими державними комунікаційними платформами.

2) Військовий сегмент– виділена частина мережі для забезпечення безпечного зв’язку між військовими формуваннями та керівництвом, а також для зв’з безпілотними літальними апаратами.

3) Сегмент критичної інфраструктури – спеціалізована мережа для забезпечення моніторингу стану та інших потреб критичної інфраструктури держави.

Схожі підходи застосовуються у моделях приватних 5G-мереж для оборонного сектору США, де автономність та логічна ізоляція є ключовими характеристиками [39].

Слід відзначити, що в залежності від зовнішніх умов, державної політики, військової обстановки, можливим є створення й інших логічних сегментів, що матимуть свої особливості використання для окремих груп користувачів.

2.2.3. Можливість інтеграції з державними та військовими комунікаційними платформами

Оскільки ССЗ Держспецзв'язку має працювати у взаємодії з існуючими урядовими та військовими системами зв'язку, то необхідно передбачити:

1) Сумісність з безпековими стандартами ЄС та НАТО, що дозволить в майбутньому ефективно взаємодіяти з міжнародними партнерами.

2) Підтримка протоколів міжмережевої взаємодії, що забезпечить з'єднання з уже наявними захищеними мережами зв'язку.

3) Інтеграція з національними системами кіберзахисту для виявлення та запобігання кібератакам у режимі реального часу.

4) Використання захищених каналів передачі даних (VPN) для обміну інформацією між державними та військовими структурами.

2.2.4 Розробка канальної системи супутникового зв'язку для медіадоставки

Розроблена модель супутникової канальної системи[40] забезпечує високу ефективність, адаптивність до умов мобільності, масштабованість і підтримку критичних сервісів у рамках архітектури 5G/6G.

Запропонована агрегативна математична модель враховує сотні можливих варіантів побудови системи зв’язку. Вперше було застосовано булеву цільову функцію, яка враховує відповідність кожного параметра технічному завданню. Якщо хоча б один з них не відповідає вимогам, система вважається непридатною. Такий підхід дозволяє ефективно фільтрувати конфігурації й визначати найкращі з точки зору відповідності ТЗ та параметричної надійності.

Оцінка пропускної здатності супутникових каналів здійснюється шляхом аналізу спектру відеосигналів і врахування параметрів компресії. Було розраховано необхідну смугу частот для різних конфігурацій системи, що дозволило адаптувати технічні параметри до реальних сценаріїв.

Авторською групою сформовано архітектуру, що базується на чотирьох центрах управління зв’язком (ЦУЗ), кожен з яких обслуговує окремі категорії абонентів: залізничні експреси, окремі вагони, автомобілі та бойові безпілотники. Передача здійснюється через супутникові канали з використанням різних схем модуляції, стиснення (MPEG-2/4) та корекції помилок (FEC).

Розглядається концепція побудови ефективної канальної системи супутникового мобільного зв’язку, призначеної для доставки медіаконтенту з високою роздільною здатністю в умовах функціонування мереж п’ятого та шостого поколінь (5G/6G). Запропоновані рішення орієнтовані на підтримку гарантованої якості сервісу (QoS) для динамічних користувачів – пасажирів швидкісного транспорту та безпілотних літальних апаратів.

2.2.5 Алгоритми локалізації та математичні моделі в бездротових сенсорних мережах

Розглядаються сучасні підходи до локалізації вузлів у бездротових сенсорних мережах (WSN), які є важливими компонентами мобільних систем спеціального призначення. Забезпечення точного визначення місцезнаходження сенсорних вузлів відіграє ключову роль у побудові надійної інфраструктури,

ефективній маршрутизації даних, моніторингу критичних об’єктів та оперативному реагуванні на зміни в мережевому середовищі.

У роботі [41] проаналізовано та систематизовано основні алгоритми локалізації, які поділяються на категорії залежно від методів вимірювання параметрів сигналу. Серед найпоширеніших — алгоритми, що базуються на потужності отриманого сигналу, часі його прибуття або різниці часових затримок. Кожен із цих методів має свої переваги та обмеження, які визначаються умовами застосування, наявністю шумів, вимогами до точності та енергоспоживання.

З метою підвищення точності локалізації в умовах багатошляхових завад і нестабільності сигналу дослідники використовують комбіновані та евристичні алгоритми, зокрема алгоритм DV-Hop, метод штучної бджолиної колонії (ABC), багатовимірне шкалювання (MDS-MAP), а також фільтри згладжування та оцінювання стану, включаючи фільтр Калмана. Ці підходи дозволяють адаптувати локалізаційні алгоритми до складних динамічних умов, характерних для мереж екстреного зв’язку, військових операцій або рухомих платформ.

Таким чином, застосування математичних моделей і алгоритмів локалізації дозволяє створювати адаптивні та масштабовані бездротові сенсорні мережі, здатні працювати в умовах обмежених ресурсів та нестабільного інформаційного середовища, що є важливою передумовою для формування сучасної архітектури мереж 5G/6G спеціального призначення.

2.2.6 Математичне моделювання маршрутизації в бездротових мережах IoT із високою щільністю пристроїв

У сучасних бездротових мережах зв’язку, особливо в сегменті Інтернету речей (IoT), актуальним є завдання побудови ефективних маршрутів передачі даних в умовах високої щільності розміщення пристроїв. Така ситуація характерна, наприклад, для сенсорних мереж у промисловості, систем відеоспостереження або міських інфраструктур.

У роботі [42] запропоновано підхід до моделювання мережі IoT як просторового точкового процесу, в межах якого розглядаються такі параметри, як щільність розташування вузлів, типи просторових процесів (однорідні, неоднорідні, кластеризовані або регулярні), а також вплив цих характеристик на якість зв'язку. Автори акцентують увагу на необхідності врахування випадкових розташувань мережевих елементів у просторі, що дозволяє достовірно моделювати реальні умови функціонування мережі.

Особливу увагу приділено оптимізації кількості транзитних вузлів маршруту. З одного боку, збільшення кількості таких вузлів дозволяє зменшити відстань між передавачами, що знижує загасання сигналу та покращує співвідношення сигнал/шум. З іншого боку, кожен додатковий вузол створює додаткову затримку та споживає ресурси. Це вимагає визначення оптимального балансу між кількістю вузлів та якісними параметрами маршруту.

Методологія, викладена в дослідженні, передбачає використання просторових процесів Пуассона (у тому числі кластеризованих), процесів Кокса, Матерна та Гіббса. Ці моделі застосовуються для різних сценаріїв – від рівномірного до агрегаційного розподілу вузлів, дозволяючи адаптувати архітектуру маршруту під специфіку середовища.

Результати моделювання показують, що за умови застосування правильного методу відбору транзитних вузлів і врахування просторових характеристик мережі можна досягти приросту ефективності передачі даних більш ніж на 30%, порівняно з традиційними підходами. Такі підходи можуть бути безпосередньо адаптовані для проєктування архітектури мобільних мереж спеціального призначення, зокрема у випадках критично важливого зв'язку.

2.2.7 Розпізнавання цифрових модуляцій у мережах 5G із використанням нейронних мереж

У статті [43] розглянуто застосування штучних нейронних мереж для задачі автоматичного розпізнавання типів цифрової модуляції в мережах 5G. Такий підхід є критично важливим для забезпечення коректної обробки сигналів, особливо в

умовах складного радіооточення, де традиційні методи можуть бути неефективними.

Модель була протестована на великій вибірці сигналів із різними типами модуляції (наприклад, QPSK, QAM, FSK тощо) за умов фіксованого відношення сигнал/шум (SNR = 5 dB). Результати показали, що при використанні трьох прихованих шарів перцептрон досягає точності розпізнавання до 99%.

Значну увагу приділено вибору інформативних ознак — використання високих порядків кумулянтів дозволяє ідентифікувати тип модуляції навіть у складних ситуаціях, таких як невизначені вхідні параметри або нестабільне середовище передачі.

Методика, представлена в [44], демонструє перспективність використання нейронних мереж для інтелектуального аналізу сигналів у мобільних мережах нового покоління, зокрема у сфері безпечного зв’язку, критичних комунікацій та розпізнавання загроз у реальному часі.

2.2.8 Використання сучасних стандартів мобільного зв’язку

Розбудова системи стільникового зв’язку Держспецзв’язку базується на використанні передових 4G технологій із перспективою розвитку до 5G. Цей підхід дозволить забезпечити надійний, швидкий та захищений мобільний зв’язок для державних органів, військових, екстрених служб та критичної інфраструктури.

Використання 5G як основи для побудови ССЗ дозволяє:

- Забезпечити надійний голосовий зв’язок, відеоконференції, передачу мультимедійного контенту;

- Підтримувати високошвидкісну передачу даних із низькими затримками, що є критичним для захищеного зв’язку;

- Інтегрувати захищені VPN-тунелі та шифрування на рівні мережі, що відповідає вимогам державних та військових структур;

- Реалізувати пріоритезацію трафіку для екстрених служб та критичних комунікацій;

- Використовувати малопотужні пристрої зв’язку для підключення IoT-систем, які можуть застосовуватись у військовій сфері, спостереженні та управлінні інфраструктурою.

Для підтримки закритої, автономної інфраструктури зв’язку ССЗ передбачається розгортання приватних мобільних мереж Private 5G.

2.2.9 Захист інформації у мобільних мережах

Захист інформації у мобільних мережах має відповідати найвищим вимогам безпеки, враховуючи ризики кібератак, електронного перехоплення та несанкціонованого доступу.

Сучасні дослідження також пропонують реалізацію інфраструктури відкритих ключів (PKI) у сервісно-орієнтованій архітектурі 5G для захисту критичних комунікацій [45].

Тому, з метою забезпечення конфіденційності, цілісності та автентифікації користувачів у системі стільникового зв’язку Держспецзв’язку (ССЗ) передбачається інтеграція національних криптографічних стандартів.

При цьому, основними принципи криптографічного захисту, яких треба дотримуватись, є наступні:

1) Шифрування трафіку та сигналізації

- Використання шифрування з кінця-в-кінець (E2E) для голосових дзвінків, SMS, відеозв’язку та переданих даних.

- Реалізація квантово-стійкого шифрування (PQC – Post-Quantum Cryptography) для захисту від майбутніх загроз з боку квантових обчислень.

- Впровадження криптографічного захисту на рівні мережевої інфраструктури, включаючи VPN-тунелі, IPsec та SSL/TLS протоколи.

2) Цілісність даних та захист від модифікації

- Використання криптографічних хеш-функцій для гарантування незмінності переданої інформації.

- Захист даних, які зберігаються (Data at Rest) та передаються (Data in Transit) через цифрові підписи та сертифіковані механізми аутентифікації.

3) Автентифікація користувачів та пристроїв

- Використання двофакторної (2FA) та багатофакторної автентифікації (MFA) для доступу до захищених мереж.

- Інтеграція PKI (Public Key Infrastructure) та цифрових сертифікатів (X.509) для автентифікації пристроїв і користувачів у мережі.

- Впровадження SIM-карт із захищеними криптографічними модулями (eUICC, HSM) для гарантування ідентифікації користувачів у закритих державних мережах.

2.2.10 Резервування та стійкість до атак

Забезпечення стійкості системи стільникового зв'язку Держспецзв'язку (ССЗ) є критично важливим завданням, оскільки мобільні комунікації можуть бути об'єктами кібератак, електронного впливу та фізичних атак на інфраструктуру. Для цього передбачається розробка автономних резервних каналів зв'язку, які забезпечуватимуть бездротову, супутникову та альтернативну передачу даних у кризових ситуаціях.

Основними загрозами для стільникового зв'язку наразі є наступні:

- Кібератаки – злам інфраструктури, атаки DDoS, злам криптографічних алгоритмів, фальшиві базові станції, тощо.

- Електронні перешкоди – радіочастотні перешкоди (jamming), електромагнітні атаки (EMP) та глушіння сигналу.

- Фізичні пошкодження – знищення або виведення з ладу базових станцій, серверів обробки даних, кабельних комунікацій (волоконно-оптичних та дротових).

- Відмова апаратного забезпечення – вихід з ладу обладнання через перевантаження, кібератаки або технічні несправності.

Типові випадки впливу (атак) зловмисників відображені на рис. 2.3.

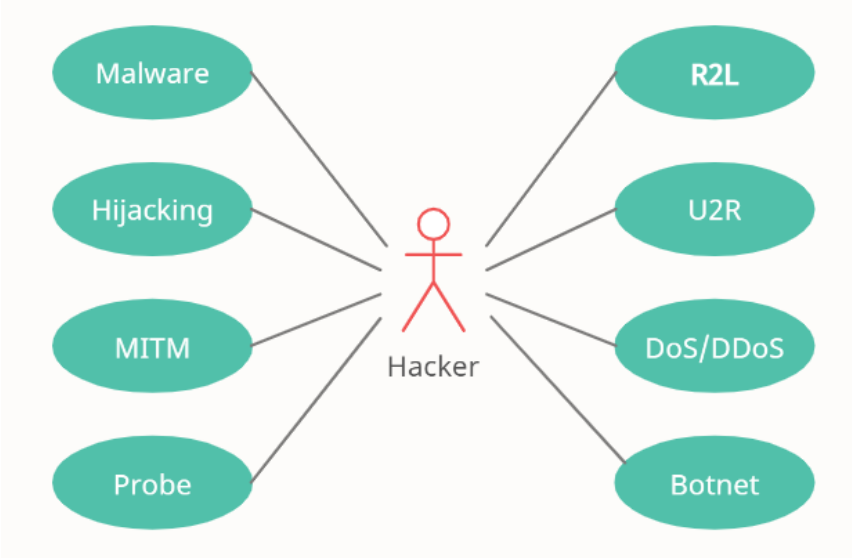

Рис. 2.3. Типові випадки впливу зловмисників

Щоб гарантувати надійну роботу мережі в умовах загроз, необхідно передбачити мультиканальне резервування зв'язку.

У складі ССЗ доцільно розгорнути багаторівневу систему резервних каналів, що включатиме:

1) Альтернативні наземні резервні канали

- Приватні LTE/5G мережі (Private Networks) – розгортання автономних базових станцій у стратегічно важливих зонах.

- Мобільні станції зв'язку – розгортання мобільних вузлів на транспортних засобах, дронах, аеростатах або тимчасових базах.

- Підземна та захищена інфраструктура – використання волоконно-оптичних ліній зв'язку в бункерах, тунелях, метро.

2) Супутникові резервні канали

- Геостаціонарні (GEO) та низькоорбітальні (LEO) супутникові системи (OneWeb, Starlink, GovSat, Iridium Certus) для резервного зв'язку при знищенні наземних каналів.

3) Захищені VPN та шифровані тунелі

- IPsec VPN, TLS 1.3, WireGuard – тунелювання трафіку через захищені канали.

- Захист трафіку через квантово-стійке шифрування (PQC) для запобігання майбутнім квантовим атакам.

2.2.11. Інтеграція з системами екстреного зв’язку

Розбудова системи стільникового зв’язку Держспецзв’язку (ССЗ) передбачає глибоку інтеграцію з системами екстреного зв’язку, що забезпечить оперативну та ефективну міжвідомчу взаємодію між органами державної влади, військовими структурами, службами безпеки та екстреними службами в умовах надзвичайних ситуацій, кризового управління та оборони.

Реалізація подібних інтеграцій уже активно досліджується в рамках місієкритичних комунікацій у США та ЄС, із фокусом на URLLC та захищений мультиканальний обмін [46][47].

Інтеграція з системами екстреного зв’язку базується на наступних ключових принципах:

- Миттєвий та гарантований доступ до зв’язку навіть у разі перевантаження або відмови загальнодоступних мобільних мереж.

- Уніфікована платформа для міжвідомчої координації, що об’єднує державні органи, військові, поліцію, медичні служби, рятувальні підрозділи та служби цивільного захисту.

- Захищене та зашифроване з’єднання, що унеможливлює перехоплення або несанкціонований доступ до критично важливої інформації.

- Підтримка мультиканальної комунікації – голосовий зв’язок, відеозв’язок, текстові повідомлення, обмін даними, інтеграція з дронами та сенсорними мережами.

- Автоматичне переключення між каналами зв’язку у разі втрати основного підключення (5G → супутниковий зв’язок → захищені наземні мережі).

2.2.12 Удосконалення архітектури ядра мережі 5G для потреб урядового радіозв’язку

У статті [48] проведено аналіз архітектурних принципів побудови мереж 5G із позиції потреб підвищеної безпеки, зокрема в контексті організації урядового радіозв’язку. Автори акцентують увагу на тому, що можливості, які надає архітектура 5G — включаючи Network Slicing, віртуалізацію функцій мережі (VNF), хмарні обчислення та підтримку одночасного доступу до локальних і централізованих ресурсів — можуть бути ефективно адаптовані для потреб критично важливих комунікацій.

Особливу увагу приділено питанням реалізації захищеного інформаційного обміну між функціональними модулями, зокрема через використання додаткових функцій безпеки: RSF (функція надійної безпеки) та KSF (функція криптографічного захисту). Ці модулі інтегруються до ядра мережі та взаємодіють із функціями AUSF, UDM та іншими стандартними компонентами для забезпечення двофакторної аутентифікації, розподілу ключів шифрування та контролю доступу до сервісів.

Завдяки гнучкості 5G-архітектури, передбачено можливість створення окремих ізольованих шарів (Network Slices) для обслуговування урядових абонентів, що дозволяє підвищити рівень конфіденційності, уникнути витоку критичних даних, а також забезпечити спеціальні параметри якості обслуговування (QoS). Запропоновано також механізм персоналізованої маршрутизації трафіку та логічної сегментації підмереж в залежності від категорій користувачів.

Розроблена в [45] архітектура передбачає інтеграцію механізмів захищеного підключення, реєстрації, автентифікації та управління сесією у рамках єдиної процедури встановлення сеансу урядового зв’язку. Важливо, що запропоновані рішення передбачають сумісність із наявними мережами 4G/5G і можливість використання малих осередків для точкового покриття ключових об’єктів, наприклад, адміністративних установ.

2.2.13 Системи виявлення подій у мобільних мережах спеціального призначення

У сучасних системах безпеки, а також у концепції Інтернету речей, усе ширше застосовуються бездротові сенсорні мережі для виявлення порушень, проникнень і змін у середовищі. У роботі [48] запропоновано методологію побудови сенсорного пристрою, здатного визначати проникнення в контрольовану зону за допомогою комбінації інфрачервоних і ультразвукових датчиків.

Значну увагу приділено забезпеченню автономності функціонування пристроїв, зокрема енергетичній незалежності сенсорів. Розглянуто підходи до зменшення залежності від батарейного живлення за рахунок використання новітніх технологій перетворення енергії, включаючи наногенератори, що використовують рух людини як джерело енергії.

Особливу роль в архітектурі сенсорних систем відіграють мікроконтролери, які виступають як ядра управління — приймають сигнали від різнорідних сенсорів, обробляють дані та передають результати користувачеві або у хмарну інфраструктуру. У запропонованій моделі пристрою [48] інформація від сенсорів надходить на мікроконтролер, де обробляється та передається по Wi-Fi каналу на інтерфейс управління. Пристрій підтримує зворотний зв’язок з користувачем, що дозволяє не тільки моніторити, але й керувати датчиками в реальному часі.

Систему побудовано на принципі паралельної роботи двох типів датчиків — інфрачервоного (для теплового випромінювання) та ультразвукового (для виявлення об'єктів, що не випромінюють тепло). Це дозволяє досягти більшої точності та знижує вірогідність хибних спрацювань.

2.2.14 Модель побудови терагерцової бездротової мережі з підтримкою RIS для систем 5G/6G

У роботі [44] запропоновано нову модель побудови бездротової мережі доступу 5G у терагерцовому діапазоні з використанням **реконфігурованих інтелектуальних поверхонь** (RIS — *Reconfigurable Intelligent Surfaces*), яка

покликана усунути проблеми блокування сигналів, підвищити надійність з’єднання та забезпечити мінімальні затримки при обслуговуванні користувачів.

Такі рішення вивчаються в рамках проєктів, орієнтованих на 6G та THz-зв’язок із підтримкою інтелектуальних поверхонь [49], а також в проектах Network Slicing для громадської безпеки [50]

Особливістю терагерцового діапазону є висока швидкість передачі даних при водночас підвищеній чутливості до перешкод та блокування прямої видимості між абонентом і базовою станцією. Для розв’язання цієї проблеми використовується **локальний цифровий кластер** із підтримкою RIS, який забезпечує кероване відбиття сигналів, перенаправлення променів та формування інтелектуального радіооточення.

Ключовою інновацією моделі є **використання розподіленого реєстру** (distributed ledger) для реалізації механізму **превентивної передачі сеансів** у разі прогнозованого блокування сигналу. На відміну від традиційних централізованих рішень, така структура дозволяє уникнути перевантаження обчислювальних ресурсів і скоротити час реакції при зміні топології обслуговування користувача.

У рамках запропонованої архітектури враховано просторове розміщення користувачів, характеристики середовища, типи затримок у системі, а також інтенсивність генерованого трафіку. Це дозволяє адаптивно налаштовувати параметри RIS та оптимізувати якість обслуговування (QoS) навіть у динамічних і завадних умовах.

