ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ NGN ПРИ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

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

_____ Георгій ЖДАНОВИЧ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-62
Георгій ЖДАНОВИЧ
Ім'я, ПРІЗВИЩЕ

Керівник: Володимир РУЖИНСЬКИЙ
к.т.н. *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ждановичу Георгію Олексійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Впровадження технології NGN при модернізації телекомунікаційних систем та мереж
керівник кваліфікаційної роботи Володимир РУЖИНСЬКИЙ, к.т.н.
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10. 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. NGN.
2. Модернізація телекомунікаційних систем та мереж.
3. ЦОД.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Виникнення та модернізація мереж.
2. Мережі NGN як основа модернізації телекомунікаційних систем.
3. Використання потужних ЦОД для модернізації NGN.
4. Проблеми трафіка при модернізації мереж.

5. Перелік ілюстративного матеріалу: ___презентація на____слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	15.10.2025	Викон.
2	Розробка першого розділу	22.10.2025	Викон.
3	Розробка другого розділу	02.11.2025	Викон.
4	Розробка третього розділу	12.11.2025	Викон.
5	Розробка четвертого розділу	22.11.2025	Викон.
6	Висновки, вступ, реферат	02.12.2025	Викон.
7	Розробка презентації	12.12.2025	Викон.

Здобувач вищої освіти _____ Георгій ЖДАНОВИЧ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Володимир РУЖИНСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Жданович Г.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Впровадження технології NGN при модернізації телекомунікаційних систем та мереж»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Жданович Георгій Олексійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Ждановича Георгія Олексійовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Володимир РУЖИНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Жданович Г.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Ждановича Георгія Олексійовича
(прізвище, ім'я, по батькові)
на тему «Впровадження технології NGN при модернізації телекомунікаційних систем та мереж»

Актуальність.
Актуальність роботи зумовлена стрімким розвитком телекомунікаційних технологій, зростанням обсягів трафіку та переходом від традиційних мереж із комутацією каналів до пакетно-орієнтованих IP-архітектур. Мережі наступного покоління (NGN) забезпечують конвергенцію сервісів, гнучке керування трафіком, масштабованість і підтримку сучасних послуг, зокрема 4G/5G та хмарних сервісів. В умовах підвищених вимог до якості обслуговування й інформаційної безпеки, а також модернізації телекомунікаційної інфраструктури України, дослідження принципів побудови та функціонування NGN є своєчасним і практично значущим.
Позитивні сторони.
1. В роботі проведено глибокий аналіз механізмів керування трафіком і забезпечення якості обслуговування в мережах NGN.
2. Окрему увагу приділено питанням інформаційної безпеки та еволюції методів захисту даних у телекомунікаційних системах.
Недоліки.
1. Недостатньо широко представлено кількісні оцінки, моделювання або розрахунки для підтвердження теоретичних тверджень.
2. Питання економічної ефективності впровадження NGN розглянуті недостатньо глибоко.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Жданович Георгій Олексійович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь, вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 78 стор., 15 рис., 4 табл., 25 джерел.

Мета роботи – дослідження принципів побудови та функціонування мереж наступного покоління (NGN) у процесі модернізації телекомунікаційних систем, а також аналіз механізмів керування сервісами, трафіком і забезпечення якості обслуговування та інформаційної безпеки в умовах конвергенції послуг.

Об’єкт дослідження – телекомунікаційні системи та мережі зв’язку нового покоління, що базуються на пакетно-орієнтованих IP-архітектурах.

Предмет дослідження – архітектурні рішення мереж NGN, механізми керування трафіком і сервісами, а також методи забезпечення якості обслуговування та інформаційної безпеки в процесі модернізації телекомунікаційних мереж.

Короткий зміст роботи: у кваліфікаційній роботі розглянуто впровадження технології NGN під час модернізації телекомунікаційних систем і мереж. Проаналізовано еволюцію мереж від 1G до 5G та визначено основні тенденції розвитку архітектур, механізмів керування й безпеки. Особливу увагу приділено принципам побудови NGN, забезпеченню якості обслуговування, інформаційній безпеці та ролі високошвидкісних транспортних технологій. Розглянуто перспективи розвитку NGN в Україні. Зроблено висновок, що NGN є ефективною основою для забезпечення гнучкості, масштабованості та надійності сучасних телекомунікаційних мереж.