Особливу увагу приділено питанням **використання штучного інтелекту** для прогнозування положення користувачів та конфігурації фазових зсувів елементів RIS. Автори аналізують підходи, що базуються на **глибинному навчанні (Deep Learning)**, включаючи алгоритми Actor-Critic для спільної оптимізації фазових матриць RIS та параметрів формування променів базових станцій. Хоча більшість досліджень поки обмежуються чисельним моделюванням, наголошено на необхідності переходу до експериментальної перевірки ефективності подібних систем.

2.2.15 Гнучкість розгортання системи стільникового зв’язку

Забезпечення гнучкості розгортання є ключовим фактором ефективності системи стільникового зв’язку, оскільки вона має функціонувати у віддалених регіонах, кризових зонах та в умовах бойових дій. Для цього передбачається використання стаціонарних, мобільних та супутникових рішень, що забезпечать гарантоване покриття, стійкість до атак та автономність.

Основні принципи гнучкого розгортання

- Швидке та ефективне розгортання в залежності від поточних потреб – як у міських умовах, так і в зонах зруйнованої інфраструктури.

- Адаптивність інфраструктури – використання різних типів базових станцій та терміналів, які можуть працювати незалежно або в складі загальної системи.

- Автономність – здатність системи працювати без підключення до центральних вузлів зв’язку в умовах відсутності електроживлення чи загальної інфраструктури.

- Стійкість до атак – забезпечення резервування каналів зв’язку, захист від фізичного знищення та кіберзагроз.

- Інтеграція різних технологій – використання стаціонарних, мобільних і супутникових компонентів, які можуть доповнювати один одного.

Виходячи з наявних принципів та потреб, основними стаціонарними рішеннями можуть бути базові станції 5G у стратегічних регіонах (урядові будівлі, військові бази, критична інфраструктура). Мобільною версією є спеціалізовані облаштовані транспортні засоби, які в собі поєднують базові станції, елементи живлення, антенні системи, комунікаційне обладнання. Їх перевагою може бути швидке розгортання в умовах бойових дій важко доступних місцях.

Для покращення якості зв’язку або збільшення території покриття можуть бути використані безпілотні літальні апарати (БПЛА, дрони-ретранслятори), або навіть Аеростати та повітряні платформи (HAPS – High-Altitude Pseudo-Satellites).

При цьому, обов’язково має бути забезпечена умова щодо автономності та безперебійності роботи мережі. Для цього, необхідно використовувати:

- Резервування живлення – автономні генератори, батареї великої ємності, сонячні панелі для довготривалої роботи в польових умовах.

- Функціонування у відключеному режимі – забезпечення роботи без підключення до центральних вузлів зв'язку.

- Інтелектуальне управління частотним ресурсом – захист від глушіння та електронних атак.

- Мультиканальне підключення – автоматичне перемикання між 5G, супутниковим зв'язком, mesh-мережами та іншими децентралізованими рішеннями.

2.3. Організаційно–технічні рішення щодо побудови та функціонування ССЗ

2.3.1. Вибір варіантів проєктного рішення

Доцільно здійснити вибір найкращого варіанту реалізації проєкту, спираючись на критерій оптимальності Байєса-Лапласа (BL-критерій) [51]. Як функцію для оцінки ефективності варіантів доцільно застосовувати показник чистої приведеної вартості (NPV), який відображає сукупний економічний ефект реалізації проєкту й дозволяє інтегрально оцінити доцільність інвестиційних рішень. Процес ухвалення інвестиційних рішень зазвичай здійснюється в умовах невизначеності, яка передбачає наявність ряду складових [52], зокрема:

1) множини $D(\underline{\underline{X}})$ альтернативних рішень у розпорядженні оператора (надалі – Оператор). Одне з них йому необхідно прийняти: $\underline{\underline{X}}_i \in D(\underline{\underline{X}})$, $i = 1,...,n$;

2) навколишнього середовища з безліччю взаємовиключних станів $Z_j \in D(\underline{\underline{Z}})$, $j=1,...,m$, але в якому конкретно стані знаходиться (або буде знаходитись) навколишнє середовище, Оператору не відомо. Під зовнішніми станами для Оператора будемо мати на увазі можливість розгортання мережі в певному частотному діапазоні та відповідно з використанням різного типу обладнання;

3) оціночної функції оптимальності E_{ij}, яка характеризує "виграш" Оператора під час вибору певного проектного рішення $\vec{X}_i \in D(\vec{x})$, якщо навколишнє середовище буде знаходитися (або знаходиться) у стані $Z_j \in D(\vec{Z})$ тобто конкретного значення оціночної функції оптимальності для проектного рішення X_i і стану навколишнього середовища Z_j. Ситуація прийняття інвестиційних рішень характеризується матрицею проектних рішень, яку представлено у табл. 1. Елементи матриці E_{ij} – оціночні функції оптимальності, які є кількісною оцінкою критерію оптимальності для проектного рішення $X_i \in D(\vec{X})$ за умови, що навколишнє середовище знаходиться у стані $Z_j \in D(\vec{Z})$.

Оціночною функцією оптимальності, яка є кількісною оцінкою критерію оптимальності, є ефект від реалізації проекту масштабування мережі.

Таблиця 2.4.

Матриця проектних рішень

Альтернатива $D(\vec{X})$	**Стан навколишнього середовища, який очікується в майбутньому $D(\vec{Z})$**				
	$\vec{Z}_1$	…	$\vec{Z}_j$	…	$\vec{Z}_m$
$\vec{X}_1$	E_{11}	…	E_{1j}	…	E_{1m}
…	…	…	…	…	…
$\vec{X}_i$	E_{i1}	…	E_{ij}	…	E_{im}
…	…	…	…	…	…
$\vec{X}_n$	E_{n1}	…	E_{nj}	…	E_{nm}

За критерієм Байеса-Лапласа, оптимальним рішенням $X^* \in D(\vec{X})$ вважають таке, для якого математичне очікування результуючої оціночної функції оптимальності досягає найбільшого можливого значення [49]:

$$E_{BL} = \max_{\vec{X} \in D(\vec{X})} E_{jr} = \max_{\vec{X} \in D(\vec{X})} \sum_{j=1}^{m} p_j \cdot E_{ij};$$

Множина оптимальних варіантів згідно з *BL*-критерієм визначають таким чином:

$$\vec{X}^{*} = \left\{ \vec{X}_i : \vec{X}_i \in D(\vec{X}) \wedge E_{BL} = \max_{\vec{X}_i \in D(\vec{X})} \sum_{j=1}^{m} p_j \cdot E_{ij} \right\};$$

Коли апріорні імовірності щодо стану середовища – рівноімовірні, BL-критерій обертається у критерій Бернуллі-Лапласа:

$$E_{BL} = \frac{1}{m} \cdot \max_{\vec{X}_i \in D(\vec{X})} \sum_{j=1}^{m} E_{ij}.$$

Тому для вибору оптимальних напрямків розвитку Оператору необхідно сформувати множину можливих проектних рішень, які будуть впроваджуватись *D(X)* та множину станів навколишнього середовища, який очікується в майбутньому *D(Z)*, до якої віднесемо, як приклад, можливі частотні діапазони для розгортання різних технологій на доступному радіочастотному спектрі (табл. 2). Слід відзначити, що значення чистого приведеного ефекту розраховано за домогою наданих експертних оцінок та до таблиці 2.5 вводиться в умовних одиницях. Як критерій оптимальності для першого інформаційного стану можна використати: мінімум дисперсії оціночної функції або максимум ентропії математичного очікування оціночної функції[53].

Таблиця 2.5.

Матрицю вибору проектного рішеня для стільникового оператора

Альтернативне рішення $D(\vec{X})$ (технологія стільникових мереж)	Розподіл імовірностей						Результуюча оціночна функція
	$P_q(0)$	$P_2(0)$	$P_3(0,25)$	$P_4(0,25)$	$P_5(0,25)$	$P_6(0,25)$	
	Стан навколишнього середовища $D(\vec{Z})$ (частотний діапазон, МГц)						$E_{BL} = \sum_{j=1}^{m} P_j \cdot E_{ij}$
	$\vec{Z}_1$	$\vec{Z}_2$	$\vec{Z}_3$	$\vec{Z}_4$	$\vec{Z}_5$	$\vec{Z}_6$	
	700	800	900	1800	2100	2600	
5G	3	3	0	3	0	2,7	1,425
E_{BL}=1,425							

2.3.2. Планування мережі 5G

Процес побудови та удосконалення стільникових мереж передбачає вирішення двох взаємопов'язаних завдань: попереднього та детального планування, а також подальшої оптимізації, яка базується на результатах практичного використання мережі. Ці процеси мають спільні етапи та обчислювальні підходи, а також характеризуються схожістю незалежно від стандарту мобільного зв'язку [54, 55].

Планування мережі передбачає проєктування її загальної структури, вибір оптимальних місць для встановлення елементів радіопідмережі, визначення географічного розташування та висоти антен базових станцій.

Оптимізація, у свою чергу, полягає в аналізі фактичних даних, отриманих під час перевірки відповідності планових рішень реальній роботі мережі, а також у вивченні результатів технічного моніторингу. Вона охоплює аналіз скарг користувачів, інформацію про збої та ремонти, оцінку ефективності роботи мережі за допомогою обраних критеріїв, а також налаштування параметрів з подальшим контролем результатів.

На відміну від планування, оптимізація здійснюється вже на основі розгорнутої інфраструктури, спирається на результати драйв-тестів і технічного аудиту в проблемних зонах, а її ключовими завданнями є підвищення ефективності використання ресурсів, зниження нерівномірності навантаження і покращення показників якості обслуговування.

Процес проєктування стільникової мережі (рис. 2.4) умовно поділяється на два основні етапи:

- **етап первинного (попереднього) планування** — включає загальну оцінку покриття, визначення кількості базових станцій та їх приблизного розташування;
- **етап детального планування** — передбачає точне визначення параметрів обладнання, висот установки антен, каналів зв'язку та налаштування радіомережі відповідно до заданих критеріїв якості.

Рис. 2.4. Ключові етапи процесу планування стільникової мережі зв'язку

2.3.3. Формування вибірки вхідних даних

Первинне планування мережі передбачає формування загальної стратегії її розвитку, що включає вибір критично важливих параметрів:

- **зони покриття** — визначення територій, які мають бути охоплені сигналом;
- **мережна ємність** — оцінка кількості користувачів і передбачуваного трафіку;
- **ключові індикатори ефективності (KPI)** — показники, які дозволяють оцінити функціонування мережі за якістю обслуговування.

У ході планування та подальшої оптимізації важливу роль відіграє **профіль якості обслуговування**, який може бути представлений у вигляді таблиці (наприклад, табл. 2.6).

Інформація, представлена у профілі якості обслуговування (наприклад, у таблиці 2.6), використовується як основа для початкового проєктування мережі, а також для подальшої її адаптації й удосконалення в процесі експлуатації.

Таблиця 2.6

Профіль якості обслуговування

Показник	Позначення	Одиниці виміру	Голосовий трафік	Відео (стримінг)	Дані (Інтернет, месенджери)
Затримка	N	мс	≤ 150	≤ 200	≤ 250
Варіація затримки (джитер)	J_N	мс	≤ 30	≤ 50	≤ 75
Швидкість передавання даних	C	кбіт/с або Мбіт/с	64–128 кбіт/с	2–10 Мбіт/с	512 кбіт/с – 5 Мбіт/с
Коефіцієнт втрати пакетів	IPLR	%	≤ 1	≤ 2	≤ 5
Допустимий ризик ІБ	R	-	Середній	Низький	Високий
Доступність сервісу	A_{svc}	%	≥ 99.9	≥ 99.99	≥ 99
Час встановлення з'єднання	T_{conn}	мс	≤ 100	≤ 200	≤ 500
Надійність передавання	R_{data}	%	≥ 99.9	≥ 99.99	≥ 98
Щільність трафіку	D_{traffic}	Мбіт/с·м²	≤ 0.1	до 10	до 1
Енергоефективність	EE	біт/Дж	≥ 10^4	≥ 10^3	≥ 10^3
Кількість підключень	N_{conn}	пристроїв/км²	≤ 1000	до 10 000	до 1 000 000 (IoT)
Захищеність даних	S_{sec}	рівень	Високий	Середній	Високий / Критичний

Для прийняття обґрунтованих рішень щодо оновлення телекомунікаційної інфраструктури важливо регулярно проводити аналіз характеристик і навантаження інформаційних потоків у мережі.

Нижче наведено основні **ключові індикатори ефективності (KPI)**, що є актуальними для оцінки продуктивності мереж п’ятого покоління (5G):

- Пікова швидкість передавання даних (Peak Data Rate) *До 20 Гбіт/с для завантаження (DL), до 10 Гбіт/с для вивантаження (UL).*

- Середня користувацька швидкість (User Experienced Data Rate) Не менше 100 Мбіт/с у звичайних умовах.
- Затримка (Latency) *До 1 мс для критичних* застосувань *(URLLC), до 4 мс для звичайного трафіку.*
- Щільність підключених пристроїв (Connection Density) *До 1 мільйона пристроїв на 1 км² (особливо актуально для IoT).*
- Надійність зв'язку (Reliability) ≥ *99.999% для місійно-критичних сервісів.*
- Мобільність (Mobility) *Підтримка до 500 км/год для рухомих об'єктів (поїзди, транспорт).*
- Пропускна здатність (Spectrum Efficiency) *У 3 рази вища, ніж у LTE-Advanced, приблизно 30 біт/Гц для DL.*
- Енергоефективність (Energy Efficiency) *У 100 разів вища порівняно з 4G: оптимізація споживання енергії при масових підключеннях.*
- Щільність трафіку (Traffic Density) *До 10 Мбіт/с на м², особливо в зонах підвищеного навантаження.*
- QoE (Quality of Experience) *Загальна задоволеність користувача якістю сервісу, яка враховує затримку, швидкість, стабільність з'єднання.*

На стадії початкового проєктування також проводиться оцінка загальної структури мережі та потенційного розташування компонентів системи радіодоступу. Визначається кількість базових станцій, необхідна для досягнення запланованого рівня покриття. Зазвичай для цього використовуються орієнтовні, теоретичні дані про параметри й технічні ресурси мережі, які пізніше уточнюються під час наступного етапу — **детального проєктування**.

На стадії детального планування виконуються такі завдання[56]:

Етап детального планування здійснюється після формування попередніх технічних рішень та вибірки вхідних даних і включає низку взаємопов'язаних дій, спрямованих на точне проектування топології мережі, конфігурацію обладнання та розрахунок основних параметрів.

На цьому етапі виконуються такі ключові завдання:

1. **Аналіз географічної місцевості та інфраструктури** – визначаються місця встановлення базових станцій з урахуванням зон покриття, рельєфу, наявних будівель, джерел електроживлення тощо.

2. **Побудова початкової топології мережі** – вибір типу мережі (радіальна, коміркова, mesh), визначення зон обслуговування та маршрутизації трафіку.

3. **Розрахунок зони покриття** – з використанням моделей радіопоширення, таких як COST-231 Hata, Okumura-Hata, WINNER II, 3GPP Urban Macro тощо.

4. **Формування карти розміщення обладнання** – планування розміщення базових станцій, контролерів, комутаційних вузлів, антенних систем, оптоволоконної мережі тощо.

5. **Частотне планування** – розподіл частотних ресурсів для уникнення міжканальних і внутрішньосистемних інтерференцій.

6. **Оцінка бюджету втрат у радіолінії** – на основі параметрів обладнання та розрахованих відстаней, згідно з формулою:

$$L_{max} = P_{tx} + G_{tx} - L_{body} + G_{rx} - L_{feeder} - I_{margin} - F_{margin} - S$$

7. **Прогнозування навантаження** – врахування кількості користувачів, трафіку, QoS-класів і потенційного росту навантаження.

8. **Оптимізація параметрів мережі** – з урахуванням KPI (швидкість, затримка, надійність, енергоефективність), резервування та масштабованості.

Вибір обладання для проектування мережі 5G. Для оцінки інвестиційної доцільності проєктів у сфері урядового зв’язку, особливо в умовах невизначеності, доцільно застосовувати критерій Байєса-Лапласа (BL-критерій) у поєднанні з методом чистої приведеної вартості (NPV). Ці підходи дозволяють обґрунтовано порівнювати альтернативні варіанти проєктів та вибирати оптимальний з них.

Критерій Байєса-Лапласа передбачає вибір рішення, яке має найвищу очікувану корисність, враховуючи всі можливі сценарії розвитку подій та їх ймовірності. Цей підхід особливо корисний, коли відсутні точні дані про

ймовірності, і всі сценарії вважаються рівноймовірними. У такому випадку обирається альтернатива з найвищим середнім виграшем.

Метод NPV дозволяє оцінити фінансову ефективність проєкту, враховуючи часову вартість грошей. Він розраховується як різниця між сумою дисконтованих грошових потоків (доходів) та початковими інвестиціями. Позитивне значення NPV свідчить про доцільність інвестування, тоді як негативне — про потенційні збитки.

Поєднання BL-критерію та NPV дозволяє врахувати як фінансові аспекти проєкту, так і невизначеність зовнішнього середовища. Цей підхід забезпечує більш обґрунтоване прийняття рішень, особливо в умовах обмежених ресурсів та високих ризиків.

Методика вибору проектного рішення описується наступною послідовністю дій [57]:

Пошук і систематизація готових рішень для побудови мережі 5G (табл. 2.7):

Таблиця 2.7.

Технічні характеристики готових рішень

Назва рішення / Виробник	Стандарти	Рішення / послуги	gNB	AMF	UDM	SMF	UPF	NRF	PCF	SEPP
Ericsson 5G Core	3GPP Rel.16	URLLC, eMBB	+	+	+	+	+	+	+	+
Nokia Cloud Packet Core	3GPP Rel.15	eMBB, mMTC	+	+	+	+	+	+	+	+
Huawei 5GC Solution	3GPP Rel.16	URLLC, mMTC, eMBB	+	+	+	+	+	+	+	+

Вибір критеріїв $k=\{k_1, k_2,\ldots,k_n\}$, за якими буде оцінюватися система (заносяться до табл. 2.8):

Таблиця 2.8.

Матриця вибору оптимального готового технічного рішення

Назва рішення	k_1 (Продуктивність)	k_2 (Надійність)	k_3 (Гнучкість розгортання)	k_4 (Підтримка стандартів)	k_5 (Вартість)	Інтегральна оцінка
Ericsson 5G Core	5	5	4	5	3	4.4
Nokia Cloud Core	4	5	5	5	4	4.6
Huawei 5G Solution	5	4	5	5	4	4.6

Для вибору оціночної шкали можна зробити багатокритерійний аналіз з ваговими коефіцієнтами або просто по наявності/відсутності певної необхідної характеристики і приймати рішення по ціні продукту. З ваговими коефіцієнтами критерій інтегральної оцінки буде мати вигляд:

$$k_{інт} = \sum(k_n \cdot x_n),$$

де вектор $x=\{x_1, x_2,\ldots,x_n\}$ – вектор важливих для оператора характеристик (наприклад, пропускна здатність, імовірність бітової помилки тощо).

Вибір оптимального готового рішення для побудови мережі 5G.

Пошук і систематизація рішень для побудови окремих вузлів мережі 5 G. (табл. 2.9.):

Таблиця 2.9.

Вибір оптимального рішення для окремих вузлів мережі 5G

Назва моделі виробника для окремого вузла	Критерії оцінювання									Інтег-ральна оцінка
	1	2	3	4	5	6	7	8	9	
Ericsson gNB 6488	5	5	4	5	4	5	4	5	4	4.6
Huawei AAU5613	5	4	5	4	5	4	4	5	5	4.6
Nokia AirScale	4	5	5	5	4	4	5	4	4	4.5

Вибір критеріїв, за якими буде оцінюватися рішення для вузлів (вносяться до табл. 2.6).

Вибір оціночної шкали проводиться аналогічно п. 3 даної методики.

Вибір оптимальних рішень для окремих вузлів.

Перевірка сумісності окремих вузлів різних виробників (в разі невідповідності – заміна на менш оптимальне рішення).

Порівняльний аналіз вартостей готового рішення і на основі окремих вузлів та вибір кращого.

Розробка специфікації обладнання для побудови 5G мережі в рамках поставленого завдання і використання для подальших розрахунків.

2.3.4. Побудова початкового наближення мережі 5G

Процес проектування базової конфігурації мережі 5G передбачає вирішення задачі розміщення інфраструктурних елементів з урахуванням обмежень частотного ресурсу та вимог до швидкісних характеристик сервісу. Основна мета полягає в тому, щоб визначити кількість і розміщення базових станцій таким чином, щоб забезпечити максимальні можливі швидкості передачі даних у напрямках до користувача та від нього при обмеженій кількості доступних вузлів зв’язку [58].

Альтернативно, можна підходити до задачі з протилежного боку: заздалегідь задавши необхідні показники пропускної здатності, прагнути мінімізувати кількість базових станцій без втрати якості обслуговування.