КЛЮЧОВІ СЛОВА: МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ, NGN, ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ, МОДЕРНІЗАЦІЯ МЕРЕЖ, IP-АРХІТЕКТУРА, КОНВЕРГЕНЦІЯ СЕРВІСІВ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, QOS, SLA, ІНФОРМАЦІЙНА БЕЗПЕКА, МОБІЛЬНІ МЕРЕЖІ, 5G

ABSTRACT

Text part of the master's qualification work: 78 pages, 15 figures, 4 table, 25 sources.

The purpose of the work is to study the principles of building and operating next-generation networks (NGN) in the process of modernizing telecommunication systems, as well as to analyze the mechanisms for managing services, traffic, and ensuring quality of service and information security in the context of service convergence.

Object of the research is telecommunication systems and new-generation communication networks based on packet-oriented IP architectures.

Subject of the research is architectural solutions for NGN networks, mechanisms for managing traffic and services, as well as methods for ensuring quality of service and information security in the process of modernizing telecommunication networks.

Summary of the work: the qualification work considers the implementation of NGN technology during the modernization of telecommunication systems and networks. The evolution of networks from 1G to 5G is analyzed and the main trends in the development of architectures, control mechanisms and security are identified. Particular attention is paid to the principles of building NGN, ensuring quality of service, information security and the role of high-speed transport technologies. The prospects for the development of NGN in Ukraine are considered. It is concluded that NGN is an effective basis for ensuring flexibility, scalability and reliability of modern telecommunication networks.

KEYWORDS: NEXT GENERATION NETWORKS, NGN, TELECOMMUNICATION NETWORKS, NETWORK MODERNIZATION, IP ARCHITECTURE, CONVERGENCE OF SERVICES, QUALITY OF SERVICE, QOS, SLA, INFORMATION SECURITY, MOBILE NETWORKS, 5G

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 ВИНИКНЕННЯ ТА МОДЕРНІЗАЦІЯ МЕРЕЖ 11
1.1 Розвиток зв’язку 11
1.2 Розвиток технологій в 3 та 4 поколіннях 19
1.3 Максимальна модернізація зв’язку в мережах 5 покоління 27
РОЗДІЛ 2 МЕРЕЖІ NGN ЯК ОСНОВА МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ 32
2.1 Архітектура NGN та механізми керування сервісами і трафіком 32
2.2 Забезпечення якості обслуговування та безпеки в мережах NGN 41
РОЗДІЛ 3 ВИКОРИСТАННЯ ПОТУЖНИХ ЦОД ДЛЯ МОДЕРНІЗАЦІЇ NGN 51
3.1 Технологія 400GE в ЦОД 51
3.2 Характеристики 400GE 55
3.3 Ethernet 400GE як компонент для апгрейду в мережах NGN 64
РОЗДІЛ 4 ПРОБЛЕМИ ТРАФІКА ПРИ МОДЕРНІЗАЦІЇ МЕРЕЖ 69
4.1 Виявлення слабих місць 69
4.2 Оптимальні рішення при модернізації мереж 73
ВИСНОВКИ 77
ПЕРЕЛІК ПОСИЛАНЬ 79
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 81

ВСТУП

Стрімкий розвиток інформаційно-комунікаційних технологій, постійне зростання обсягів передаваних даних та поява нових цифрових сервісів зумовлюють необхідність системної модернізації телекомунікаційних систем і мереж. Традиційні мережі зв’язку, побудовані на принципах жорсткої спеціалізації сервісів і комутації каналів, поступово вичерпують свої можливості та вже не здатні повною мірою відповідати сучасним вимогам щодо пропускної здатності, гнучкості, масштабованості та рівня інформаційної безпеки. У цих умовах особливої актуальності набуває концепція мереж наступного покоління — Next Generation Networks (NGN), яка розглядається як фундамент для подальшого розвитку телекомунікаційної інфраструктури.

Мережі NGN передбачають перехід до пакетно-орієнтованої IP-архітектури, у межах якої різнорідні сервіси — голосовий зв’язок, передавання даних, відео та мультимедійні застосунки — функціонують на єдиній транспортній платформі. Такий підхід забезпечує конвергенцію сервісів, спрощує інтеграцію різних технологій доступу та створює умови для швидкого впровадження нових послуг. Водночас модернізація мереж у напрямі NGN потребує вирішення складних технічних і організаційних завдань, зокрема забезпечення гарантованої якості обслуговування, високого рівня надійності та комплексної інформаційної безпеки.

Особливе значення впровадження NGN набуває в контексті розвитку мобільних мереж п’ятого покоління, хмарних обчислень, дата-центрів і сервісів, що працюють з великими обсягами даних. Для підтримки таких середовищ необхідні сучасні механізми керування трафіком, інтеграція угод рівня обслуговування з системами моніторингу, а також використання високошвидкісних транспортних технологій. Усе це робить NGN ключовим елементом цифрової трансформації телекомунікаційної галузі та суміжних секторів економіки.

Актуальність теми даної кваліфікаційної роботи зумовлена також потребами модернізації телекомунікаційних мереж в Україні, де розвиток NGN і технологій 5G розглядається як важлива складова цифрової економіки, державних сервісів,

промислових і корпоративних мереж. Перехід до сучасних мережевих архітектур відкриває значні можливості для підвищення ефективності та якості послуг, але водночас вимагає комплексного підходу до проєктування, експлуатації та захисту мережевої інфраструктури.

Метою даної кваліфікаційної роботи є дослідження принципів і особливостей впровадження технології NGN при модернізації телекомунікаційних систем та мереж, а також аналіз механізмів забезпечення якості обслуговування й інформаційної безпеки в умовах конвергенції сервісів і зростаючих вимог до сучасних телекомунікаційних середовищ.

1 ВИНИКНЕННЯ ТА МОДЕРНІЗАЦІЯ МЕРЕЖ

1.1 Розвиток зв’язку

1G — перше покоління мобільного зв’язку: становлення технології та фундаментальні проблеми безпеки

Перше покоління мобільного зв’язку, відоме як 1G, стало початковим етапом розвитку стільникових телекомунікацій і заклало базу для всіх подальших поколінь мобільних мереж. Комерційне впровадження мереж 1G розпочалося у 1979 році в Японії, яка першою у світі запустила повноцінну стільникову систему мобільного телефонного зв’язку. У наступні роки подібні мережі з’явилися в США та країнах Європи, однак їх розвиток відбувався фрагментарно та без єдиного міжнародного стандарту.

Технологічною основою мереж першого покоління був аналоговий радіозв’язок, що означало передавання голосу у вигляді безперервного електромагнітного сигналу без цифрового кодування чи обробки. Такий підхід був логічним продовженням класичної проводової телефонії, але в умовах радіоефіру він мав значні обмеження. Аналоговий сигнал виявився надзвичайно чутливим до шумів, завад, інтерференції та ослаблення, що безпосередньо впливало на якість зв’язку. Розмови часто супроводжувалися тріском, спотворенням голосу або навіть повною втратою зв’язку, особливо на межі зони покриття базової станції.