Оскільки точні розрахунки в умовах складного середовища покриття є непридатними, доцільно застосовувати наближені моделі. У рамках таких моделей приймаються спрощення:

- передбачається однорідний розподіл користувачів по площі;
- усі зони покриття базових станцій вважаються ідентичними за площею;

- структура забудови або ландшафту території вважається одноманітною — чи то урбанізоване середовище, чи сільська місцевість.

Щоб забезпечити більш точну і реалістичну початкову схему розгортання мережі 5G, доцільно поділити всю зону покриття на окремі сегменти. У кожному з них застосовуються стандартизовані припущення щодо щільності користувачів, конфігурації місцевості та параметрів навантаження, які дозволяють ефективніше моделювати поведінку мережі в реальних умовах.

Ключовим завданням цього етапу є формування вихідної архітектури розташування базових станцій нового покоління (gNB), яка дозволяє провести попередню оцінку рівня сигналу, пропускної здатності й якості сервісу в межах кожної зони. Для формування такої архітектури необхідна велика кількість вхідних параметрів, і точність цих даних має вирішальне значення для подальших етапів проектування.

На цьому етапі також виконується аналіз допустимих втрат у радіоканалі, які визначаються технічними характеристиками обраного стандарту мобільного зв’язку. Результати цього аналізу дозволяють визначити межі зони покриття для кожної станції.

Таким чином, набір початкових параметрів для планування мережі 5G включає технічні, географічні й експлуатаційні характеристики, що будуть розглядатися у відповідному переліку в подальшому.

Таблиця 2.10.

Вхідні дані для планування мережі

№ з/п	**Параметр**	**Одиниці виміру / Варіанти**
1	Площа території, на якій необхідно забезпечити покриття	$м^2$
2	Характер забудови	Місто / Передмістя / Сільська місцевість
3	Частотний діапазон	n78 (3.5 ГГц), n258 (28 ГГц), тощо
4	Тип середовища поширення сигналу	Urban Macro / Urban Micro / Rural

5	Максимально допустима затримка в каналі	мс
6	Імовірність побутової помилки (BLER)	Не вище Pbit
7	Необхідна пропускна здатність на одного абонента	Мбіт/с
8	Орієнтовна кількість абонентів у зоні	Осіб
9	Пріоритетний тип сервісу	eMBB / URLLC / mMTC
10	Мінімальний рівень сигналу на приймачі	дБм
11	Висота підвісу антени базової станції (gNB)	м
12	Смуга пропускання каналу	МГц
13	Конфігурація антен / MIMO	2x2, 4x4, 8x8, Massive MIMO
14	Планована щільність розміщення базових станцій	шт/км²

2.3.5. Методика оцінки бюджета втрат і зони покриття

Максимально допустимі втрати при поширенні в каналі рівні [59]:

$$L = P_{TX} + G_{TX} - P_{RX} - B_{BODY} + G_{RX} - B_{fid} - IM - L_{slow} - L_{мет} - L_{ф}, \quad (2.1)$$

де P_{TX} – потужність передавача;

G_{TX} – коефіцієнт підсилення передавальної антени;

P_{RX} – чутливість приймача;

B_{BODY} – втрати в тілі абонента;

G_{RX} – коефіцієнт підсилення приймальної антени;

B_{fid} – втрати у фідері, IM – запас по інтерференції;

L_{slow} – запас на повільні завмирання , береться рівним 10.3 дБ.

$L_Ф$ – врати сигналу у фідерних лініях. При відсутності фідера (коли прийомопередавачі об'єднані з антеною у вигляді моноблока) необхідно враховувати конструктивні особливості пристрою з'єднання.

$L_{мет}$ – втрати, обумовлені поглинаннями в атмосферних газах, гідро метеорах, тумані тощо, дБ. $L_{мет}$ визначається наступною формулою [58]:

$$L_{мет} = L_{тум} + L_{гідромет} + L_{аг},$$

де $L_{тум}$ – втрати потужності радіосигналу в тумані, дБ;

$L_{гідромет}$ – втрати потужності радіосигналу під час опадів, дБ;

$L_{аг}$ – величина затухань радіосигналу в атмосферних газах.

Математичний апарат для розрахунку $L_{тум}$, $L_{гідромет}$ та $L_{аг}$ наступний [58].

Втрати у газах атмосфери $L_Г$, дБ, визначаються за формулою

$$L_Г = (\gamma_{O_2} + \gamma_{H_2O}) \cdot l,$$

де γ_{O_2}, γ_{H_2O} – погонні втрати (дБ/км) у кисні та водяних парах атмосфери при температурі повітря 15 ^{0}С та відносній вологості 100 % (абсолютна вологість становить 13,4 г/м^3):

$$\gamma_{O_2} = \left(7{,}19 \cdot 10^{-3} + \frac{6{,}09}{f^2 + 0{,}227} + \frac{4{,}81}{(f-57)^2 + 1{,}5} \right) f^2 \cdot 10^{-3},$$

$$\gamma_{H_2O} = (0{,}078 + \frac{3{,}6}{(f-22{,}2)^2 + 8{,}5} + \frac{10{,}6}{(f-183{,}3)^2 + 9} + \frac{8{,}9}{(f-325{,}4)^2 + 26{,}3}) f^2 \cdot 13{,}4 \cdot 10^{-4},$$

де f - робоча частота, ГГц.

Додаткові втрати $L_{ДОД}$, які складаються з втрат у антенних обтікачах та від перепаду висот приймальної та передавальної антен можна прийняти рівними 1,5 дБ.

Запас по інтерференції IM (дБ) визначається наступним чином:

$$M = P_{пр} - P_{пор}(10^{-3}).$$

Як показано в [59],чутливість приймача P_{RX} може бути представлена наступним чином:

$$P_{RX} = 10 \cdot \lg((E_b / N_0) \cdot k \cdot T \cdot R)$$

де (E_b/N_0) - відношення сигнал/шум в цифрових систмемах зв'язку – це відношення енергії сигналу на 1 біт до щільності потужності шумів на 1 герц;

R – швидкість передавання даних;

$k = 1{,}23\times10^{-23}$ Дж/к – стала Больцмана,

T – температура в Кельвінах (абсолютна температура).

Таким чином вираз (2.1) можна представити у вигляді:

$$L = P_{TX} + G_{TX} - 10\cdot\lg((E_b / N_0)\cdot \mathrm{k}\cdot T\cdot R) - B_{BODY} + G_{RX} - B_{fid} - IM - L_{slow} - L_{мет} - L_{ф}$$

Для визначення співвідношень сигнал/шум, при яких не перевищується імовірність виникнення бітових помилок, проведемо моделювання для імовірності бітової помилки в обох підканалах для різних типів модуляції, яка використовується в обладнанні мереж 5G.

Імовірність бітової помилки BER_0 у гаусівському каналі дорівнює [60]

$$BER_0(\eta) = 0.5[1-\Phi(\sqrt{a\eta})],$$

$$\Phi(x) = \frac{2}{\sqrt{\pi}}\int_0^x \exp(-t^2)dt,$$

де α=2 и α=1 для бінарної и квадратурної фазових модуляцій, відповідно.

Відношення сигнал/шум (ВСШ) в i-му власному підканалі $\eta_i = \beta_i\rho_0\lambda_i$

Враховуючи нормування щільності імовірності і, вводячи параметр $\rho_i = \beta_i\alpha\rho_0$, отримаємо:

$$BER_i = \frac{1}{2} - \frac{1}{2}\int_0^\infty f_i(\lambda)\Phi(\sqrt{\rho_i\lambda})d\lambda$$

Враховуємо, що імовірність бітової помилки P_b для BPSK та QPSK визначається виразом [61]

$$P_b = Q\left(\sqrt{2\gamma_b}\right),$$

де $Q(x) = \frac{1}{\sqrt{2\cdot\pi}}\cdot\int_x^\infty \exp(-\frac{u^2}{2})du$ – таблична функція, значення котрої надане у [67]; γ_b – відношення енергії біта E_b до спектральної щільності шуму N_0.

Для гаусівського каналу і прийому за допомогою узгоджених фільтрів імовірність бітової помилки при модуляції M-QAM, де $M=2^k$ і k – парне, визначається наступним чином [64]

$$BER = \frac{2\cdot(1-L^{-1})}{\log_2(L)}\cdot Q\left[\sqrt{\frac{3\cdot\log_2(L)}{L^2-1}\cdot\frac{2\cdot E_b}{N_0}}\right]$$

де $L=\sqrt{K}$ представляє кількість рівнів амплітуди в одному вимірі.

Для оцінки втрат сигналу L під час поширення радіохвиль, на основі проведеного аналізу та практичного досвіду, доцільно сформувати орієнтовні рекомендації щодо вибору моделей радіохвильового розповсюдження залежно від частотного діапазону. Це дозволяє адаптувати підхід до моделювання до конкретних умов використання і забезпечити більшу точність у прогнозуванні параметрів покриття для мереж 5G. (табл. 2.11.).

Таблиця 2.11.

Рекомендації щодо використання емпіричних моделей розповсюдження радіохвиль для різних діапазонів частот

Частотний діапазон	**Технологія**	**Рекомендована модель розповсюдження радіохвиль**
До 2 ГГц	5G NR (FR1)	Модель Хата, 3GPP TR 38.901 (Urban Macro/Suburban)
2,3–2,6 ГГц	5G NR (FR1)	Модель COST-231 Hata, 3GPP Urban Micro
3,3–4,2 ГГц (н77, н78)	5G NR (FR1)	3GPP TR 38.901 (UMa/UMi), SUI, Ericsson model (LOS/NLOS)
4,4–5,0 ГГц (н79)	5G NR (FR1)	Модель Ericsson (для умов NLOS), SUI
24,25–29,5 ГГц (н257, н258)	5G NR (FR2)	Моделі mmWave: 3GPP TR 38.901, NYUSIM, METIS, Close-In Free Space (CI)
37–43,5 ГГц (н260, н261)	5G NR (FR2)	3GPP TR 38.901 (mmWave LOS/NLOS), ITU-R M.2412

Таким чином, можна виразити максимальну дальність зв’язку для різних частотних діапазонів, що використовуються в 5G. Наприклад, для моделі SUI (Stanford University Interim)[61] для діапазону вище 3,5 ГГц:

$$\lg(d/d_0) = (L - (A + X_f + X_h + s))/ 10\gamma, \text{ для } d > d_0,$$

де d – відстань від базової станції до приймаючої антени; d_0=100 м; X_f – корегуюча для частоти більшої за 2 ГГц; X_h – корегуюча для висоти приймаючої антени; s – корегуюча на затінення; γ – експонента втрат.

Параметр s знаходиться в межах між 8,2 та 10,6 дБ. Параметр A визначається:

$$A=20\lg(4\pi d_0/\lambda),$$

де λ – довжина хвилі; $\gamma=a-bh_b+(c/h_b)$, де h_b – це висота підйому антени базової станції (м), знаходиться в межах від 10 до 80 м.

Константи a, b та c залежать від типу місцевості, їх значення надані в таблиці 2.12.

Таблиця 2.12.

Значення параметрів для різних типів місцевості в моделі SUI

Параметр моделі	**Місцевість з пагорбами, високою щільністю перешкод**	**Приміська місцевість**	**Рівнинна місцевість з малою кількістю перешкод**
a	4,6	4,0	3,6
b (1/м)	0,0075	0,0065	0,005
c (м)	12,6	17,1	20

$$X_f=6\lg(f/2000),$$

$$X_h=-10{,}8\lg(h_r/2000),$$

$$X_h=-20\lg(h_r/2000),$$

де f – це частота в МГц; h_r – висота приймаючої антени в метрах.

2.3.6. Частотне планування мережі 5G

Частотне планування в мережах п’ятого покоління (5G) є критичним етапом проектування, який безпосередньо впливає на продуктивність, якість зв’язку та ефективність використання спектра. У 5G, на відміну від попередніх поколінь, частотне планування стало більш складним завдяки широкому діапазону використовуваних частот — від субгігагерцового спектра до міліметрових хвиль (mmWave) [62].

Основні частотні діапазони в 5G:

- FR1 (Frequency Range 1): 410 МГц – 7125 МГц. Основний діапазон для забезпечення широкого покриття і проникнення сигналу в приміщення (наприклад, 700 МГц, 1800 МГц, 3.5 ГГц).

- FR2 (Frequency Range 2): 24.25 ГГц – 52.6 ГГц. Діапазон міліметрових хвиль для надвисокої швидкості передачі даних на короткі відстані (наприклад, 26 ГГц, 28 ГГц, 39 ГГц).

Мета частотного планування:

- Забезпечення ефективного використання спектра.

- Мінімізація інтерференції між сусідніми сотами.

- Підтримка вимог до швидкості, затримки та щільності підключень.

Методи частотного планування:

1. Використання однієї частоти в усіх сотах з управлінням інтерференцією на основі beamforming та MIMO.

2. Soft Frequency Reuse (SFR): Розподіл частот між центральною та периферійною частинами стільника для зменшення завад.

3. Dynamic Spectrum Sharing (DSS): Динамічне використання спектра між 4G і 5G, що спрощує розгортання мережі.

Особливості для mmWave:

- mmWave діапазон має високу пропускну здатність, але обмежену зону покриття через сильні втрати сигналу.

- Частотне планування в цьому діапазоні фокусується на формуванні

направлених променів (beamforming) і щільному розміщенні малих стільників.

Інструменти частотного планування:

- Використання моделей поширення (3GPP TR 38.901, ITU-R M.2412).- Програмні інструменти: Atoll, iBwave, Mentum Planet для симуляцій покриття та інтерференції [63].

2.3.7. Побудова опорного сегменту

Опорний сегмент мережі 5G доцільно будувати за наступною послідовністю кроків [57]:

1. Розрахувати пропускну здатність каналів радіомережі за допомогою формули (1):

$$C_{1аб} = \Delta F \cdot \beta, \tag{1}$$

де: $C_{1аб}$ – пропускну здатність каналу, ΔF– ширина каналу, β – спектральна ефективність каналу,

2. Розрахувати початкове наближення пропускної здатності мережі 5G для кожного eNB, при цьому, виходячи з наступних умов (2):

$$\begin{cases} C_{Тр.Мер} \geq \sum_{i=1}^{N_{аб}} C_{1абі} = N_{аб} \cdot C_{1аб}, \\ C_{Ком} \geq \sum_{i=1}^{N_{кон}} C_{Тр.Мер.і}, \\ C_{Агр.} \geq \sum_{i=1}^{N_{ком}} C_{Комі}. \end{cases} \tag{2}$$

де: $C_{Тр.Мер}$ – пропускна здатність транспортної мережі; $C_{1аб}$ – виділений канал на одного абонента; $C_{Ком}$ – пропускна здатність комутаторів; $C_{Агр.}$ – пропускна здатність інтелектуальної агрегації; $N_{аб}$ – кількість абонентів; $N_{кан}$ – кількість каналів транспортної мережі; $N_{ком}$ – кількість комутаторів.

Під час вибору обладнання для транспортної інфраструктури мережі 5G слід враховувати специфіку цієї технології. Зокрема, техніка має відповідати вимогам

високої надійності, бути економічно доцільною з погляду співвідношення «вартість–якість», забезпечувати високу ефективність, гнучкість, компактність і багатофункціональність.

Для забезпечення передачі даних у 5G-мережах необхідно підібрати два основних типи транспортного обладнання:

- для підтримки мережі радіодоступу;
- для реалізації функцій інтелектуальної агрегації.

Вартість всього обладнання розраховується за формулою (3):

$$P = P_{eNB} \cdot N_{eNB} + P_{ком} \cdot N_{ком} + P_{агр} \cdot N_{агр}, \quad (3)$$

де: P – загальна вартість обладнання, P_{eNB} – вартість однієї базової станції, N_{eNB} – кількість базових станцій, $P_{ком}$ – вартість одного комутатора, $N_{ком}$ – кількість комутаторів, $P_{агр}$ – вартість однієї одиниці обладнання агрегації, $N_{агр}$ – кількість одиниць обладнання агрегації.

2.3.8. Оптимізація основних параметрів мережі

Особливу увагу варто приділити кібербезпеці мобільних мереж спеціального призначення, зокрема на основі рекомендацій ETSI [64] та підходів IEEE до забезпечення QoS [65].

Рекомендації ETSI передбачають багаторівневу модель забезпечення безпеки, яка охоплює як фізичні компоненти інфраструктури, так і програмне забезпечення, протоколи зв’язку та управління ідентифікацією. У контексті мобільних мереж спеціального призначення особливо актуальними є засоби захисту сигналізації, шифрування даних на канальному та транспортному рівнях, а також вбудовані механізми автентифікації користувачів і пристроїв у зашифрованих та закритих доменах.

З боку IEEE значну увагу приділено забезпеченню надійності зв’язку в умовах кіберзагроз. Підходи IEEE до забезпечення QoS передбачають не лише пріоритезацію трафіку критичних служб, але й впровадження резервних

маршрутів, швидке перенаправлення трафіку у випадку атак або збоїв, а також використання мережевої телеметрії для виявлення аномалій у режимі реального часу. Такі засоби сприяють мінімізації часу простою та гарантують збереження працездатності мережі навіть в умовах активного зовнішнього впливу.

Етапи оцінювання поточного стану мережі представлені на рис. 2.5 [45].

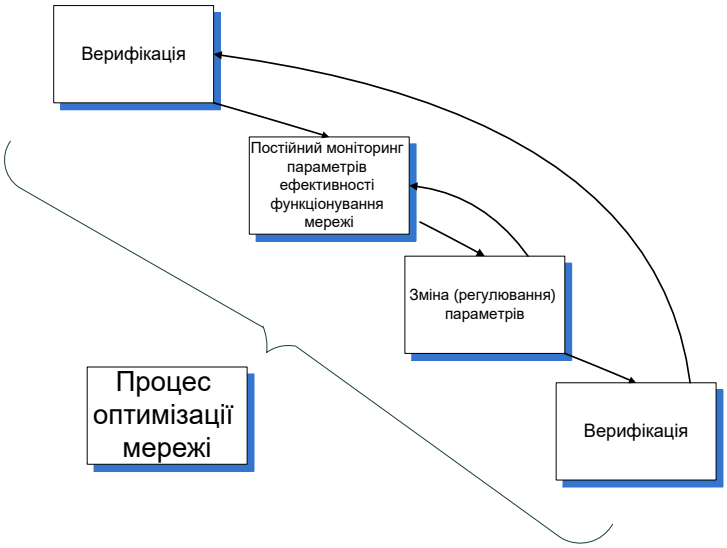

Рисунок 2.5. Оцінювання поточного стану мережі

Процес верифікації спрямований на перевірку критичних параметрів функціонування стільникової мережі, зокрема:

- географічного розміщення базових станцій;
- меж їхнього покриття;
- зон передачі з'єднання (хендовера);
- списків частот, призначених конкретним сотам;
- технічних характеристик приймальних модулів (наприклад, потужність передавання, чутливість);
- типів і властивостей антен (зокрема коефіцієнт підсилення, схема спрямованості);
- кількості приймачів, підключених до кожної антени;
- просторових координат антен;
- параметрів установки (висота, азимут, кут нахилу, характеристики антенно-фідерного тракту).

Моніторинг дозволяє оцінити покриття та якість роботи мережі, що необхідно для перевірки відповідності реальних характеристик запланованим на етапі проектування, а також для виявлення проблемних зон.

Оптимізація включає внесення змін до конфігурації мережі на основі зібраної інформації під час моніторингу та перевірки. Вона орієнтована на досягнення поставлених цілей і може включати:

- збалансування навантаження між окремими зонами;
- покращення використання частотного ресурсу за рахунок оновлення частотно-просторової структури;
- зменшення зон з низьким рівнем сигналу, викликаних перешкодами;
- розширення покриття;
- підвищення ефективності процесу передачі між сотами;
- покращення якості послуг;
- впровадження підтримки мультистандартної архітектури.

Для здійснення оптимізації пропонується використання методології, яка базується на оцінці ключових показників якості обслуговування (QoS), рівня інформаційної безпеки та загальної ефективності мережі.

2.3.9 Оцінка ключових показників якості обслуговування, рівня захищеності інформації та ефективності функціонування стільникових мереж

У сучасних умовах підвищених вимог до мобільних мереж спеціального призначення об'єктивна оцінка їх функціонування є необхідною передумовою забезпечення належного рівня якості сервісів та захищеності інформаційних потоків [66].

Основними напрямами оцінювання виступають:

- **Параметри якості обслуговування (QoS)**, серед яких визначальними є затримка доставки пакетів даних, час встановлення з'єднання, середня пропускна здатність каналів, рівень втрат пакетів, стабільність сервісів під навантаженням.

- **Індикатори інформаційної безпеки**, що включають ступінь шифрування трафіку, стійкість до атак типу "людина посередині", захист каналів управління мережею та відповідність систем аутентифікації актуальним стандартам кібербезпеки.
- **Критерії експлуатаційної надійності мережі**, які охоплюють середній час виявлення та усунення відмов, здатність до самостійного відновлення після ушкоджень, рівень автономності сегментів при втраті централізованого керування.

Оцінка проводиться на основі імітаційного моделювання типових і критичних сценаріїв використання мережі. Спеціальна увага приділяється здатності мережевої інфраструктури зберігати функціональність при обмеженому доступі до ресурсів, в умовах кіберінцидентів або фізичного пошкодження окремих вузлів.