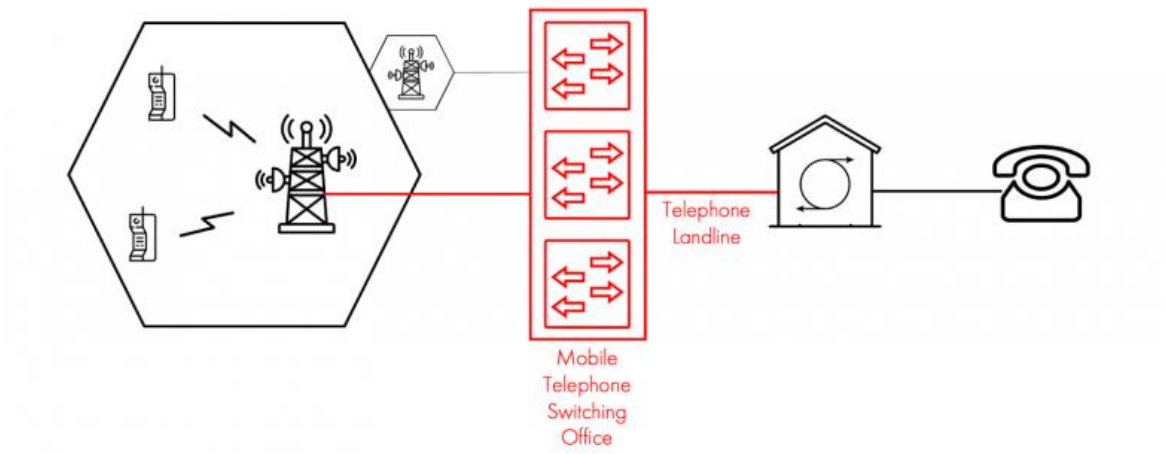


Рис. 1.1 Концептуальна схема побудови мереж 1 покоління

Покриття мереж 1G було локальним і обмеженим, а щільність базових станцій — низькою. Користувачі могли користуватися мобільним зв’язком лише в межах обслуговування конкретного оператора. Про повноцінний роумінг не йшлося: міжоператорська та міжнародна сумісність практично була відсутня, оскільки кожна країна розробляла власні стандарти, використовувала різні частотні діапазони та технічні рішення. У результаті мобільний телефон, придбаний в одній державі, зазвичай був абсолютно непридатним для використання в іншій.

Архітектура мобільних мереж першого покоління

Попри всі обмеження, саме в мережах 1G сформувалася базова архітектурна модель мобільного зв’язку, яка в еволюціонованому вигляді зберігається і в сучасних мережах 4G та 5G. Основна ідея полягала у поділі мережі на радіодоступну частину та центральне ядро, що забезпечує комутацію викликів.

Процес встановлення з’єднання в мережі 1G виглядав наступним чином. Коли абонент ініціював дзвінок зі свого мобільного телефону, аналоговий радіосигнал передавався по ефіру до найближчої базової станції. Далі цей сигнал пересилався у центральний вузол мережі оператора, який у першому поколінні мав назву Mobile Telephone Switching Office (MTSO).

Функціональність MTSO була вкрай обмеженою. Фактично цей вузол виконував роль телефонної комутаційної станції, адаптованої до мобільного середовища. Його завдання зводилося до:

- комутації викликів між абонентами однієї мережі,
- або маршрутизації дзвінків у проводову телефонну мережу загального користування (PSTN), тобто на стаціонарні домашні чи офісні телефони.

Будь-які механізми управління якістю послуг, контролю доступу, захисту інформації або інтелектуальної обробки трафіку були відсутні. Мережа розглядалася виключно як інфраструктура для передавання голосу, а не як складна інформаційна система.

Ключові проблеми безпеки мереж 1G

Найсерйознішим недоліком мереж першого покоління була практично повна відсутність концепції інформаційної безпеки. На етапі їх проєктування основна

увага приділялася забезпеченню стабільності зв’язку та покриття, тоді як захист даних користувачів фактично ігнорувався.

Передавання голосових даних здійснювалося у відкритому вигляді, без використання будь-яких алгоритмів шифрування або механізмів перевірки цілісності. Це означало, що будь-який сторонній спостерігач, маючи елементарний радіоприймач або сканер частот, міг без значних зусиль перехоплювати телефонні розмови. Налаштувавшись на відповідний частотний канал, зловмисник отримував прямий доступ до конфіденційної інформації абонентів.

Ситуацію ускладнювало й те, що канал зв’язку між базовою станцією та ядром мережі оператора також не мав захисту. У разі фізичного або мережевого доступу до цієї ділянки зловмисник міг втручатися у передавання сигналу, здійснювати його перехоплення або модифікацію.

Не менш критичною проблемою була відсутність механізмів аутентифікації абонентів. Мережа не перевіряла, чи є користувач, який ініціює з’єднання, справжнім власником облікового запису. Абоненти ідентифікувалися за простими ідентифікаційними номерами, які легко копіювалися або підмінялися. Це відкривало можливість для масового шахрайства: зловмисник міг видати себе за іншого користувача, користуватися його послугами та здійснювати дзвінки за чужий рахунок.