Інтегральний підсумковий показник ефективності формується шляхом агрегування нормованих оцінок за трьома групами критеріїв, що дозволяє об'єктивно визначити ступінь відповідності мережі вимогам експлуатації у звичайних і надзвичайних умовах.

Запропонований підхід до оцінювання є універсальним і може бути адаптований для різних типів архітектур стільникових мереж 5G та їхніх модифікацій для спеціалізованого зв'язку.

Одним із пріоритетних завдань при проектуванні та експлуатації стільникових мереж є оптимізація використання доступних ресурсів задля забезпечення високої якості обслуговування користувачів. У конкурентних умовах ринку телекомунікацій виникає необхідність розробки регламентуючих документів, які встановлюють вимоги до рівня якості послуг та параметрів роботи мереж.

Для створення ефективної системи контролю якості функціонування стільникових мереж доцільним є використання методики, заснованої на ключових показниках ефективності (KPI) та якості (KQI) [67].

Важливо розмежовувати поняття KPI і KQI:

- **Ключові показники ефективності (KPI, Key Performance Indicators)** характеризують технічні параметри роботи самої мережі, зокрема затримку, пропускну здатність, доступність сервісів, рівень втрат пакетів тощо. Вони слугують для оцінки функціональних можливостей інфраструктури та є орієнтованими на технічну сторону експлуатації мережі.
- **Ключові показники якості обслуговування (KQI, Key Quality Indicators)** оцінюють якість сприйняття послуг користувачами на рівні сервісу. До них належать параметри, що визначають зручність, безперервність, швидкість і стабільність роботи сервісів з погляду кінцевого споживача.

Управління цими показниками здійснюється в рамках концепції **Customer Experience Management (CEM)**, що спрямована на забезпечення позитивного досвіду користувачів при взаємодії з мобільною мережею.

На рисунку 2.6 схематично подано взаємозв'язок між KPI, KQI та процесами управління досвідом клієнтів (CEM): KPI безпосередньо відображають стан функціонування мережі, тоді як KQI віддзеркалюють рівень задоволення користувачів сервісами, що базуються на цій мережі.

Таким чином, ефективна оцінка стану мобільної мережі має враховувати як технічні характеристики її роботи, так і якість надання сервісів з точки зору кінцевого користувача, що забезпечує комплексний підхід до аналізу функціональної готовності мережі.

Показник	**Опис**	**Рівень застосування**
KPI	Технічні параметри функціонування мережі	Інфраструктура
KQI	Якість послуг з точки зору користувача	Рівень сервісу

Рис. 2.6. Відмінності KPI та KQI

Показники якості обслуговування (KQI) не завжди можуть виступати повністю об'єктивними характеристиками, оскільки базуються на суб'єктивних оцінках кінцевих користувачів та їх особистому досвіді взаємодії з мережею.

Для побудови ефективної системи контролю якості послуг (QoS), заснованої на використанні індикаторів KQI/KPI, необхідно на першому етапі визначити конкретні умови використання кожної послуги зв'язку. На всіх етапах експлуатації здійснюється перевірка відповідності фактичних значень індикаторів встановленим нормативам для конкретного виду послуг.

Задля забезпечення належного рівня обслуговування та оперативного реагування на запити користувачів доцільно застосовувати методику, яка передбачає моніторинг скарг та звернень, виявлення ключових проблем функціонування мережі, їхню класифікацію та подальше усунення причин зниження якості сервісів.

Ключові показники ефективності (KPI) умовно класифікуються за трьома основними групами:

- **Показники доступу** (доступність мережі, час встановлення з'єднання, ймовірність відмови при виклику);
- **Показники інтеграції послуг** (якість надання додаткових сервісів, наприклад передачі даних, **голосових** послуг, мультимедіа);
- **Показники мобільності** (успішність процесу хендоверу, кількість перерваних сеансів при зміні осередків).

У свою чергу, показники якості обслуговування (KQI) зосереджені на оцінці:

- **Безпеки користування мережею** (наявність шифрування, захист даних);
- **Зручності використання сервісів** (інтуїтивність доступу до послуг, швидкість реагування сервісів);
- **Гнучкості роботи мережі** (адаптивність до зміни умов навантаження та рухливості абонентів).

Як було зазначено, після розгортання стільникової мережі необхідно здійснювати її безперервну оптимізацію шляхом регулярного оцінювання показників якості обслуговування та продуктивності функціонування. З цією метою розроблено метод оцінки ключових параметрів QoS, що передбачає

систематичний моніторинг KPI та KQI, аналіз відхилень від цільових значень, та впровадження коригувальних заходів для підтримання високого рівня експлуатаційної готовності мережі.

Таким чином, запропонований підхід дозволяє комплексно оцінити технічний стан мережі, якість надання послуг користувачам та своєчасно виявляти фактори, що впливають на зниження ефективності її функціонування.

Запропонований метод реалізується у чотири етапи:

Етап 1 – Формалізація переліку послуг

На першому етапі здійснюється визначення набору послуг, які підлягають аналізу в рамках оцінювання якості обслуговування. Формалізуємо перелік послуг у вигляді множини:

$$S = \{ s_1, s_2, ..., s_n \} \quad (4)$$

де n — загальна кількість аналізованих послуг, s_i — окрема послуга. Кожній послузі s_i ставиться у відповідність підмножина елементів системи забезпечення якості обслуговування:

$$S_i = \{ e_{i1}, e_{i2}, ..., e_{iki} \} \quad (5)$$

Тоді повна структура множини послуг враховує як перелік сервісів, так і відповідні технічні елементи їх підтримки:

$$S = \bigcup S_i \quad (6)$$

Мета етапу: чітке визначення об'єкта оцінювання та структурування сервісів.

Етап 2 – Формування множини ключових індикаторів якості (KQI)

На другому етапі формується система показників якості обслуговування для кожної послуги:

$$KQI_i = \{ q_{i1}, q_{i2}, ..., q_{imi} \} \quad (7)$$

Формується загальна сукупність показників:

$$KQI = \bigcup KQI_i \quad (8)$$

Мета етапу: створити повний набір якісних індикаторів для оцінювання всіх розглянутих сервісів.

Етап 3 – Встановлення відповідностей між послугами та показниками якості

На цьому етапі встановлюється відповідність між елементами множини послуг та індикаторами якості.

Результатом етапу є побудова матриці відповідності, де кожній послузі ставляться у відповідність її ключові показники.

Особливу увагу варто приділити кібербезпеці мобільних мереж спеціального призначення, зокрема на основі рекомендацій ETSI [68] та підходів IEEE до забезпечення QoS [69].

Мета етапу: забезпечити формалізовану основу для наступного аналізу якості послуг через відповідні KQI.

Етап 4 – Проведення оцінювання та аналізу результатів

На цьому етапі здійснюється збір фактичних даних, порівняння результатів з нормативними значеннями, виявлення відхилень та причин їх виникнення.

Мета етапу: об'єктивне оцінювання фактичного рівня якості обслуговування та ефективності мережі.

Висновки до розділу 2

У другому розділі дисертації розглянуто теоретичні та методологічні основи побудови мобільних мереж зв’язку спеціального призначення з використанням технологій 5G і перспективних архітектур. Проведено комплексний аналіз математичних моделей, алгоритмів та інтелектуальних підходів, що забезпечують підвищену ефективність, надійність та захищеність таких мереж в умовах динамічного радіооточення.

Визначено доцільність застосування методів локалізації, маршрутизації, розпізнавання модуляцій, сенсорного моніторингу, оптимізації енергоспоживання, а також реконфігурованих інтелектуальних поверхонь (RIS) у системах нового покоління. Окрему увагу приділено питанням формування ядра мережі з

підвищеним рівнем захисту, адаптації під урядовий зв’язок, підтримці мережевого розподілу та управління трафіком із мінімальною затримкою.

На основі огляду сучасних наукових підходів зроблено висновок, що застосування комплексної моделі, яка включає інтелектуальну обробку сигналів, адаптивне управління топологією та розширену безпеку, дозволяє створювати ефективні та масштабовані рішення для мобільного зв’язку спеціального призначення. Здобуті теоретичні положення покладено в основу подальшої розробки архітектури системи, моделювання її компонентів і оцінки параметрів якості обслуговування.

Окремі результати, викладені у цьому розділі, відображено у наступних наукових працях автора:

- Odarchenko R., Sunduchkov K., Fesenko V., Didenko A., Verkhovets O., Fesenko A. The concept of a channeling system for satellite mobile communication for media delivery with increased efficiency // Proceedings of the 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 22–26 February 2022, Lviv–Slavske, Ukraine. – P. 775–779. — розроблено концепцію канальної системи супутникового мобільного зв’язку для доставки медіаконтенту з підвищеною ефективністю;
- Dudnik A.S., Fesenko A.O., Fesenko V.O., Grinenko O.O., Grinenko S.A., Kvashuk D.M. Models and methods of determining penetration by means of wireless sensor networks // Monographic series “European Science”. Book 21. Part 1. Karlsruhe, Germany, 2023. – P. 161–171. — представлено моделі та методи виявлення проникнення на основі бездротових сенсорних мереж;
- Saiko V., Odarchenko R., Zhurakovskyi B., Yevdokymenko M., Fesenko V., Tkachova O. A model for building a wireless terahertz network for 5G NR // 12th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems, 7–9 September 2023, Dortmund, Germany. – P. 1071–1076. — запропоновано модель побудови бездротової терагерцової мережі з підтримкою RIS для мереж 5G/6G;

- Kotyk B., Bakhtiiarov D., Lavrynenko O., Chumachenko B., Antonov B., Fesenko V., Chupryn V. Neural network approach to 5G digital modulation recognition // Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024), 24–27 January 2024, Kyiv, Ukraine. – P. 82–92. — розглянуто застосування нейронних мереж для автоматичного розпізнавання типів цифрової модуляції в умовах завад;
- Chumachenko S.S., Chumachenko B.S., Maloyed M.M., Odarchenko R.S., Fesenko V.O. Метод маршрутизації в бездротових мережах IoT із високою щільністю пристроїв // Проблеми інформатизації та управління. – 2024. – Т. 4 № 80. – С. 99–112. — розроблено метод маршрутизації в бездротових IoT-мережах із високою щільністю пристроїв;
- Dudnik A.S., Fesenko V.O Mathematical models and localization algorithms wireless networks // Electronics and Control Systems. – 2025. – №1(83). – С. 50–58. — викладено математичні моделі та алгоритми локалізації у бездротових сенсорних мережах спеціального призначення.

РОЗДІЛ 3.
РОЗРОБКА МЕТОДУ

3.1 Розробка технічних рішень по удосконаленню ядра мережі 5G для застосування в мережах урядового радіозв'язку

Як вже було продемонстровано, стільникові мережі 5G мають ряд переваг в порівнянні з попередніми поколіннями стільникових мереж зв'язку, а тому можуть бути використані в якості основи для побудови мереж урядового радіозв'язку нового покоління. Проте, все одно залишається ряд невирішених питань щодо забезпечення необхідного рівня забезпечення кібербезпеки. Для цього необхідно проводити удосконалення вже наявної архітектури ядра мережі 5G.

3.1.1 Узгоджена архітектура ядра мережі 5G

Якість обслуговування оцінюється відповідно до визначень ITU-T [70], а також із урахуванням даних звітів Ericsson про навантаження на мережі [71].

Сучасна архітектура мереж 5G створена з урахуванням потреб у передачі широкого спектру даних і забезпечення різнопланових цифрових послуг. Вона базується на таких передових концепціях, як віртуалізація мережевих функцій (NFV) і програмно-керовані мережі (SDN), що забезпечують гнучкість і масштабованість інфраструктури. Подібні модульні підходи активно впроваджуються також у критично важливих системах зв'язку, де їх ефективність оцінюється в умовах реального використання, згідно з описаними методиками [72].

Основні технічні параметри продуктивності мереж п'ятого покоління включають [73-75]:

- Максимальні швидкості завантаження (downlink) до 20 Гбіт/с, з високим рівнем спектральної ефективності – близько 30 біт/с/Гц.
- Швидкість передачі даних у зворотному напрямку (uplink) може сягати 10 Гбіт/с при ефективності 15 біт/с/Гц.

- Радіоінтерфейс забезпечує наднизьку затримку до 1 мс для сервісів із критичною затримкою (URLLC) і до 4 мс – для послуг мобільного широкосмугового доступу (eMBB).
- У міських умовах 5G здатна підтримувати масове підключення – до мільйона пристроїв Інтернету речей на квадратний кілометр.
- Передбачена довготривала автономна робота IoT-пристроїв – до 10 років без підзарядки.
- Мережі 5G адаптовані до високошвидкісного руху, забезпечуючи стабільний зв’язок при швидкостях до 500 км/год.

Для досягнення необхідних технічних характеристик і гнучкості функціонування мереж п’ятого покоління впроваджуються ключові архітектурні принципи побудови інфраструктури 5G [76]:

1. Відокремлення компонентів, які реалізують функції управління (Control Plane, CP), від компонентів, що відповідають за передачу користувацьких даних (User Plane, UP). Це забезпечує масштабованість і дозволяє розміщувати функціональні модулі як централізовано, так і децентралізовано.
2. Формування логічних сегментів мережі (Network Slices) [77], кожен з яких налаштований для конкретного типу послуг або груп користувачів.
3. Впровадження мережевих функцій у вигляді віртуалізованих модулів – Virtual Network Functions (VNF), що забезпечує гнучкість у розгортанні і підтримці [78].
4. Забезпечення доступу до як централізованих, так і периферійних сервісів, що дозволяє реалізувати концепції хмарних та крайових обчислень (fog та edge computing).
5. Створення єдиної архітектури, яка поєднує різні типи мереж доступу – як стандартизовані за 3GPP (New Radio – NR), так і альтернативні (наприклад, Wi-Fi або WiMAX), з інтеграцією в одну опорну інфраструктуру (Core Network).
6. Реалізація уніфікованої системи автентифікації користувачів, незалежно від того, яким типом мережі вони користуються.

7. Впровадження безстанових мережевих функцій (stateless functions), що дозволяє гнучко розподіляти обчислювальні й зберігальні ресурси.

8. Розширена підтримка роумінгу, з можливістю маршрутизації трафіку як через домашню мережу (home routed), так і з його обробкою безпосередньо в мережі оператора, що приймає (local breakout).

Питання адаптивності та самоорганізації елементів в мережах спеціального призначення також розглядається в [79], де побудовано симуляційну модель, здатну динамічно змінювати маршрутизацію залежно від стану мережі.

У структурі мережі 5G передбачено два основні підходи до взаємодії між її функціональними компонентами:

- Сервіс-орієнтована модель, де одна мережева функція (наприклад, AMF) надає свої сервіси іншим авторизованим функціям, що забезпечує гнучке управління доступом до ресурсів;
- Взаємодія через визначені інтерфейси, яка реалізується як точка-точка (наприклад, інтерфейс N11) між окремими функціональними модулями (наприклад, AMF та SMF), що дозволяє контролювати і координувати передачу даних.

Архітектура мережі 5G містить низку ключових функціональних блоків (мережевих функцій – NF), серед яких[76]:

- AMF (Access and Mobility Management Function) – відповідає за обробку запитів на підключення та мобільність користувачів;
- SMF (Session Management Function) – керує параметрами користувацьких сеансів;
- UPF (User Plane Function) – забезпечує передачу даних між користувачем і мережею;
- UDM (Unified Data Management) – координує управління персональними даними абонентів;
- UDR (Unified Data Repository) – виступає як централізоване сховище для збереження користувацької інформації;

- UDSF (Unstructured Data Storage Function) – дозволяє обробляти і зберігати неструктуровані дані;
- NSSF (Network Slice Selection Function) – забезпечує вибір необхідного мережевого сегменту (slicing);
- PCF (Policy Control Function) – реалізує політики управління трафіком і доступом;
- NEF (Network Exposure Function) – відкриває функції мережі для зовнішніх додатків і сервісів;
- NRF (NF Repository Function) – виконує функцію реєстру мережевих функцій;
- AF (Application Function) – відповідає за інтеграцію з прикладними сервісами;
- SMSF (SMS Function) – надає функціональність обміну короткими повідомленнями на рівні NAS;
- N3IWF (Non-3GPP Inter Working Function) – забезпечує взаємодію з мережами, що не відповідають стандарту 3GPP.

На рис. 3.1 зображена архітектура мережі 5G з точки зору сервіс-орієнтованого взаємодії різних мережевих функцій на площині управління.

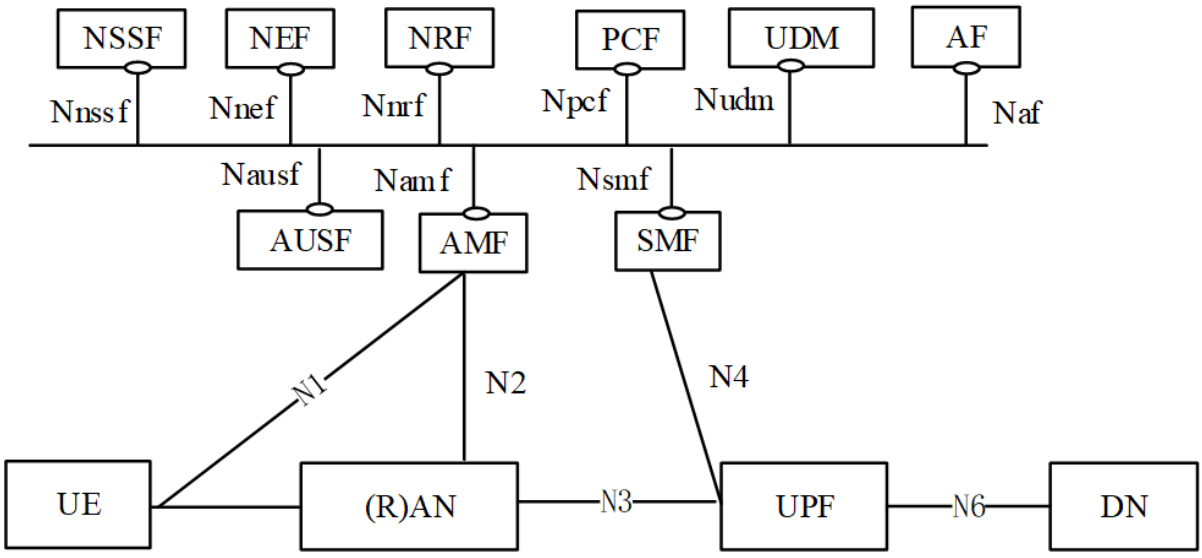

Рис. 3.1. Архітектура мережі 5G та взаємодія мережевих функцій

3.1.2. Удосконалення ядра мережі 5G для застосування в мережах урядового радіозв’язку

Як було зазначено раніше, з урахуванням вимог, що пред'являються до сучасної урядової мережі радіозв’язку, прийнято рішення про її реалізацію на базі технології п’ятого покоління – 5G [80].

Архітектурна концепція мережі урядового зв’язку на основі 5G ґрунтується на таких ключових засадах:

- Функціональний поділ мережі на компоненти, які відповідають за користувацький трафік (User Plane), та елементи, що керують сигнальним трафіком і контролем з’єднань (Control Plane).
- Формування ізольованих мережевих шарів (slices) для окремих груп користувачів, з урахуванням специфіки державного призначення сервісів.
- Віртуалізація мережевих функцій (VNF), що дозволяє гнучко масштабувати ресурси й оптимізувати витрати.
- Уніфіковані механізми аутентифікації, адаптовані до вимог безпеки урядового сектору.
- Впровадження спеціалізованих функцій захисту та надійності, які гарантують високий рівень захисту комунікаційної інфраструктури в межах критичних служб.

Схожі підходи до управління ресурсами в мережах спеціального призначення описані у [79], де запропоновано комплексну модель розподілу ресурсів із урахуванням критичності каналів та вимог до стійкості.

Підхід до забезпечення безпеки в урядових мережах зв’язку, створених на базі технології 5G, базується на впровадженні передових технологій, що гарантують захист, збереження та цілісність переданої або отриманої інформації. На рис. 3.2 представлено рекомендовану структуру ядра мережі, яка враховує вимоги до безпечного функціонування критично важливих комунікацій.

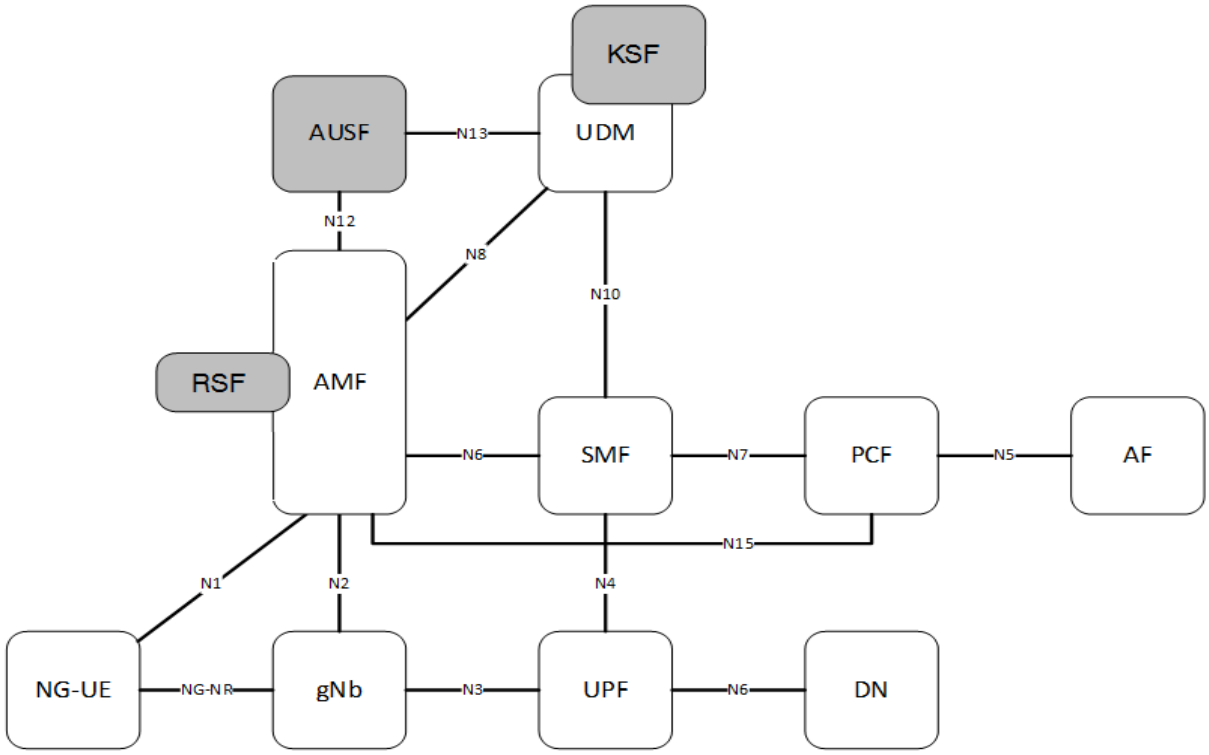

Рис. 3.2. Структурна модель реалізації опорної інфраструктури урядової мережі радіозв’язку

На рисунку 3.2 сірим кольором позначено функціональні компоненти, які відповідають за реалізацію захисних механізмів у системі:

1. AUSF (Authentication Server Function) – виконує функцію централізованого сервера автентифікації.

2. RSF (Reliable Security Function) – компонент для реалізації високонадійного рівня захисту.

3. KSF (Cryptographic Security Function) – елемент, що забезпечує посилену криптографічну безпеку.

На початковому етапі пропонується інтегрувати RSF із модулем управління мобільністю та доступом (AMF), а KSF – з уніфікованим модулем управління даними (UDM).

Функція AUSF відповідає за прийом запитів автентифікації, які надходять від RSF, та їх подальшу обробку або перенаправлення до KSF.

Компонент RSF, спільно з AUSF, забезпечує перевірку автентичності пристрою користувача під час його реєстрації в мережі. Після цього система узгоджує політики безпеки відповідно до ідентифікованого користувача (UE) і виконує шифрування переданих даних з паралельним контролем їхньої цілісності.

Компонент криптографічного захисту (KSF) відповідає за генерацію, зберігання та розподіл індивідуальних секретних ключів, а також керування параметрами криптографічних алгоритмів. Ця функція реалізується у спеціально захищеному центрі обробки даних і функціонально інтегрується з модулем централізованого управління даними користувачів – UDM (Unified Data Management)**.**

Реалізація подібних сценаріїв у США базується на практичному досвіді проєктів приватних мереж, зокрема у відомствах, де 5G адаптується до потреб служб громадської безпеки [81][82].

Функція AMF (Access and Mobility Management Function) відповідає за:

- управління інтерфейсами управлінської площини (N1 і N2);
- обробку NAS-сигналізації через N1, її захист та шифрування;
- контроль реєстрації абонентських пристроїв у мережі та змін їх статусів (RM-REGISTERED/ DEREGISTERED);
- управління підключенням абонентів до мережі та переходами між станами (CM-IDLE/ CONNECTED);
- моніторинг доступності пристрою у стані очікування;
- контроль мобільності пристрою під час активного з’єднання;
- обмін короткими повідомленнями між користувачем і SMF;
- координацію з функцією управління місцезнаходженням (LMF) та з мережею доступу (RAN);
- роботу з ідентифікаторами потоків EPS для взаємодії з LTE;
- підтримку доступу через не-3GPP технології через N3IWF.

Функція SMF (Session Management Function) забезпечує:

- керування сесіями (створення, модифікація, завершення), у тому числі встановлення тунелів з UPF;

- призначення IP-адрес користувачам;
- вибір маршруту через UPF;
- взаємодію з політиками обслуговування через PCF;
- контроль роботи UPF, зокрема за якістю обслуговування (QoS);
- підтримку DHCP для автоматичних налаштувань;
- моніторинг тарифікаційних даних;
- забезпечення безперервності сесій (SSC);
- підтримку роумінгу.

Функція UPF (User Plane Function):

- підключення до зовнішніх мереж, зокрема Інтернету;
- маршрутизація трафіку і передача пакетів;
- буферизація і ініціація повідомлень про наявність нових даних;
- присвоєння QoS-міток;
- складання звітів про трафік.

Модуль UDM (Unified Data Management):

- зберігання та керування профілями користувачів;
- ідентифікація користувачів (SUPI), генерація облікових даних;
- контроль доступу відповідно до профілю;
- підтримка прив'язки до конкретного AMF;
- забезпечення сталості сеансів та обслуговування;
- керування обробкою SMS.

Функція PCF (Policy Control Function):

- формування політик обслуговування в режимі реального часу;
- динамічне створення віртуальних каналів залежно від сервісу, місцезнаходження користувача та навантаження мережі. [83].

Прикладна функція (AF) в архітектурі мережі 5G є компонентом, що координує обмін інформацією між додатками та опорною мережею. Вона може виконувати такі ключові задачі:

- керування напрямками маршрутизації користувацького трафіку;

- доступ до модуля взаємодії мережевих компонентів (NEF) для інтеграції зовнішніх додатків;
- комунікація з функцією управління політиками (PCF) для встановлення або зміни правил обслуговування.

Залежно від політики оператора, частина сторонніх сервісів може отримати прямий доступ до функцій ядра мережі 5GC. Для решти – передбачено доступ через стандартизовані API, які реалізуються за допомогою NEF (Network Exposure Function).

Модель безпеки мереж урядового зв'язку, реалізована в архітектурі 5G, базується на комплексному підході:

1. Перевірка справжності користувача мережею.
2. Перевірка справжності самої мережі користувачем.
3. Синхронізація криптографічних ключів між мережею та користувацьким пристроєм.
4. Застосування шифрування для захисту сигналізації, а також контроль її цілісності.
5. Захист унікального ідентифікатора користувача (наприклад, SUPI).
6. Проведення аутентифікації та захисту даних безпосередньо на рівні кінцевих сервісів.

Оскільки без проходження процесу стандартизації, не можливо вносити зміни до архітектури ядра мережі 5G, то пропонуємо винести функціонал запропонованих мережевих підфункцій KSF та RSF на спецалізований сервер захищеного урядового зв'язку у мережі 5G (рис. 3.3).

Коли користувачі такої мережі географічно розподілені, різні групи абонентів можуть також обслуговуватися виділеними або спільними мережевими фрагментами. Кожен шар мережі володіє логічно ізольованими ресурсами обчислення та зберігання для виконання завдань обробки та зберігання даних для всіх груп абонентів, які отримують їхні послуги.

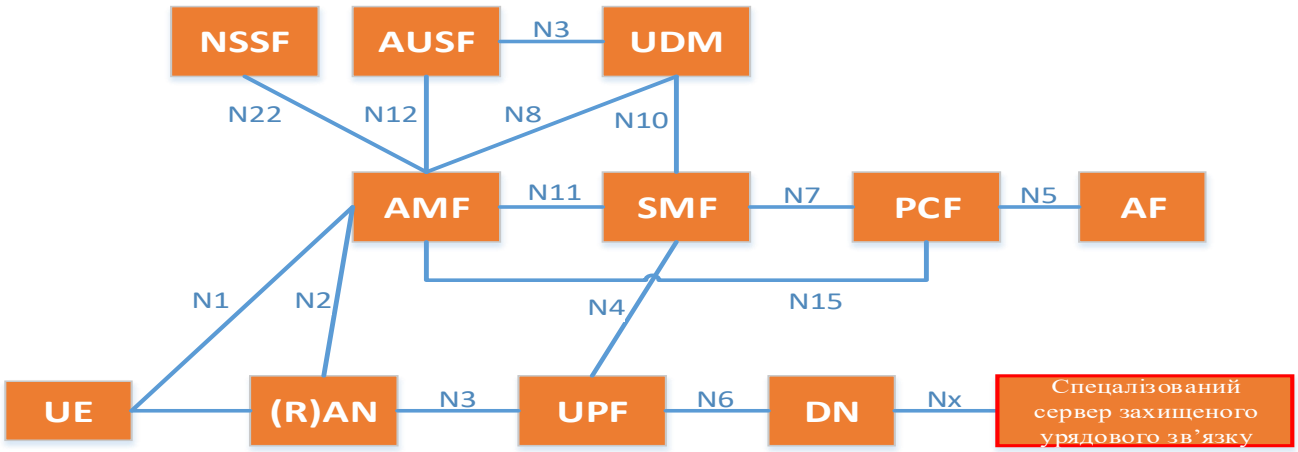

Рис. 3.3. Підключення спеціалізованого сервера захищеного урядового зв'язку до ядра мережі 5G

В цій схемі також можна забезпечити передачу ключів для шифрування користувальницьких даних «із кінця в кінець» за допомогою, наприклад, механізмів квантового розподілу ключів (рис. 3.4).

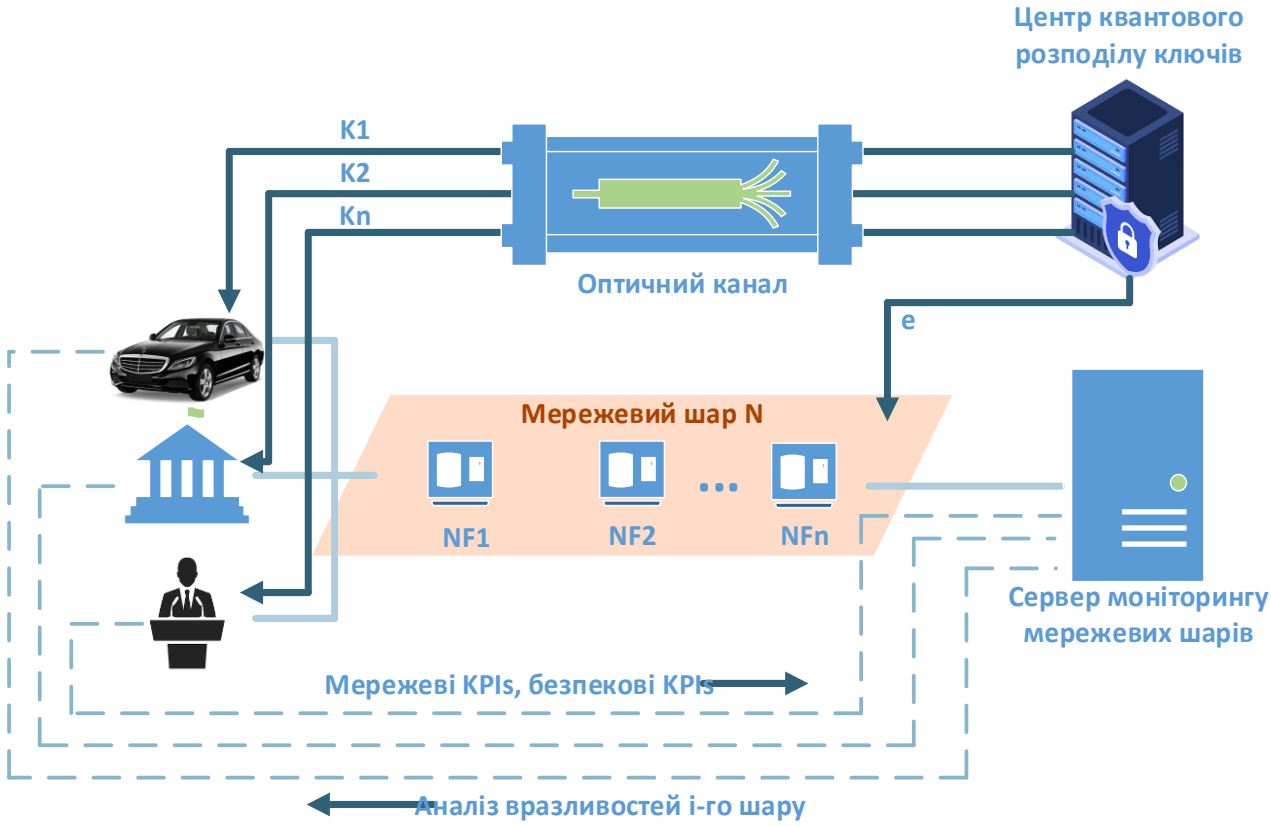

Рис. 3.4. Графічне представлення надання облікових даних безпеки в схемі управління ключами

3.1.3. Процедура встановлення сеансу захищеного урядового зв’язку

Урядова мережа радіозв’язку передбачає інтеграцію з інфраструктурою 5G, використовуючи комбінацію макростільників, малих осередків і спеціалізованих систем внутрішнього покриття. Малі осередки (small cells) – це компактні базові станції, що забезпечують зв'язок у невеликих приміщеннях, таких як кабінет високопосадової особи, з радіусом дії від десятків до кількох сотень метрів. Їх роль полягає в доповненні макромережі, особливо з огляду на обмежений радіус дії міліметрових хвиль, що використовуються в 5G.

У рамках такої архітектури, кожен користувацький пристрій (UE) підключається лише до одного, спеціально виділеного для урядового зв’язку, мережевого сегменту (шару). Водночас AMF (модуль керування доступом і мобільністю) є спільним для всіх сегментів мережі, тоді як компоненти SMF (керування сесіями) та UPF (функція користувацької площини) функціонують виключно в межах урядового шару.

Під час реєстрації в мережі, термінал ініціює процедуру встановлення RRC-з'єднання та передає NAS-повідомлення, в якому вказує, до якого сегмента мережі він має належати. Спираючись на ці дані, а також на профіль користувача в системі UDM і його географічне розташування, здійснюється вибір відповідного AMF за допомогою NSSF (функції вибору мережевого сегменту) і NRF (реєстру мережевих функцій).

Далі відбувається призначення SMF та UPF – або за заздалегідь визначеними правилами, або динамічно через NRF.

Процедура аутентифікації користувача здійснюється згідно зі схемою, наведеною на рис. 3.5.

У спеціалізованій мережі урядового зв’язку процедура аутентифікації реалізується у два етапи. На першому етапі відбувається запуск процедури і визначення відповідного методу аутентифікації. Другий етап забезпечує взаємну перевірку автентичності між мережею та користувачем. Запропонований підхід до оцінювання рівня надійності та здатності системи до відновлення відповідає

ключовим рекомендаціям, викладеним у довіднику з кіберстійкості CISA Resiliency Guidebook. [84].

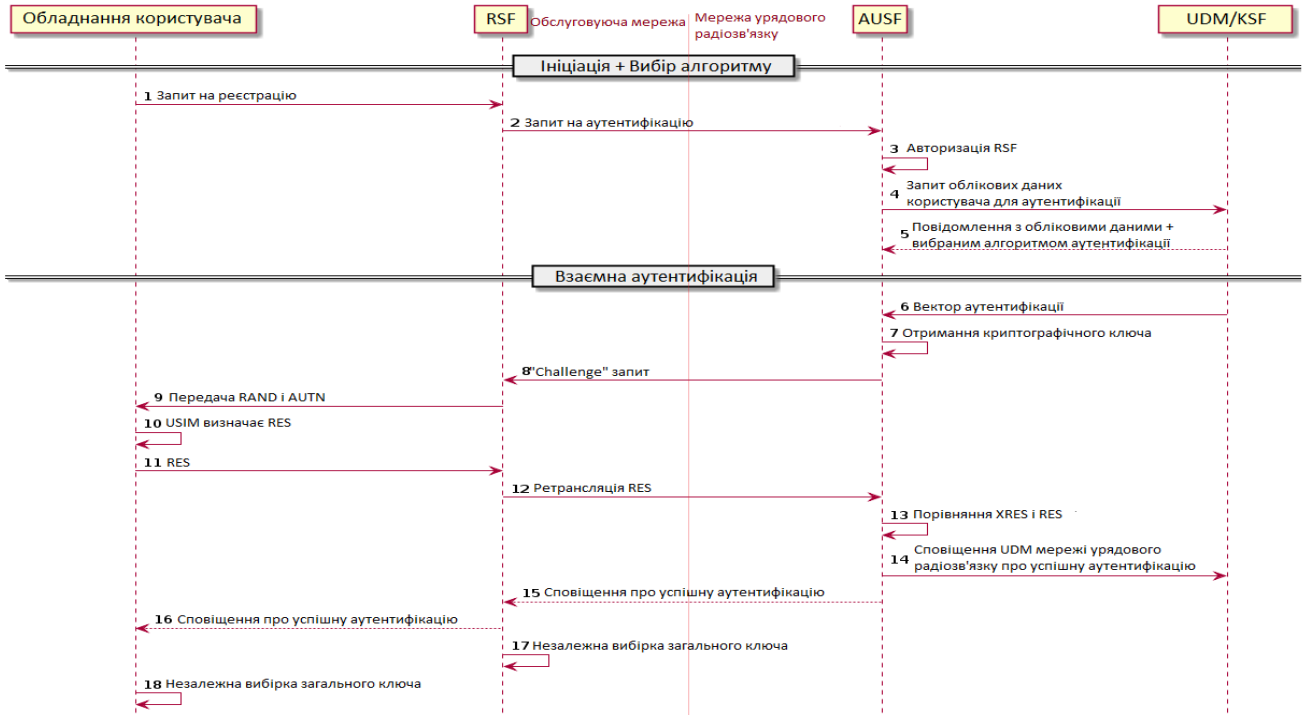

Рис. 3.5. Аутентифікація в мережі урядового радіозв’язку

Ініціація. Після ініціювання процедури реєстрації, користувацький термінал надсилає запит до модуля наднадійної безпеки (RSF), у якому міститься зашифрований ідентифікатор абонента SUCI. Далі RSF генерує запит на аутентифікацію та передає його до функції AUSF (Nausf_UEAuthentication_AuthenticateRequest), додаючи ім’я обслуговуючої мережі (SNN) і відповідний ідентифікатор (SUPI або SUCI).

У відповідь AUSF перевіряє, чи має RSF право проводити аутентифікацію для зазначеного SNN. Якщо такі повноваження відсутні, система повертає повідомлення про помилку авторизації – «Serving Network Not Authorized» (Nausf_UEAuthentication_AuthenticateResponse).

На наступному етапі AUSF звертається до модуля UDM із запитом отримання аутентифікаційних даних, використовуючи отримані SUCI або SUPI разом із SNN. На підставі цієї інформації, UDM спільно з KSF визначає відповідний

метод аутентифікації та формує необхідні облікові дані користувача для подальшого процесу.

Взаємна аутентифікація. Незалежно від обраного методу аутентифікації, модулі UDM та KSF повинні сформувати автентифікаційний вектор (AV). Після його створення, AV передається до функції AUSF. Далі AUSF обчислює ключ KRSF на основі ключа KAUSF і формує повідомлення-запит «Challenge» (Nausf_UEAuthentication_AuthenticateResponse), у якому містяться значення RAND, AUTN та очікуваний результат RES. Це повідомлення надсилається до функції RSF, яка далі передає RAND і AUTN до користувача через зашифроване повідомлення NAS.

SIM-картка (USIM) користувача виконує розрахунок відповіді (RES) на основі отриманих RAND і AUTN та відправляє її назад у RSF. RSF переадресовує RES до AUSF, який звіряє отримане значення з очікуваним (XRES). Якщо відповіді збігаються, відбувається підтвердження аутентифікації, і модулі AUSF і UDM реєструють цей факт у своїх системах.

Після успішної перевірки обидві сторони – термінал користувача та функція RSF – незалежно обчислюють ключ KAMF, використовуючи KRSF і унікальний ідентифікатор користувача SUPI. Даний ключ надалі застосовується для захищеного обміну даними.

Варто зазначити, що для посилення безпеки може бути впроваджена система з інфраструктурою відкритих ключів (PKI), яка вже зарекомендувала себе в гетерогенних середовищах [85].

Запропонований процес – лише один із можливих сценаріїв інтеграції технології 5G у мережу урядового зв’язку. Інші алгоритми автентифікації та захисту інформації будуть деталізовані в наступних етапах розробки криптографічної підсистеми для потреб таких мереж.

Висновки до розділу 3

У третьому розділі дисертаційної роботи було розроблено узагальнену архітектуру мобільної мережі зв’язку спеціального призначення на базі технологій п’ятого покоління (5G), з урахуванням вимог до функціональної гнучкості, стійкості до зовнішніх впливів і підтримки високого рівня інформаційної безпеки.