Такі вразливості створювали умови для цільових атак соціальної інженерії. Отримавши можливість імітувати конкретного абонента, зловмисник міг телефонувати його знайомим, родичам або колегам, представлятися жертвою та виманювати гроші або конфіденційну інформацію.

Окремої уваги заслуговує проблема доступності мережі. У мережах 1G використовувався примітивний механізм розподілу радіоресурсів: увесь частотний спектр поділявся на обмежену кількість вузьких каналів, кожен з яких виділявся одному абоненту на час розмови. Кількість таких каналів була дуже малою, що робило мережу надзвичайно вразливою до перевантажень. Надсилаючи велику кількість запитів на встановлення з’єднання, зловмисник міг повністю вичерпати

доступні ресурси базової станції, унеможлививши обслуговування легітимних користувачів.

Таким чином, мережі першого покоління характеризувалися низькою якістю зв’язку, відсутністю сумісності та вкрай слабким рівнем безпеки. Захист персональних даних, конфіденційність розмов і стійкість до атак не входили до пріоритетів операторів мобільного зв’язку того часу. Основною метою було забезпечити сам факт мобільного телефонного зв’язку — можливість здійснювати дзвінки без фізичного підключення до мережі.

Водночас стрімке зростання популярності мобільних телефонів продемонструвало величезний потенціал цієї технології. На початку 1990-х років кількість користувачів мереж 1G досягла близько 20 мільйонів осіб, що зробило мобільний зв’язок надзвичайно привабливим з комерційної точки зору. Усвідомлення як фінансових перспектив, так і численних технічних обмежень першого покоління стало ключовим стимулом для подальших досліджень і розробок.

Саме на основі досвіду експлуатації 1G було сформульовано вимоги до мереж другого покоління (2G), у яких вперше з’явилися цифрова передача даних, базові механізми шифрування, аутентифікація абонентів і більш ефективне використання радіочастотного спектра. Таким чином, попри всі недоліки, 1G відіграло вирішальну роль у становленні сучасних мобільних телекомунікацій.

2G — друге покоління мобільного зв’язку: цифровізація, аутентифікація та поява SIM-карт

Другий етап розвитку мобільних телекомунікацій, відомий як 2G, став якісним стрибком порівняно з мережами першого покоління. Комерційне розгортання мереж 2G розпочалося у 1991 році у Фінляндії, де було запущено першу мережу стандарту GSM (Global System for Mobile Communications). Саме GSM, а також його подальші розширення GPRS та EDGE, прийнято вважати класичними представниками другого покоління мобільного зв’язку.