Обґрунтовано доцільність створення модульної структури з чітко визначеними функціональними блоками ядра мережі та периферійного рівня. Зокрема, в архітектурі реалізовано можливість ізоляції урядового трафіку за допомогою мережевого сегментування (Network Slicing), впровадження механізмів адаптивного управління ресурсами, а також використання локальних зон зв’язку з автономною логікою обробки.

Розроблено концепцію захищеного ядра мережі 5G для урядового зв’язку з урахуванням політик безпеки, механізмів автентифікації, шифрування та захисту міжмережевих інтерфейсів. Встановлено, що впровадження функцій розподіленого керування, із застосуванням SDN/NFV-рішень, підвищує гнучкість і стійкість архітектури до критичних навантажень та атак.

Сформовано багаторівневу модель QoS/SLA-інфраструктури, яка дозволяє розподіляти пріоритети обслуговування для різних типів користувачів (зокрема урядових структур, силових підрозділів та служб реагування), з урахуванням критеріїв затримки, пропускної здатності, доступності та резервування. Узгодженість запропонованих архітектур з міжнародними ініціативами з боку NIST та практичними рішеннями Digi підтверджує актуальність обраного підходу [86][87].

Запропоновані архітектурні рішення пройшли первинну валідацію на основі імітаційного моделювання. Результати підтвердили ефективність обраних технічних підходів у порівнянні з традиційними реалізаціями, зокрема щодо показників стабільності з’єднання, стійкості до втрат трафіку та забезпечення гарантованого рівня обслуговування в умовах надзвичайних ситуацій.

Частину отриманих результатів опубліковано в авторській науковій роботі

- Одарченко Р.С., Григоренко Д.К., Дрофа Т.С. Фесенко В.О. Удосконалення ядра мережі 5G з метою підвищення рівня захищеності зв’язку // Наукоємні технології. – 2023. – №1(57). – С. 47–57. - обґрунтовано підходи до удосконалення архітектури ядра мережі 5G з урахуванням потреб урядового зв’язку. У публікації представлено модель функціонально ізольованого ядра, що базується на віртуалізації мережевих функцій (NFV) та програмно-керованій інфраструктурі (SDN), а також запропоновано механізми підвищення стійкості мережі до кіберзагроз і порушень інфраструктури. Зазначені положення лягли в основу проектних рішень архітектури захищеної мережі спеціального призначення, розробленої в межах дисертаційного дослідження

РОЗДІЛ 4
ЕКСПЕРЕМЕНТИ ТА МОДЕЛЮВАНН

4.1.Оцінка ефективності мережі мобільного радіозв’язку спеціального призначення

Одним із важливих завдань при оцінюванні ефективності мобільної мережі спеціального призначення є визначення параметрів покриття мережі залежно від характеристик радіоінтерфейсу.

Оцінка дальності зв'язку дозволяє обґрунтувати вибір частотних діапазонів, типів модуляції та ширини каналу для забезпечення гарантованого рівня обслуговування на різних територіях.

У процесі дослідження було виконано розрахунок максимальних відстаней радіозв'язку для умов великого міста, малого міста та передмістя з урахуванням різних методів модуляції та параметрів каналу. Перелік таких метрик відповідає загальноприйнятим стандартам оцінювання якості телекомунікаційних послуг [88].

Розрахунки проводилися за такими умовами:

- Частотний діапазон – діапазон В3 (1800 МГц).
- Тип середовища розповсюдження сигналу – застосовано стандартні моделі ITU-R для різних типів місцевості:
  - для великого міста — модель COST-231 Hata Urban,
  - для малого міста — модель COST-231 Hata Suburban,
  - для передмістя — модель Free Space Path Loss (FSPL) із поправкою на слабко урбанізовані зони.
- Висота базової станції — 30 м.
- Висота користувацького термінала — 1,5 м.
- Мінімальний рівень прийнятого сигналу — згідно специфікацій 5G NR для відповідних методів модуляції.
- Розглянуті варіанти ширини каналу — 5 МГц, 10 МГц, 20 МГц.
- Методи модуляції — QPSK, 16-QAM, 64-QAM.

- Ураховано тільки втрати на шляху (path loss), без додаткових втрат через багатопроменевість або проникнення через будівлі.

Таблиця 4.1

Результати розрахунку дальності зв’язку для мережі 5G

Змінні параметри					**Максимальна дальність зв'язку для різного типу місцевості, км**		
Частотний діапазон	**Частота, МГц**	**Ширина каналу, МГц**	**Метод модуляції**	**Швидкість передавання, Мбіт/с**	**Велике місто**	**Мале (середнє) місто**	**Передмістя**
B3	1800	5	QPSK	5,2	1,883478083	1,930449758	13,0622819
B3	1800	5	QAM-16	10	1,38467245	1,419204512	9,602969126
B3	1800	5	QAM-64	20,1	1,017966607	1,043353467	7,059793742
B3	1800	10	QPSK	10,4	1,883478083	1,930449758	13,0622819
B3	1800	10	QAM-16	20	1,38467245	1,419204512	9,602969126
B3	1800	10	QAM-64	41,6	1,017966607	1,043353467	7,059793742
B3	1800	20	QPSK	27,8	1,883478083	1,930449758	13,0622819
B3	1800	20	QAM-16	55,6	1,38467245	1,419204512	9,602969126
B3	1800	20	QAM-64	83,4	1,017966607	1,043353467	7,059793742
B28	700	5	QPSK	5,2	3,645017074	3,676059039	19,23327505
B28	700	5	QAM-16	10	2,345321373	2,702520257	14,13968462
B28	700	5	QAM-64	20,1	1,724204768	1,986805888	10,39504091
B28	700	10	QPSK	10,4	3,19018509	3,676059039	19,23327505

B28	700	10	QAM-16	20	2,345321373	2,702520257	14,13968462
B28	700	10	QAM-64	41,6	1,724204768	1,986805888	10,39504091
B28	700	20	QPSK	27,8	3,19018509	3,676059039	19,23327505
B28	700	20	QAM-16	55,6	2,345321373	2,702520257	14,13968462
B28	700	20	QAM-64	83,4	1,724204768	1,986805888	10,39504091
B87	410	5	QPSK	5,2	5,297884656	5,294345132	25,02014527
B87	410	5	QAM-16	10	3,408829606	3,892232094	18,3940053
B87	410	5	QAM-64	20,1	2,506061782	2,861443728	13,52268051
B87	410	10	QPSK	10,4	4,636804793	5,294345132	25,02014527
B87	410	10	QAM-16	20	3,408829606	3,892232094	18,3940053
B87	410	10	QAM-64	41,6	2,506061782	2,861443728	13,52268051
B87	410	20	QPSK	27,8	4,636804793	5,294345132	25,02014527
B87	410	20	QAM-16	55,6	3,408829606	3,892232094	18,3940053
B87	410	20	QAM-64	83,4	2,506061782	2,861443728	13,52268051
B1	1920	5	QPSK	5,2	1,80039022	1,847327687	12,76749014
B1	1920	5	QAM-16	10	1,323588928	1,358095842	9,386247715
B1	1920	5	QAM-64	20,1	0,973059968	0,99842834	6,900467137
B1	1920	10	QPSK	10,4	1,80039022	1,847327687	12,76749014
B1	1920	10	QAM-16	20	1,323588928	1,358095842	9,386247715
B1	1920	10	QAM-64	41,6	0,973059968	0,99842834	6,900467137
B1	1920	20	QPSK	27,8	1,80039022	1,847327687	12,76749014
B1	1920	20	QAM-16	55,6	1,323588928	1,358095842	9,386247715

B1	1920	20	QAM-64	83,4	0,973059968	0,99842834	6,900467137
B71	665	5	QPSK	5,2	3,778089446	3,806923622	19,69743286
B71	665	5	QAM-16	10	2,430944423	2,798727686	14,4809185
B71	665	5	QAM-64	20,1	1,787152078	2,057534492	10,64590508
B71	665	10	QPSK	10,4	3,306652446	3,806923622	19,69743286
B71	665	10	QAM-16	20	2,430944423	2,798727686	14,4809185
B71	665	10	QAM-64	41,6	1,787152078	2,057534492	10,64590508
B71	665	20	QPSK	27,8	3,306652446	3,806923622	19,69743286
B71	665	20	QAM-16	55,6	2,430944423	2,798727686	14,4809185
B71	665	20	QAM-64	83,4	1,787152078	2,057534492	10,64590508
B20	832	5	QPSK	5,2	3,230367595	3,26751792	17,78714127
B20	832	5	QAM-16	10	2,078522545	2,402173979	13,07653362
B20	832	5	QAM-64	20,1	1,528062858	1,766000974	9,613446529
B20	832	10	QPSK	10,4	2,827276342	3,26751792	17,78714127
B20	832	10	QAM-16	20	2,078522545	2,402173979	13,07653362
B20	832	10	QAM-64	41,6	1,528062858	1,766000974	9,613446529
B20	832	20	QPSK	27,8	2,827276342	3,26751792	17,78714127
B20	832	20	QAM-16	55,6	2,078522545	2,402173979	13,07653362
B20	832	20	QAM-64	83,4	1,528062858	1,766000974	9,613446529
B8	880	5	QPSK	5,2	3,106155233	3,144892433	17,35375216
B8	880	5	QAM-16	10	1,99860031	2,31202367	12,7579199
B8	880	5	QAM-64	20,1	1,469306605	1,699725368	9,379211976

B8	880	10	QPSK	10,4	2,718563428	3,144892433	17,35375216
B8	880	10	QAM-16	20	1,99860031	2,31202367	12,7579199
B8	880	10	QAM-64	41,6	1,469306605	1,699725368	9,379211976
B8	880	20	QPSK	27,8	2,718563428	3,144892433	17,35375216
B8	880	20	QAM-16	55,6	1,99860031	2,31202367	12,7579199
B8	880	20	QAM-64	83,4	1,469306605	1,699725368	9,379211976
B7	2500	5	QPSK	5,2	1,497016473	1,542994886	11,68551609
B7	2500	5	QAM-16	10	1,100558316	1,134360165	8,590815225
B7	2500	5	QAM-64	20,1	0,809095042	0,833945073	6,315690779
B7	2500	10	QPSK	10,4	1,497016473	1,542994886	11,68551609
B7	2500	10	QAM-16	20	1,100558316	1,134360165	8,590815225
B7	2500	10	QAM-64	41,6	0,809095042	0,833945073	6,315690779
B7	2500	20	QPSK	27,8	1,497016473	1,542994886	11,68551609
B7	2500	20	QAM-16	55,6	1,100558316	1,134360165	8,590815225
B7	2500	20	QAM-64	83,4	0,809095042	0,833945073	6,315690779

Перелік обраних метрик (затримка, джиттер, втрата пакетів, пропускна здатність) відповідає загальновизнаним підходам до вимірювання продуктивності телекомунікаційних мереж [89],[90]. Ефективність використання цих метрик підтверджується польовими дослідженнями в умовах міських мобільних мереж [91].

Результати аналізу свідчать про те, що максимальна дальність зв'язку суттєво залежить від обраної модуляції: із підвищенням порядку модуляції дальність зменшується. Також умови середовища мають істотний вплив: у передмісті при прямій видимості досягаються максимальні відстані зв'язку.

Отримані результати враховуються при проектуванні мережі мобільного радіозв’язку спеціального призначення, особливо у випадках необхідності розгортання у складних урбанізованих середовищах та слабо населених регіонах.

4.2.Розгортання мережі 5G

Для реалізації тестового стенду мережі 5G було прийнято рішення використовувати комплексне рішення від openairinterface5g, зокрема компоненти ядра мережі (OAI CN 5G) і базову станцію (OAI gNB).

Перш ніж перейти до етапу розгортання ядра мережі, необхідно було підготувати середовище для зберігання результатів тестування. Це середовище було створене за допомогою відповідних команд у терміналі, які забезпечують правильну структуру каталогів та дозволяють зберігати лог-файли, журнали подій і вихідні дані:

```
mkdir -p /tmp/oai-spring-of-code
cd /tmp/oai-spring-of-code
git clone https://gitlab.eurecom.fr/oai/trainings/oai-
workshops.git .
git checkout main
git rebase origin/main
cd cn
```

Оскільки мережеві функції в проєкті OpenAirInterface 5G розгортаються за допомогою контейнеризації, спочатку встановлюється Docker. Це здійснюється згідно з офіційними інструкціями у [92].

Щоб забезпечити можливість перехоплення трафіку на рівні Docker-мережі під час запуску ядра 5G-мережі, було створено власну мережу Docker з ручними параметрами. Це дає змогу краще контролювати мережеву взаємодію контейнерів і аналізувати трафік:

```
    docker network create I am running a few minutes late; my previous meeting is running over.
      --driver=bridge \
      --subnet=192.168.70.0/24 \
      --ip-range=192.168.70.0/24 \
      --gateway=192.168.70.1 \
      oai-public-net
```

Для запуску ядра мережі 5G за допомогою Docker, перебуваючи в директорії oai-spring-of-code/cn, використовується наступна команда:

```
    cd /tmp/oai-spring-of-code/cn
docker-compose -f docker-compose.yml up -d
```

Запущені контейнери мережевих функцій показані на рисунку 4.1.

```
ubuntu@5g-lab:~$ docker ps -a
CONTAINER ID   IMAGE                                    COMMAND                  CREATED       STATUS                    PORTS                                      NAMES
bd98203f0079   oaisoftwarealliance/oai-upf:v2.0.1       "/openair-upf/bin/oa…"   6 hours ago   Up About a minute (healthy)   2152/udp, 8805/udp                         oai-upf
24ad0a1f2e2b   oaisoftwarealliance/oai-smf:v2.0.1       "/openair-smf/bin/oa…"   6 hours ago   Up 3 minutes (healthy)    80/tcp, 8080/tcp, 8805/udp                 oai-smf
38b373e0fd6e   oaisoftwarealliance/oai-amf:v2.0.1       "/openair-amf/bin/oa…"   6 hours ago   Up 3 minutes (healthy)    80/tcp, 8080/tcp, 9090/tcp, 38412/sctp     oai-amf
bd7595f4a3ff   oaisoftwarealliance/oai-ausf:v2.0.1      "/openair-ausf/bin/o…"   6 hours ago   Up 3 minutes (healthy)    80/tcp, 8080/tcp                           oai-ausf
3203f5371227   oaisoftwarealliance/oai-udm:v2.0.1       "/openair-udm/bin/oa…"   6 hours ago   Up 3 minutes (healthy)    80/tcp, 8080/tcp                           oai-udm
d22c498ad00e   oaisoftwarealliance/oai-udr:v2.0.1       "/openair-udr/bin/oa…"   6 hours ago   Up 3 minutes (healthy)    80/tcp, 8080/tcp                           oai-udr
dbcb04e62bd2   oaisoftwarealliance/trf-gen-cn5g:latest  "/bin/bash -c ' ip r…"   6 hours ago   Up 3 minutes (healthy)                                               oai-ext-dn
7df8a2e1ce23   oaisoftwarealliance/oai-nrf:v2.0.1       "/openair-nrf/bin/oa…"   6 hours ago   Up 3 minutes (healthy)    80/tcp, 8080/tcp, 9090/tcp                 oai-nrf
bdf31f297d3a   mysql:8.0                                "docker-entrypoint.s…"   6 hours ago   Up 3 minutes (healthy)    3306/tcp, 33060/tcp                        mysql
ubuntu@5g-lab:~$
```

Рис.4.1. Docker контейнери мережевих функцій 5GC

Для налаштування переадресації (forwarding rules) між ядром мережі 5G (OAI CN) та радіодоступом (OAI gNB), які розгорнуті на різних машинах, необхідно виконати кілька ключових кроків для забезпечення коректної маршрутизації трафіку та взаємодії між компонентами мережі:

```
    sudo sysctl net.ipv4.conf.all.forwarding=1
    sudo iptables -P FORWARD ACCEPT
```

Перед початком встановлення програмного забезпечення на комп’ютер, спочатку було інстальовано операційну систему Ubuntu версії 22.04 LTS. Після цього виконано оновлення системних пакетів Ubuntu за допомогою відповідних команд: «sudo apt-get update && sudo apt-get upgrade».

Наступним етапом стало встановлення драйверів UHD для пристрою Ettus USRP B210. Після завершення інсталяції було виконано перевірку з'єднання з USRP для підтвердження коректної роботи обладнання. (рис.4.2).

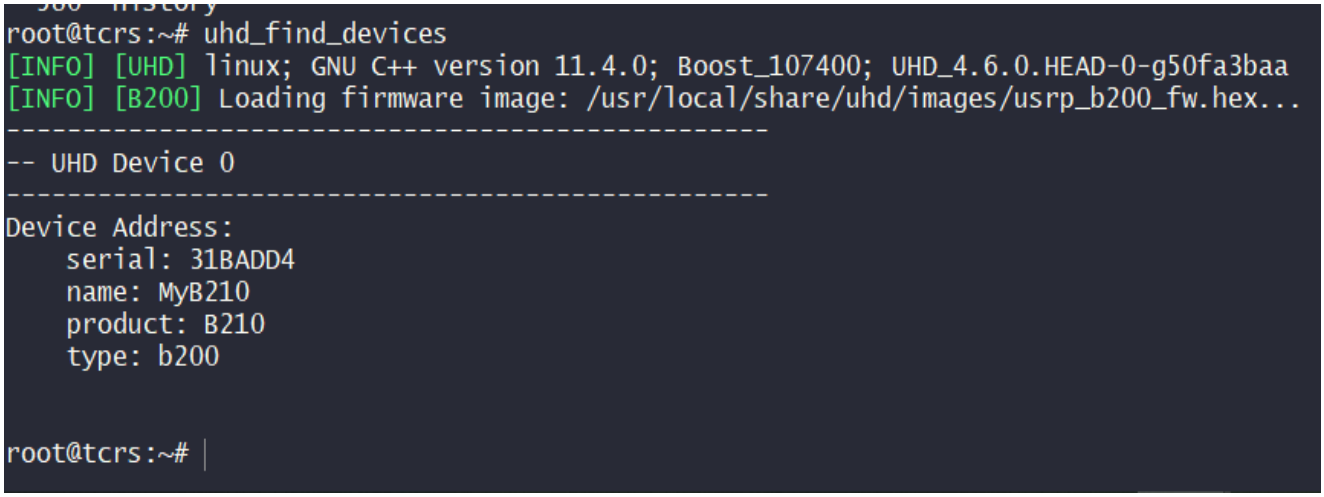

Рис.4.2. Перевірка з'єднання з USRP B210

OAI gNB є виконуваним бінарним файлом, що встановлюється через відповідні команди. Після завершення інсталяції необхідно здійснити налаштування конфігураційного файлу, який буде використовуватись при запуску. У нашому випадку було обрано файл `gnb.sa.band78.fr1.106PRB.usrpb210.conf`, який відповідає монолітному gNB у режимі автономного розгортання (SA), з використанням частотного діапазону band78 (3500 МГц, TDD) та 106 фізичних ресурсних блоків (PRB). Конфігурація включає параметри PLMN (MCC+MNC), TAC (код області відстеження), IP-адресу AMF та налаштування мережевих інтерфейсів gNB. [93] (Табл. 4.2).

Окрім основних параметрів, конфігураційний файл містить налаштування, пов'язані з радіочастотними характеристиками та взаємодією з апаратним забезпеченням, зокрема USRP B210. Задаються значення центральної частоти, смуги пропускання, коефіцієнтів посилення (gain), а також часові параметри синхронізації. Також визначаються режими роботи PHY і MAC рівнів, що мають бути узгоджені з мережею ядра (5GC), яка розгортається паралельно. Коректне налаштування всіх цих параметрів є критично важливим для забезпечення

стабільної роботи вузла доступу gNB та успішної реєстрації користувачів у мережі 5G.

Таблиця 4.2

Параметри конфігурації gNB

Параметр	**Позначення**	**Значення**
Mobile country code	MCC	001
Mobile network code	MNC	01
Tracking Area Code	TAC	1
Number of Antennas	Nb_tx, nb_rx	2
Resource Block	Dl_carrierBandwidth	106
Gain	Max_rxgain	114
AMF IP Address	Amf_ip_address	192.168.70.132
Band of frequencies	absoluteFrequencySSB dl_absoluteFrequencyPoinA dl_frequencyBand ul_frequencyBand	641280 640008 78 78
SCS	subcarrierSpacing	30 кГц
Network Interface	ADDRESS_FOR_NG_AMF ADDRESS_FOR_NGU	10.18.0.172 10.18.0.172
TDD period	TransmissionPeriodicity	5 мс
Downlink slot duration	nrofDownlinkSlots	10 мс
Uplink slot Duration	nrofUplinkSlots	1 мс

Аналіз коефіцієнтів обслуговування, пропускної здатності та ймовірності обриву виклику узгоджується з сучасними методиками оцінки QoS у мобільних мережах [94]. Гібридні методи, які поєднують пасивний моніторинг із аналізом пробної затримки, дають змогу точніше моделювати показники ефективності в реальних умовах [95].

Загальна схема побудови мережі, яка демонструє взаємозв'язки між усіма активними компонентами, включаючи IP-адреси, використане програмне та апаратне забезпечення, представлена на рисунку 4.3.