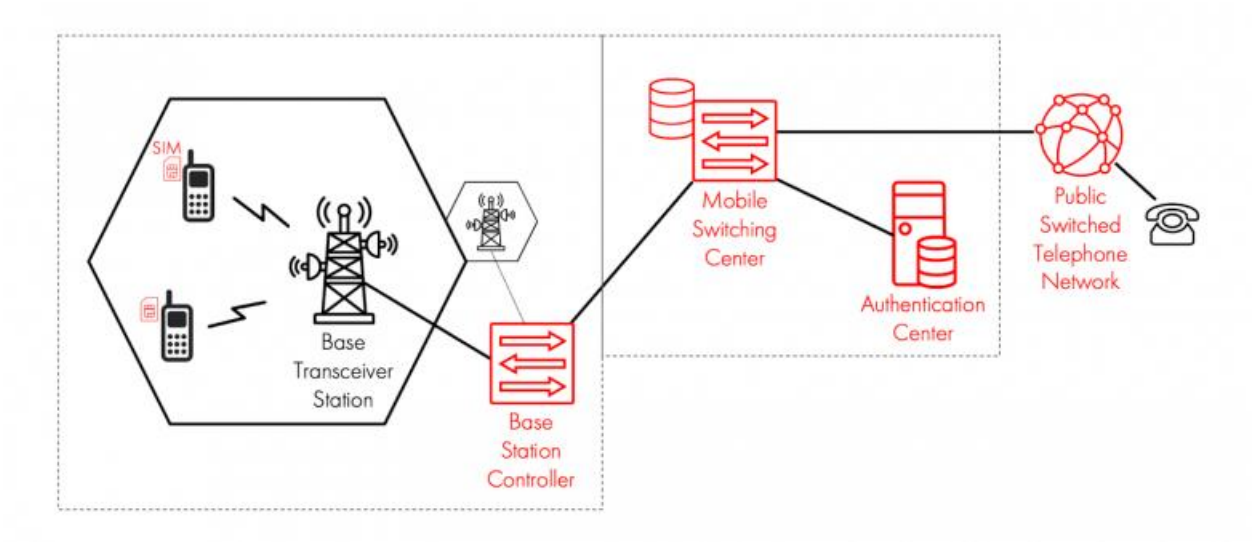


Рис. 1.2 Концептуальна схема побудови мереж 2 покоління

Ключовою відмінністю 2G від 1G став перехід від аналогової до цифрової передачі даних. Голос більше не передавався у вигляді безперервного аналогового сигналу — він оцифровувався, стискався та передавався у вигляді цифрових бітових потоків. Це дозволило кардинально покращити якість звуку, зменшити вплив шумів і завад, а також значно ефективніше використовувати радіочастотний спектр.

Разом із цифровізацією з’явилися нові послуги, які раніше були неможливими. Користувачі отримали можливість надсилати SMS-повідомлення, а згодом і MMS. Запровадження стандарту GPRS відкрило доступ до мобільного інтернету, хоч і з невисокими швидкостями за сучасними мірками. EDGE, у свою чергу, став еволюційним розвитком GPRS і дозволив ще більше підвищити пропускну здатність мережі без повної зміни інфраструктури.

Еволюція архітектури мережі GSM

Перехід до другого покоління супроводжувався суттєвою перебудовою архітектури мобільної мережі. Якщо в 1G ядро мережі було монолітним і виконувало мінімальний набір функцій, то в GSM відбулося чітке розділення ролей і функціональних компонентів.

По-перше, у мережі з’явився контролер базових станцій (Base Station Controller, BSC). Цей елемент взяв на себе управління радіоресурсами та базовими станціями. Саме BSC:

- виділяв радіоканали для абонентів,
- керував потужністю передавання,
- здійснював хендовер — процедуру безшовного перемикання абонента з однієї базової станції на іншу під час його переміщення.

Під час хендоверу необхідно не лише змінити фізичний радіоканал, але й передати сигнальну інформацію та частину користувацьких даних, щоб з'єднання не переривалося. Саме цю складну координацію забезпечував контролер базових станцій, що значно підвищило стабільність мобільного зв'язку.

По-друге, в архітектурі GSM чітко виокремився Mobile Switching Center (MSC) — центральний комутаційний вузол мережі. MSC відповідав за:

- комутацію голосових викликів,
- маршрутизацію трафіку до інших операторів,
- з'єднання з проводовими телефонними мережами загального користування (PSTN),
- а також підтримку роумінгу між різними мережами.

Таким чином, архітектура мережі стала багаторівневою, що дозволило масштабувати систему та впроваджувати нові сервіси.

Аутентифікація абонентів і поява SIM-карт

Найважливішою інновацією другого покоління з точки зору безпеки стало впровадження механізму аутентифікації абонентів. Для цього в архітектуру мережі GSM був доданий спеціальний компонент — Authentication Center (AuC).

У центрі аутентифікації оператор зберігав:

- унікальний ідентифікатор абонента,
- пов'язаний із ним закритий криптографічний ключ, який ніколи не передавався по мережі у відкритому вигляді.

Ці самі дані записувалися на SIM-карту (Subscriber Identification Module) — знімний модуль, який уперше з'явився саме в мережах 2G. SIM-карта фактично стала криптографічним носієм, що зберігав секрет між абонентом і оператором. Відтоді й до сьогодні більшість механізмів безпеки в мобільних мережах ґрунтується саме на принципі спільного секрету, відомого лише двом сторонам.

Процедура аутентифікації в GSM

Аутентифікація в мережі GSM реалізовувалася за схемою challenge–response. Її суть полягала в наступному. Authentication Center генерував випадкове число (RAND) і надсилав його на мобільний пристрій абонента. SIM-карта, використовуючи:

- отримане випадкове число,
- закритий ключ абонента,
- криптографічний алгоритм A3,

обчислювала аутентифікаційний код (SRES) і повертала його назад у мережу.

Паралельно Authentication Center, маючи той самий закритий ключ і те саме випадкове число, генерував очікуване значення аутентифікаційного коду. Далі отримане від абонента значення порівнювалося з еталонним. Якщо коди збігалися, це означало, що абонент дійсно володіє закритим ключем, а отже — є легітимним користувачем мережі. У протилежному випадку доступ до послуг оператора блокувався, оскільки йшлося про можливу спробу підміни особи.

Шифрування та його обмеження в 2G

Після успішної аутентифікації в мережі GSM генерувався сеансовий ключ шифрування за алгоритмом A8. Цей ключ використовувався для захисту радіоканалу між мобільним пристроєм і базовою станцією за допомогою алгоритму A5.

Проте тут крилася серйозна проблема. Шифрування застосовувалося виключно на радіоінтерфейсі, тобто між абонентом і базовою станцією. Усі дані, які передавалися далі — від базової станції до контролера, комутатора та інших елементів ядра мережі, — передавалися у незашифрованому вигляді. Це означало, що зловмисник, який отримував доступ до внутрішніх каналів оператора, міг перехоплювати весь трафік, включно з голосом, SMS і службовою інформацією.

Атаки на мережі другого покоління

Атака Fake BTS

Однією з найпоширеніших атак на мережі 2G стала атака Fake BTS (підроблена базова станція). Причиною її ефективності була одностороння

аутентифікація: мережа перевіряла абонента, але абонент не перевіряв автентичність мережі.

Зловмисник міг зібрати власну базову станцію, використовуючи антену та комп’ютер з відповідним програмним забезпеченням. Така станція змушувала мобільні пристрої підключатися саме до неї, після чого зловмисник опинявся між абонентом і реальною мережею оператора. У межах такої атаки типу *man-in-the-middle* злочинці могли перехоплювати дзвінки, SMS та інші дані.

Ще однією серйозною проблемою мереж 2G стала ставка на так звану Security through obscurity — безпеку через приховування принципів роботи системи. Алгоритми A3, A5 та A8 довгий час залишалися закритими, і вважалося, що їх секретність забезпечує криптостійкість.

Однак з часом стало очевидно, що такий підхід є хибним. Коли частину алгоритму A5 було розкрито, дослідникам і зловмисникам знадобилося лише кілька тижнів, щоб зламати його та навчитися дешифрувати радіотрафік. Це остаточно підтвердило, що приховування алгоритмів не може замінити математично обґрунтовану криптографічну стійкість.

Уразливості протоколів SS7

Окрему категорію загроз становили протоколи SS7, які використовувалися для передавання голосу, SMS, сигналізації та забезпечення роумінгу між операторами. Ці протоколи були розроблені ще у 1970-х роках для проводових телефонних мереж, у часи, коли питання кібербезпеки практично не розглядалися.

Отримавши доступ до SS7-мережі, зловмисник міг:

- відстежувати місцезнаходження абонентів,
- перенаправляти SMS-повідомлення,
- перехоплювати або переадресовувати голосові виклики.

Найвідомішим прикладом зловживання SS7 стала крадіжка понад 100 000 доларів з банківських рахунків. Зловмисники заражали комп’ютери жертв банківськими троянами або використовували фішинг, отримували доступ до акаунтів, а потім за допомогою уразливостей SS7 перенаправляли одноразові SMS-

паролі на власні номери. Це дозволяло їм підтверджувати транзакції та виводити кошти.

Отже, друге покоління мобільного зв’язку стало величезним кроком уперед порівняно з 1G. Воно принесло цифрову передачу даних, аутентифікацію абонентів, SIM-карти та базові механізми шифрування. Водночас 2G успадкувало низку концептуальних вразливостей, зокрема односторонню аутентифікацію, обмежене шифрування та слабку сигналізаційну безпеку.

Саме ці проблеми згодом стали рушійною силою для розвитку мереж третього покоління (3G), у яких було впроваджено взаємну аутентифікацію та наскрізний підхід до захисту даних.