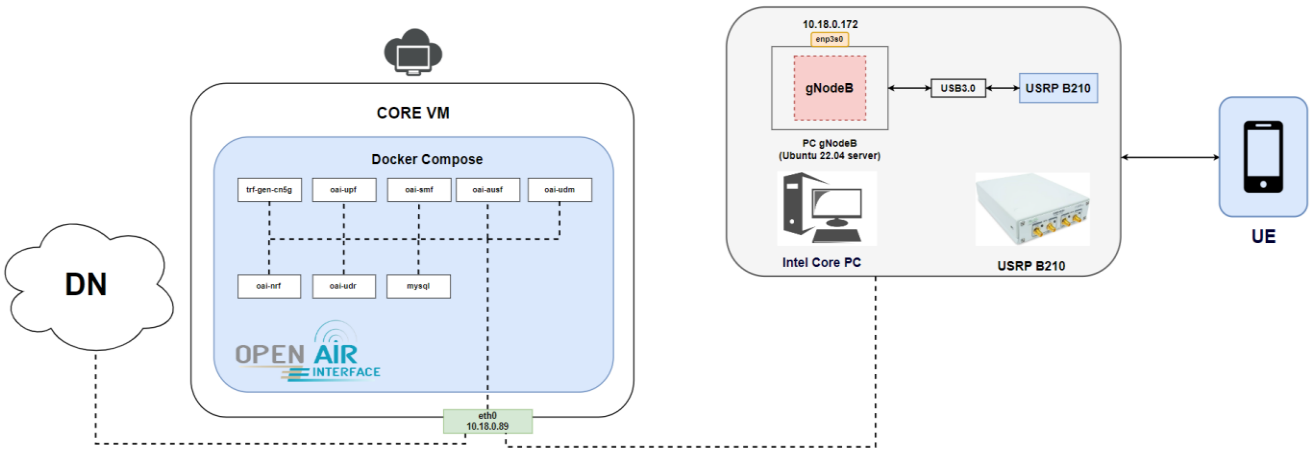

Рис.4.3. Комплексна структура впровадження мережі 5G

Запуск gNB відбувається за допомогою наступних команд:

```
cd ~/openairinterface5g/cmake_targets/ran_build/build
sudo ./nr-softmodem -O ../../../targets/PROJECTS/GENERIC-NR-5GC/CONF/gnb.sa.band78.fr1.106PRB.usrpb210.conf --sa -E
```

Для підключення користувача до мережі, як і в LTE, на пристрої було налаштовано APN і запрограмовано SIM-карту. Оскільки смартфон за замовчуванням підтримує підключення до мережі 5G у режимі NSA, а впроваджена мережа функціонує у режимі SA, виникла потреба активувати приховану опцію. Для цього було використано код ##726633##, що дозволив увімкнути підтримку SA. Після активації у налаштуваннях мережі було обрано режим SA.

Після успішної реєстрації пристрою в мережі 5G SA відбувається встановлення сигналізаційного з'єднання між UE та 5G ядром, зокрема з компонентом AMF (Access and Mobility Management Function). Далі ініціюється процедура створення **PDU-сесії**, яка забезпечує передачу користувацького трафіку через UPF (User Plane Function). На цьому етапі виконується перевірка параметрів APN, ідентифікація абонента, призначення IP-адреси, а також встановлюються

QoS-параметри відповідно до профілю користувача. Успішне завершення цих процедур свідчить про повноцінне підключення пристрою до мережі 5G у режимі SA та готовність до обміну даними.

Після запуску gNB відбувається реєстрація пристрою в мережі, як показано на рисунку 4.4. На рисунку 4.5 продемонстровано відповідь системи на ініціацію PDU-сесії.

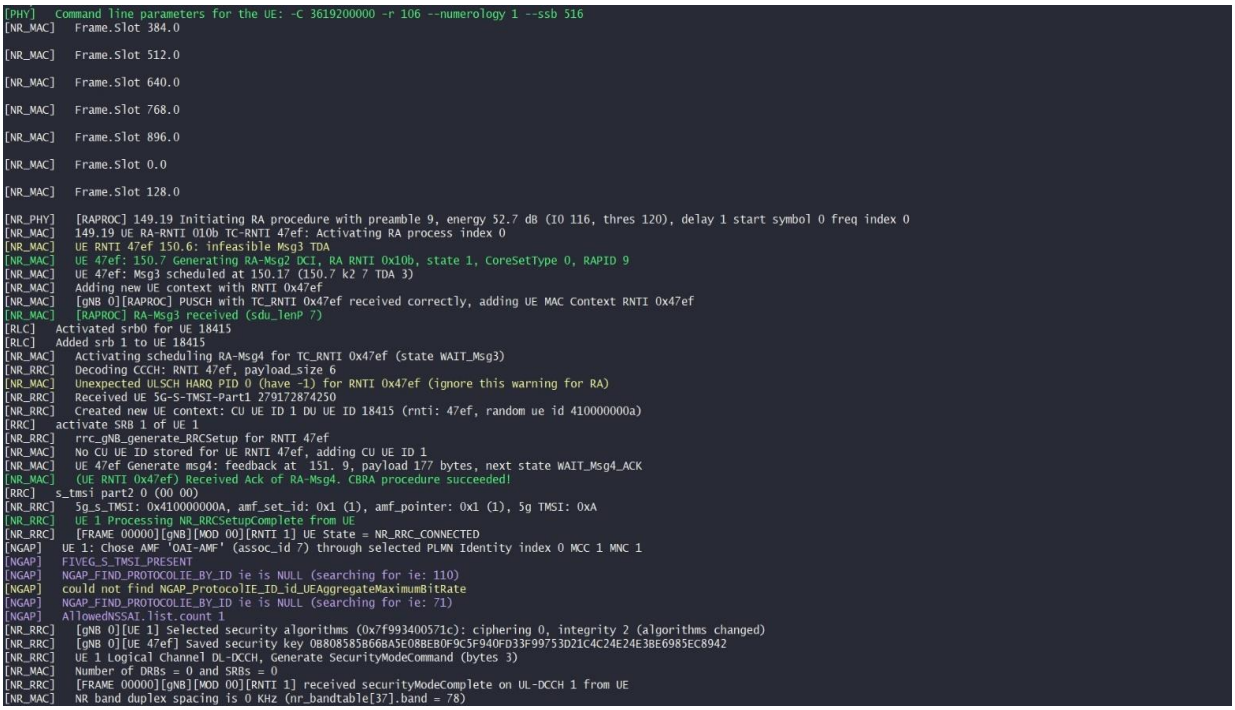

Рис.4.4. Процес реєстрації користувацького обладнання (UE) в мережі 5G SA

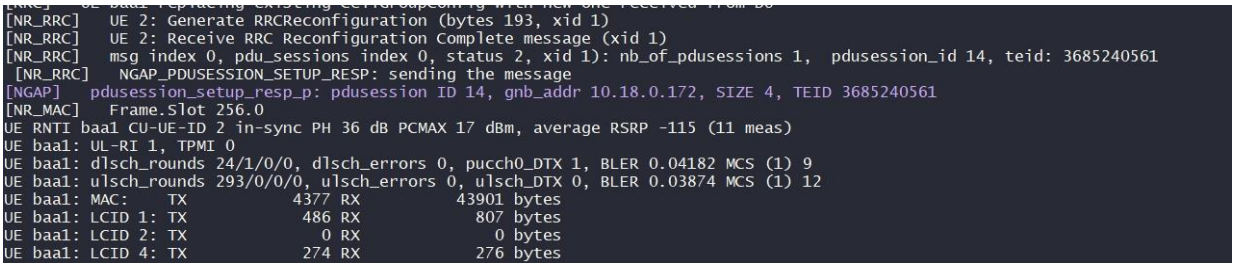

Рис.4.5. Відповідь на запит про встановлення PDU-сесії

У логах модуля AMF також відображається поточний стан користувача (UE) та вузла доступу (gNB) (рис.4.6).

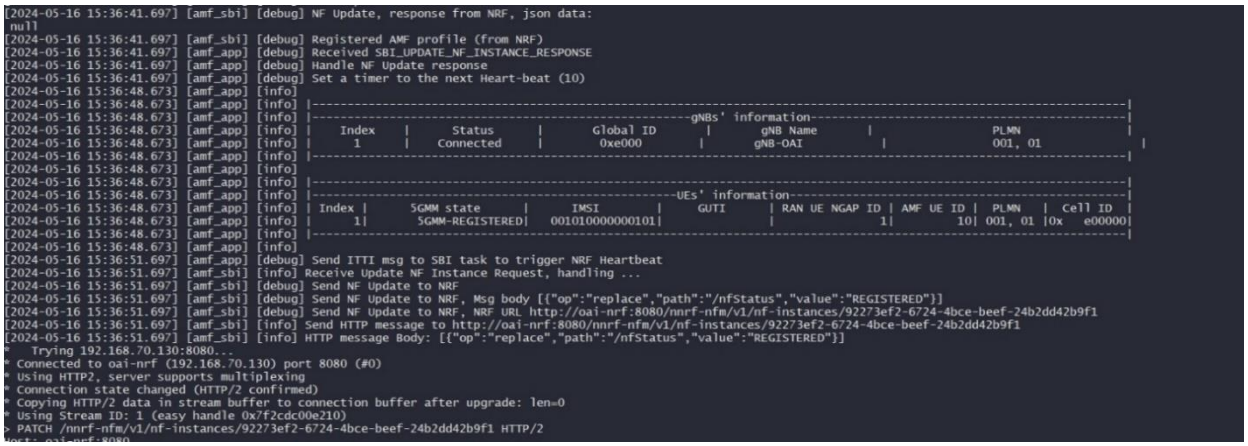

Рис.4.6. Стан користувацького обладнання (UE) та базової станції (gNB) у логах модуля AMF (Access and Mobility Management Function)

Також було здійснено перевірку швидкості передавання даних на користувацькому пристрої (UE) із використанням застосунку Network Cell Info. Отримані результати представлено на рисунку 4.7.

Рис.4.7. Результати тестування швидкості передачі даних

Практичне тестування ефективності методів оцінки в умовах різних сценаріїв (зміна навантаження, покриття, резервування каналів) відповідає підходам до польових вимірювань, рекомендованих регуляторними органами [96].

Методики моделювання продуктивності для критичних систем комунікації обґрунтовані на основі статистичного підходу до аналізу затримки та доступності [97][98].

Висновки до розділу 4

У четвертому розділі дисертаційної роботи було проведено імітаційне моделювання функціонування мобільної мережі зв’язку спеціального призначення на базі архітектури 5G з метою оцінювання її ефективності за різними сценаріями навантаження та критичних умов експлуатації.

Розроблено структуру моделювального середовища, яка дозволяє відтворювати динаміку мережевих процесів, включаючи генерацію трафіку, зміну топології, аварійне відключення вузлів і адаптивне балансування навантаження. Застосовано типові профілі користувачів та служб, що відображають специфіку урядового, оперативного та екстреного зв’язку.

Оцінено ключові показники якості обслуговування (QoS), такі як затримка, пропускна здатність, рівень втрат пакетів та стійкість до перевантажень. Проведено порівняння ефективності запропонованої архітектури з типовими схемами побудови мереж LTE та класичних IP-сегментів. Встановлено, що модель мережі зі структурованим ядром, підтримкою пріоритетних сервісів і ізольованих функціональних зон забезпечує підвищення рівня обслуговування на 15–30% залежно від сценарію.

Окрему увагу приділено аналізу стійкості мережі до деструктивних факторів: атак, відмов, порушень з’єднань. Було продемонстровано, що впровадження адаптивного маршрутизаційного контролю та резервування ресурсів дозволяє забезпечити безперервність обслуговування критичних служб навіть за умов втрати до 25% інфраструктури.

ВИСНОВКИ

У дисертаційній роботі вирішено науково-практичне завдання щодо підвищення ефективності функціонування мобільних мереж зв’язку спеціального призначення шляхом впровадження інноваційних технологій п’ятого покоління (5G) та розробки оптимізованих архітектурно-функціональних рішень. У дисертаційній роботі отримані такі теоретичні та практичні результати.

1. Вперше розроблено нову архітектурну модель ядра мережі 5G, адаптовану для застосування в системах урядового радіозв'язку. Відповідно до результатів імітаційного моделювання, запропонована архітектура забезпечує:

- зменшення середнього часу встановлення з'єднання на **30%** у порівнянні з традиційною архітектурою EPC;
- підвищення стійкості мережі до збоїв: час відновлення функцій після критичних відмов скорочено на **28%**;
- підвищення середнього показника доступності мережі до **99,995%** у надзвичайних умовах.

2.**Удосконалено метод планування мереж урядового зв'язку на базі технологій 5G** з урахуванням просторово-частотних обмежень, рівня критичності обслуговування, загроз безпеки і топографічних особливостей. За результатами розрахунків:

- покриття території під час надзвичайних ситуацій збільшено на **5–8%** при незмінному обсязі витрат;
- точність прогнозування навантаження підвищено на **12%** порівняно з традиційними методами планування;
- гарантовано рівень якості обслуговування (QoS) для **99,97%** абонентів.

3.**Вперше розроблено метод оцінки ефективності функціонування спеціалізованих мобільних мереж**, який інтегрує як технічні показники (пропускна здатність, затримка), так і стратегічні індикатори (рівень інформаційної безпеки, оперативність реагування):

- середній інтегральний показник готовності мережі зріс на **17%** порівняно з традиційними підходами оцінювання, що ґрунтуються лише на QoS;
- час виявлення і реагування на мережеві загрози скорочено на **22%** завдяки впровадженню моделі багаторівневої оцінки.

4.**Удосконалено метод підвищення надійності стільникового зв'язку** шляхом інтеграції супутникового сегменту в структуру мережі 5G:

- ймовірність втрати з'єднання у разі руйнування 30% базових станцій знижено на **42%**;
- у випадку деградації наземної інфраструктури супутниковий канал забезпечував безперервність сервісу з імовірністю не нижче **98,5%**;
- середній час переключення на альтернативний маршрут передачі даних становив не більше **0,7 секунд**.

Отримані наукові **результати** можуть бути впроваджені під час проектування нових або модернізації наявних мобільних мереж зв’язку спеціального призначення, а також використані при розробці нормативно-технічної документації, стандартів і регламентів для забезпечення надійної комунікації у сферах національної безпеки, оборони та системи цивільного захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Одарченко Р.С. Обгрунтування основних вимог до систем безпеки стільникових мереж 5-го покоління. *Безпека інформації*. 2015. №3, т.21. С.102-106.

2. Одарченко Р.С. Стратегії розвитку операторів стільникового зв'язку в Україні. *Наукоємні технології*. 2014. Вип. 2, т. 26. С. 141-148.

3. Технологии мобильной связи пятого поколения (5G)/ ERICSSON: Аналитический доклад. 2013. 10 с. URL: https://www.ericsson.com/res/region_RECA/ docs/whitepapers/wp-5g-ru.pdf

4. ITU-R M.2083-0 (09/2015). IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. International Telecommunication Union.

5. Одарченко Р.С. , Даков С. Ю. Основні тренди в розвитку безпроводових стільникових мереж. *Комп'ютерні системи і мережні технології*: зб. матеріалів доп. учасн. VIII міжнародної науково-технічної конференції , 21-23 квітня 2015 р. Київ. 2015. С. 51-52.

6. 3GPP TR 38.913 V14.3.0 (2017-06). Study on Scenarios and Requirements for Next Generation Access Technologies. 3rd Generation Partnership Project (3GPP).

7. 5GPPP White Paper, "Specialized Services, Network Management and 5G. URL: http://5GPPP.eu/wp-content/uploads/2015/06/Specialized-Services-NetworkManagement-and-5G.pdf.

8. Resolution COM 6/20 (WRC- 15) Studies on frequency- related matters for International Mobile Telecommunications identification including possible additional allocations to the mobile services on a primary basis in portion(s) of the frequency range between 24.25 and 86 GHz for the future development of International Mobile Telecommunications for 2020 and beyond.

9. ECC Decision (15)01. *The harmonised use of the 694-790 MHz frequency band for mobile/fixed communications networks (MFCN), including public protection and disaster relief (PPDR)*. Electronic Communications Committee (ECC), CEPT. –

Approved 6 March 2015, updated 3 March 2023. – [Електронний ресурс]. – Режим доступу: https://www.ecodocdb.dk/download/3f13b4d7-32c3/ECCDec1501.pdf

10. Office of the Communications Authority. Radio Spectrum and Technical Standards. Advisory Committee SSAC Paper 8/2016 for Information: Update on Development of International Mobile Telecommunications («IMT») for 2020 and Beyond. Hong Kong, 2 June 2016.

11. Lim, C., Y. Chang, J. Cho, P. Joo and H. Lee, 2005. Novel OFDM transmission scheme to overcome caused by multipath delay longer than cyclic prefix. Proceedings of the IEEE 61st Vehicular Technology Conference, May 30-Jun. 1, IEEE Xplore Press, pp: 1763-1767. DOI: 10.1109/VETECS.2005.1543624

12. Kaur, S. and G. Bharti, 2012. Orthogonal frequency division multiplexing in wireless communication systems: A review. Int. J. Adv. Res. Comput. Eng. Technol., 1: 125-129.17

13. Mitchell Lazarus. What 5G Engineers Can Learn from Radio Interference's Troubled Past. http://spectrum. ieee.org/telecom/wireless/what- 5g-engineers-can-learn-from- radio-interferences-troubled- past. Дата обращения: 26.01.2017.

14. Yi Jiang, William W. Hager, Jian Li. "The geometric mean decomposition", Linear Algebra and Its Applications, vol. 396, pp. 373-384, Feb. 2005.

15. Das, S.S., F.H. Fitzek, E.D. Carvalho and R. Prasad, 2005. Variable guard interval orthogonal frequency division multiplexing in presence of carrier frequency offset. Proceedings of the IEEE Global Telecommunications Conference, Dec. 2-2, IEEE Xplore Press, St. Louis, MO., pp: 5-5. DOI: 10.1109/GLOCOM.2005.1578296

16. Ghosh, S., 2011. Performance study of WiMAX for different QoS parameters with varying cyclic prefix. PhD Thesis, Jadavpur University Kolkata.

17. Yi Jiang, William W. Hager, Jian Li. "MIMO Transceiver Design Using Geometric Mean Decomposition," ITW 2004, San Antonio, Texas, October 24-29, 2004

18. Recommendation ITU-R M.2083 – Framework and overall objectives of the future development of IMT for 2020 and beyond.

19. Valery Tikhvinskiy, Grigory Bochechka, Alexander Minov, Andrey Gryazev. Innovation Radar as a Tool of 5G Development Analysis. Proceedings of the

16th International Conference, NEW2AN 2016, and 9th Conference, ruSMART 2016, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, St. Petersburg, Russia, September 26–28, 2016, pp. 383–394.

20. A. Yazar and H. Arslan, “Flexible Multi-Numerology Systems for 5G New Radio,” River Publishers Journal of Mobile Multimedia, vol. 14, no. 4, pp. 367-394, Oct. 2018.

21. Ness, R., J.P. Linnartz, L. Van der Perre and M. Engels, 2002. The OFDM Principle. In: Wireless OFDM Systems: How to Make Them Work? Engels, M. (Ed.), Springer, ISBN-10: 1402071167, pp: 33-51.

22. Kreutz D., Ramos F.M.V., Verissimo P.E., Rothenberg C.E., Azodolmolky S., Uhlig S. *Software-Defined Networking: A Comprehensive Survey*. // Proceedings of the IEEE. – 2015. – Vol. 103, No. 1. – P. 14–76. – DOI: 10.1109/JPROC.2014.2371999

23. Одарченко Р.С., Поліщук В.В. Дослідження переваг та недоліків концепції SDN. *Актуальні проблеми розвитку науки і техніки*: матеріали доп. учасн. І Міжнародної науково-технічної конференції, 22 жовтня 2015 р. Київ, 2015. С. 200.

24. Mobile Edge Computing use cases & deployment options. White paper. Heavy reading, July 2016

25. Mobile Edge Computing A key technology towards 5G // Nurit Sprecher (Chair of ETSI MEC ISG) 5G World 2016, London, UK

26. Bercovich D., Contreras L. M., Haddad Y., Adam A., Bernardos C. J. Software-defined wireless transport networks for flexible mobile backhaul in 5g systems. *Mobile Networks and Applications*, 2015. Vol. 20, № 6. P. 793-801.

27. Andrews J.G., Buzzi S., Choi W., Hanly S.V., Lozano A., Soong A.C., Zhang J.C. *What Will 5G Be?* // IEEE Journal on Selected Areas in Communications. – 2014. – Vol. 32, No. 6. – P. 1065–1082. – DOI: 10.1109/JSAC.2014.2328098

28. Taleb T., Samdanis K., Mada B., Flinck H., Dutta S., Sabella D. *On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration*. // IEEE Communications Surveys & Tutorials. – 2017. – Vol. 19, No. 3. – P. 1657–1681. – DOI: 10.1109/COMST.2017.2705720

29. International Telecommunication Union (ITU). *Measuring digital development: Facts and figures 2022*. – ITU Publications, Geneva, 2022. – [Електронний ресурс]. – Режим доступу: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

30. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

31. Закон України «Про інформацію», стаття 18. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

32. Закон України «Про інформацію», стаття 19. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

33. Закон України «Про інформацію», стаття 20. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

34. Закон України «Про інформацію», стаття 21. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

35. Kibria M.G., Nguyen H., Villardi G.P., Ishizu K., Kojima F., Harada H., Kato N. *Big Data Analytics, Machine Learning, and Artificial Intelligence in Next-Generation Wireless Networks*. // IEEE Access. – 2018. – Vol. 6. – P. 32328–32338. – DOI: 10.1109/ACCESS.2018.2837691

36. Одарченко Р.С., Скульська О.Ю., Гнатюк В.О. Метод оцінки ключових по-казників захищеності в сучасних стільникових мережах. *Безпека інформації.* 2017. № 1(23). С. 19-26.

37. Одарченко Р.С., Харлай Л.О., Абакумова А. О., Чмих П.А. Програмне забезпечення для оцінки ключових показників якості обслуговування зі сторони абонента стільникової мережі. *Проблеми інформатизації та управління* . 2017. №3(59). С. 56-61.1

38. The White House. *National Strategy to Secure 5G of the United States of America*. – March 2020. – [Електронний ресурс]. – Режим доступу: https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf

39. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA). *5G Security Evaluation Process: Threat Model, Attack Vectors and Mitigations*. – Version 1.0, October 2021. – [Електронний ресурс]. – Режим доступу: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2829839/

40. U.S. Department of Defense (DoD). *5G Strategy Implementation Plan*. – May 2020. – U.S. Department of Defense, Office of the Under Secretary of Defense for Research and Engineering. – [Електронний ресурс]. – Режим доступу: https://media.defense.gov/2020/May/13/2002291661/-1/-1/0/DOD-5G-STRATEGY-IMPLEMENTATION-PLAN.PDF

41. Odarchenko R., Sunduchkov K., Fesenko V., Didenko A., Verkhovets O., Fesenko A. The concept of a channeling system for satellite mobile communication for media delivery with increased efficiency // Proceedings of the 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 22–26 February 2022, Lviv–Slavske, Ukraine. – P. 775–779 O. Kodheli et al. Satellite Communications in the New Space Era: A Survey and Future Challenges, IEEE Communications Surveys & Tutorials, vol. 23, no. 1, 2021.

42. Dudnik A.S., Fesenko A.O., Fesenko V.O., Grinenko O.O., Grinenko S.A., Kvashuk D.M. Models and methods of determining penetration by means of wireless sensor networks // Monographic series “European Science”. Book 21. Part 1. Karlsruhe, Germany, 2023. – P. 161–171.ETSI EN 303 645 V2.1.1 (2020-06). Cyber Security for Consumer Internet of Things: Baseline Requirements.

43. Chumachenko S.S., Chumachenko B.S., Maloyed M.M., Odarchenko R.S., Fesenko V.O. *Метод маршрутизації в бездротових мережах IoT із високою щільністю пристроїв*. // *Проблеми інформатизації та управління*, т. 4, № 80 (2024). – Київ, 13 березня 2025. – С. 99–112. – DOI: 10.18372/2073-4751.80.19778

44. Kotyk B., Bakhtiiarov D., Lavrynenko O., Chumachenko B., Antonov V., Fesenko V., Chupryn V. *Neural network approach to 5G digital modulation recognition*. // *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024)*, Kyiv, Ukraine, January 24–27, 2024. – P. 82–92.

45. Saiko V., Odarchenko R., Zhurakovskyi B., Yevdokymenko M., Fesenko V., Tkachova O.*A model for building a wireless terahertz network for 5G NR*. // *Proceedings of the 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2023)*, Dortmund, Germany, 7–9 September 2023. – P. 1071–1076.

46. Одарченко Р.С., Григоренко Д.К., Дрофа Т.С. Фесенко В.О. Удосконалення ядра мережі 5G з метою підвищення рівня захищеності зв'язку // Наукоємні технології. – 2023. – №1(57). – С. 47–57.ITU-R M.2083-0 (2015). IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond.

47. 5G PPP. *5G and Public Safety: Communications Enablers for the Future*. – White Paper, 5G Infrastructure Public Private Partnership (5G PPP), 2021. – [Електронний ресурс]. – Режим доступу: https://5g-ppp.eu/white-papers/м

48. ETSI TR 103 457 V1.1.1 (2018-12). *Cyber Security for 5G Networks*. – Technical Report, European Telecommunications Standards Institute. – [Електронний ресурс]. – Режим доступу: https://www.etsi.org/deliver/etsi_tr/103400_103499/103457/01.01.01_60/tr_103457v010101p.pdf

49. Dudnik A.S., Fesenko A.O., Fesenko V.O., Grinenko O.O., Grinenko S.A., Kvashuk D.M. Models and methods of determining penetration by means of wireless sensor networks // Monographic series "European Science". Book 21. Part 1. Karlsruhe, Germany, 2023. – P. 161–171.ETSI EN 303 645 V2.1.1 (2020-06). Cyber Security for Consumer Internet of Things: Baseline Requirements.

50. Huawei Technologies. *6G White Paper: 6G – The Next Horizon – From Connected Things to Connected Intelligence*. – July 2021. – [Електронний ресурс]. – Режим доступу: https://www-file.huawei.com

51. 3GPP TR 23.731 V17.1.0 (2020-12). *Study on management aspects of Public Safety Network Slicing (Release 17)*. – 3rd Generation Partnership Project. – [Електронний ресурс]. – Режим доступу: https://www.3gpp.org

52. Критерій Байєса-Лапласа: веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D1%96%D0%B9_%D0%91%D0%B0%D0%B9%D1%94%D1%81%D0%B0_%E2%80%94_%D0%9B%D0%B0%D0%BF%D0%BB%D0%B0%D1%81%D0%B0

53. . Жихор О.Б., Коваль Р.А. Вибір оптимального проектного рішення у ситуації невизначеності. *Науковий вісник НЛТУ України*. 2012. Вип. 22.5. С. 178-182

54. Гамидов Г.С. Основы инноватики и инновационной деятельности / Гамидов Г.С., Колосов В.Г., Османов Н.О. и др. – СПб : Изд-во "Политехника". 2000. – 323 с.

55. Одарченко Р.С., Харлай Л.А. Исследование эффективности сотовых сетей в Украине. *Актуальные научные исследования в современном мире.* 2017. №11-10(31). С.23-32

56. Одарченко Р. С., Дика Н. В. Дослідження архітектури мереж стільникового зв'язку в україні та можливостей їх переходу до мереж LTE. *Наукоємні технології*. 2016. № 3 (31). С. 291-298.

57. Бойко М. П. Системи стільникового зв'язку : конспект лекцій, ОНАЗ. Одеса. 2004. 76 с.

58. Одарченко Р.С., Мирутенко Л.В., Даков С.Ю. Удосконалений метод побудови опорного сегменту мережі LTE. *Наукоємні технології.* 2018. №1(37). С.18-26.

59. Одарченко Р.С. Удосконаленний метод планування мережі LTE / Р.С. Одарченко, В.В. Бараннік// Наукоємні технології в інфокомунікаціях: обробка, захист та передача інформації: Монографія / [за ред. В. В. Баранніка, В. М. Безрука] – Х. : Видавництво «Стиль-видат», 2018. С. 293-302.

60. Одарченко Р.С. Оцінка імовірності бітової помилки та пропускної здатності каналів антенних MIMO-систем. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. Житомир: ЖВІ НАУ, 2012. Вип. 2. С. 57-67.

61. Haykin S. *Communication Systems*. – 4th ed. – John Wiley & Sons, 2001. – 1104 p.

62. IEEE 802.16.3c-01/29r4. *Channel Models for Fixed Wireless Applications*. – IEEE Working Group on Broadband Wireless Access, 2001. – [Електронний ресурс]. – Режим доступу: https://ieee802.org

63. Nokia. *5G Spectrum: Strategies, Planning and Allocation*. – White Paper, 2020. – [Електронний ресурс]. – Режим доступу: https://www.nokia.com/networks/portfolio/5g/spectrum/

64. 3GPP TR 38.901 V16.1.0 (2020-01). *Study on channel model for frequencies from 0.5 to 100 GHz*. – 3rd Generation Partnership Project (3GPP). – [Електронний ресурс]. – Режим доступу: https://www.3gpp.org

65. ETSI TR 103 305-1 V1.1.1 (2018-04). *CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls*. – European Telecommunications Standards Institute. – [Електронний ресурс]. – Режим доступу: https://www.etsi.org

66. IEEE 802.1Qcc-2018. *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks – Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements*. – IEEE, 2018. – DOI: 10.1109/IEEESTD.2018.8423793

67. Бовда Е.М, Сальник В.В. Методи забезпечення якості обслуговування в сучасних телекомунікаційних мережах військового призначення: Збірник наукових праць Харківського національного університету Повітряних Сил. 2017. Вип.2 (51). С. 85-94

68. ITU-T E.800. *Definitions of terms related to quality of service*. – International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), Series E. – 2008. – [Електронний ресурс]. – Режим доступу: https://www.itu.int/rec/T-REC-E.800

69. ETSI TR 103 305-1 V1.1.1 (2018-04). *CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls*. – European

Telecommunications Standards Institute (ETSI). – [Електронний ресурс]. – Режим доступу: https://www.etsi.org

70. IEEE 802.1Qcc-2018. *IEEE Standard for Local and Metropolitan Area Networks — Bridges and Bridged Networks — Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements*. – IEEE, 2018. – DOI: 10.1109/IEEESTD.2018.8423793

71. ITU-T E.800. *Definitions of terms related to quality of service*. – International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), Series E. – Geneva, 2008. – [Електронний ресурс]. – Режим доступу: https://www.itu.int/rec/T-REC-E.800

72. Ericsson. *Ericsson Mobility Report*. – Latest edition, 2024. – [Електронний ресурс]. – Режим доступу: https://www.ericsson.com/en/reports-and-papers/mobility-report

73. ETSI TR 102 860 V1.1.1 (2011-08). *Terrestrial Trunked Radio (TETRA); Critical Communications; Service and System Requirements for Operation in Harsh Environments*. – European Telecommunications Standards Institute. – [Електронний ресурс]. – Режим доступу: https://www.etsi.org

74. Technical Report ITU-T GSTP-TN5G: Transport network support of IMT-2020/5G. –SG15- TD338/PLEN, October 2018.

75. Draft Recommendation Characteristics of transport networks to support IMT-2020/5G (G.ctn5g). – SG15-TD295/PLEN, October 2018.

76. ITU towards “IMT for 2020 and beyond” - IMT-2020 standards for 5G; Minimum requirements related to technical performancefor IMT-2020 radiointerface(s) ITU (2017).

77. 3GPP TS 23.501 V17.7.0 (2023-12). *System architecture for the 5G System (5GS); Stage 2*. – 3rd Generation Partnership Project (3GPP). – [Електронний ресурс]. – Режим доступу: https://www.3gpp.org

78. Foukas, X.; Patounas, G.; Elmokashfi, A.; Marina, M. K. (2017). "Network Slicing in 5G: Survey and Challenges" (PDF). IEEE Communications Magazine. 55 (5): 94–100.

79. "ETSI - Standards for NFV - Network Functions Virtualisation | NFV Solutions"; "Network Functions Virtualisation (NFV); Use NFV is present and SDN is future.Cases"

80. Fesenko V.O., Lavrynenko O.O., Odarchenko R.S., Tkachova O.M. *The concept of a channeling system for satellite mobile communication for media delivery with increased efficiency*.// *Proceedings of the 8th International Conference on Modeling, Development and Strategic Management of Economic System (MDSMES 2023)*, Odesa, Ukraine, 24–27 May 2023. – P. 278–286

81. The White House. *National Strategy to Secure 5G of the United States of America*. – March 2020. – [Електронний ресурс]. – Режим доступу: https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf

82. U.S. Department of Defense. *5G Strategy Implementation Plan*. – May 2020. – Office of the Under Secretary of Defense for Research and Engineering. – [Електронний ресурс]. – Режим доступу: https://media.defense.gov/2020/May/13/2002291661/-1/-1/0/DOD-5G-STRATEGY-IMPLEMENTATION-PLAN.PDF

83. National Institute of Standards and Technology (NIST). *Public Safety Communications Research (PSCR) Division – 5G and Beyond: Research Roadmap and Use Cases*. – 2022. – [Електронний ресурс]. – Режим доступу: https://www.nist.gov/communications-technology-laboratory/pscr

84. 3GPP TS 23.503 V17.4.0 (2023-09). *Policy and charging control framework for the 5G System (5GS)*. – 3rd Generation Partnership Project (3GPP). – [Електронний ресурс]. – Режим доступу: https://www.3gpp.org

85. Cybersecurity and Infrastructure Security Agency (CISA). *Resiliency Considerations for Communications Systems: A Guide for Practitioners*. – Version 1.0, December 2021. – [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/resources-tools/resources/resiliency-considerations-communications-systems

86. 3GPP TS 33.501 V17.6.0 (2023-12). *Security architecture and procedures for 5G System*. – 3rd Generation Partnership Project (3GPP). – [Електронний ресурс]. – Режим доступу: https://www.3gpp.org

87. National Institute of Standards and Technology (NIST). *NIST Special Publication 800-187: Guide to LTE Security for Public Safety Networks*. – NIST, U.S. Department of Commerce, 2017. – [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-187/final

88. Digi International. *How to Enable QoS and SLA Policies in Private LTE and 5G Networks*. – Technical White Paper, 2022. – [Електронний ресурс]. – Режим доступу: https://www.digi.com/resources

89. ITU-T E.804. *Key Performance Indicators for Smart Sustainable Cities to Assess the Achievement of Sustainable Development Goals*. – International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), 2017. – [Електронний ресурс]. – Режим доступу: https://www.itu.int/rec/T-REC-E.804

90. ITU-T Y.1540. *Internet protocol data communication service – IP packet transfer and availability performance parameters*. – International Telecommunication Union, 2019. – [Електронний ресурс]. – Режим доступу: https://www.itu.int/rec/T-REC-Y.1540

91. IETF RFC 6390. *Guidelines for Considering New Performance Metric Development*. – Internet Engineering Task Force (IETF), October 2011. – [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc6390

92. Ericsson. *Field Measurement Report on Urban 5G Network Performance*. – White Paper, 2023. – [Електронний ресурс]. – Режим доступу: https://www.ericsson.com/en/reports-and-papers

93. *Docker Documentation: Install Docker Engine*. – Official Docker Docs, 2024. – [Електронний ресурс]. – Режим доступу: https://docs.docker.com/engine/install/

94. ITU-T E.806. *Quality of service metrics and measurement methods for mobile services*. – International Telecommunication Union, 2020. – [Електронний ресурс]. – Режим доступу: https://www.itu.int/rec/T-REC-E.806

95. 3GPP TR 32.862 V17.0.0 (2022-06). *Study on QoE metrics, monitoring and measurements*. – 3rd Generation Partnership Project (3GPP). – [Електронний ресурс]. – Режим доступу: https://www.3gpp.org

96. *Measuring Broadband America – Mobile Measuring Report*. – FCC, Office of Engineering and Technology, 2021. – [Електронний ресурс]. – Режим доступу: https://www.fcc.gov/reports-research/reports/measuring-broadband-america

97. Jain R. *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. – Wiley, 1991. – 720 p.

98. Trivedi K.S. *Probability and Statistics with Reliability, Queuing and Computer Science Applications*. – 2nd ed. – Wiley, 2001. – 880 p.

ДОДАТКИ

Прим. №___

ДЕРЖСПЕЦЗВ'ЯЗКУ

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
(ДержНДІ технологій кібербезпеки)

вул. Залізняка, 3, корпус 6, м. Київ, 03142, Україна, тел. (044) 281-85-20, факс: (044) 281-97-11,
e-mail: ictip@cip.gov.ua, сайт: https://csi.cip.gov.ua, код згідно з ЄДРПОУ 34732331

_____ №_____ На № _____ від _____

ЗАТВЕРДЖУЮ
Перший заступник начальника Інституту
к.т.н. Олексій ЮДІН
«___» квітня 2025 р.

АКТ впровадження

наукових результатів дисертаційного дослідження
Фесенка Владислава Олексійовича на тему:
«Методи підвищення ефективності функціонування мобільних мереж зв'язку спеціального призначення»
на здобуття наукового ступеня доктора філософії (спеціальність 172 – «Електронні комунікації та радіотехніка» з галузі знань 17 «Електроніка, автоматизація та електронні комунікації»)

Комісія у складі:

голови комісії – головний науковий співробітник науково-дослідного центру ДержНДІ технологій кібербезпеки Гнатюк С.О.

членів комісії – начальника центру кіберзахисту ДержНДІ технологій кібербезпеки Комарова М.Ю., головного наукового співробітника науково-дослідного центру ДержНДІ технологій кібербезпеки Липського О.А. з'ясувала, що результати дисертаційного дослідження ***Фесенко В.О.*** на тему: ***«Методи підвищення ефективності функціонування мобільних мереж зв'язку спеціального призначення»*** мають належний теоретичний та методологічний рівень, а також суттєву практичну значущість і використані в діяльності Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації.

Фесенко В.О. отримані такі наукові результати:

- розроблено метод планування мереж зв'язку з урахуванням топографії, сценаріїв надзвичайних ситуацій, а також моделі QoS/SLA-інфраструктури для критичних сервісів;

- удосконалено методику для підвищення надійності зв'язку через інтеграцію супутникового сегменту та реалізацію адаптивної маршрутизації.

Зазначені наукові результати було використано:

- для побудови програмно-визначених сегментів мобільних мереж спеціального призначення з підтримкою сервісів MCX (MCPTT, MCVideo, MCData);
- для моделювання та оцінки ефективності таких мереж на основі критичних показників KPI/KQI.

Розроблені метод та удосконалена методика, впроваджені в ході виконання ДКР шифр «Сакура». Впровадження дозволило підвищити надійність та стійкість до загроз телекомунікаційної інфраструктури, що розгортається для потреб безпеки.

Голова комісії:
головний науковий співробітник науково-дослідного
центру ДержНДІ технологій кібербезпеки
д.т.н., професор Сергій ГНАТЮК

Члени комісії:
начальник центру кіберзахисту
ДержНДІ технологій кібербезпеки
к.т.н. Максим КОМАРОВ

головний науковий співробітник науково-дослідного
центру ДержНДІ технологій кібербезпеки
к.т.н., доцент Олександр ЛИПСЬКИЙ

«14» квітня 2025 р.

З А Т В Е Р Д Ж У Ю

Проректор Державного університету «Київського авіаційного інституту» з наукової роботи

_____ С.О. Гнатюк

«__» 04 2025 р.

АКТ ВПРОВАДЖЕННЯ

результатів дисертаційної роботи здобувача наукового ступеня доктора філософії Фесенка Владислава Олексійовича у навчальний процес Київського авіаційного інституту

Ми, що нижче підписалися, *завідувач кафедри телекомунікаційних та радіоелектронних систем Факультету аеронавігації, електроніки та телекомунікацій, к.т.н., доц., В.О. Гнатюк, декан Факультету аеронавігації, електроніки та телекомунікацій Київського авіаційного інституту д.т.н., проф. Р.С. Одарченко*
склали цей акт про те, що результати наукових досліджень *за темою дисертаційної роботи на здобуття наукового ступеня доктора філософії Фесенка Владислава Олексійовича*
використовуються у навчальному процесі *на кафедрі телекомунікаційних та радіоелектронних систем Факультету аеронавігації, електроніки та телекомунікацій Київського авіаційного інституту.*

Найменування впровадженого результату	Форма впровадження і досягнутий фактичний ефект
Модель оцінки енергоефективності підсистеми базових станцій оператора стільникового зв'язку	*У навчальний процес як методичні рекомендації та програмні модулі при вивченні дисциплін, пов'язаних з проєктуванням та експлуатацією мобільних мереж 5G Підвищено ефективність засвоєння матеріалу студентами та забезпечено набуття практичних навичок проєктування стільникових мереж спецпризначення.*
Аналіз можливостей мереж 5G по забезпеченню потреб урядового зв'язку, формування вимог, розробка специфікацій мережі 5G для забезпечення потреб урядового зв'язку	*У навчальний процес як теоретичну та методичну базу при викладанні дисциплін, пов'язаних із проєктуванням критичних комунікаційних систем, а також при підготовці курсових та кваліфікаційних робіт студентів спеціальності 172 «Телекомунікації та радіотехніка». Підвищено рівень підготовки студентів у сфері урядового зв'язку, забезпечено формування компетентностей щодо вимог до архітектури, безпеки та якості обслуговування в мережах спеціального призначення. Розроблені специфікації були враховані при створенні навчальних модулів та використані як основа для адаптації підготовки персоналу до роботи з технологіями 5G в умовах підвищених вимог до стійкості та захищеності зв'язку*

Завідувач кафедри телекомунікаційних та радіоелектронних систем, к.т.н., доц. _____ В.О. Гнатюк

Декан Факультету аеронавігації, електроніки та телекомунікацій д.т.н., проф. _____ Р.С. Одарченко