1.2 Розвиток технологій в 3 та 4 поколіннях

3G — третє покоління мобільного зв’язку: стандартизація 3GPP та впровадження двосторонньої аутентифікації

На початку 2000-х років мобільний зв’язок уже перестав бути нішевою технологією й перетворився на масове явище. До 2004 року кількість мобільних пристроїв, що працювали в мережах другого покоління, перевищила один мільярд, що чітко продемонструвало як соціальну значущість, так і економічний потенціал мобільних телекомунікацій. Зростання кількості абонентів, поява нових сервісів та підвищені вимоги до якості зв’язку стали каталізатором для подальшої еволюції мобільних мереж.

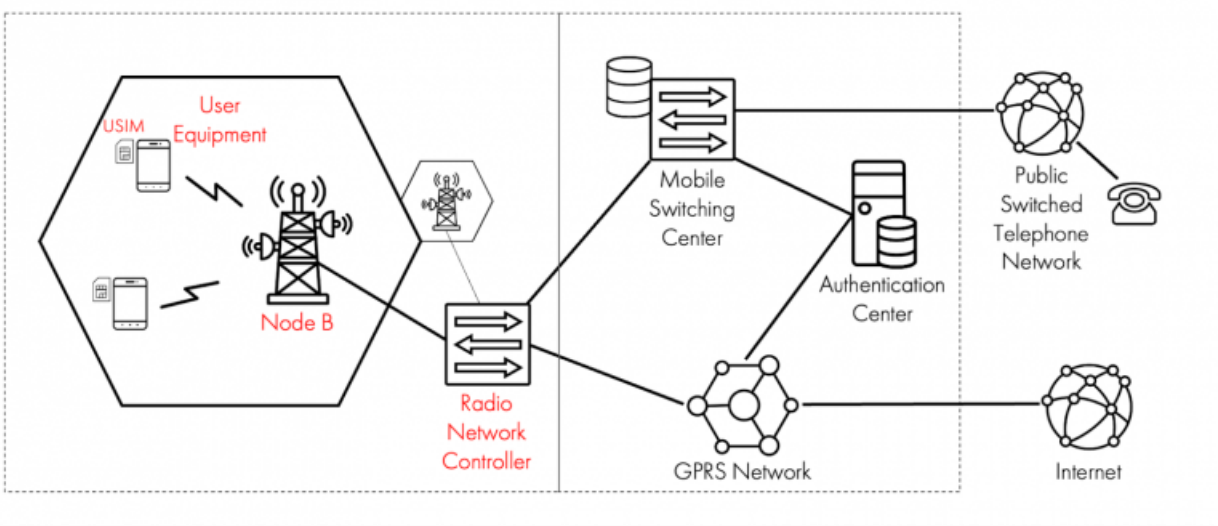


Рис. 1.3 Схема побудови мереж 3 покоління

З метою уніфікації підходів до розвитку нових стандартів був створений консорціум 3GPP (Third Generation Partnership Project) — міжнародне об'єднання телекомунікаційних компаній, виробників обладнання та наукових організацій. Саме 3GPP взяв на себе роль центрального органу зі стандартизації мереж третього покоління (3G), комерційне розгортання яких розпочалося на початку 2000-х років. На відміну від епохи 1G, де кожна країна рухалася власним шляхом, розвиток 3G відбувався вже в умовах глобальної координації та єдиних стандартів.

Принципи побудови мереж третього покоління

Одним із ключових принципів проєктування мереж 3G стала зворотна сумісність із мережами другого покоління. Оператори не могли дозволити собі повну заміну інфраструктури, тому опорна (core) мережа 3G значною мірою базувалася на архітектурі 2G, доповненій і вдосконаленій новими функціональними елементами. Це дозволило забезпечити поступовий перехід між поколіннями та зберегти працездатність уже існуючих сервісів.

Найбільш суттєві зміни відбулися в мережі радіодоступу. Для розподілу радіоресурсів між абонентами в 3G почали використовувати технологію Code-Division Multiple Access (CDMA) — множинний доступ із кодовим розділенням. На відміну від частотного або часового поділу, CDMA дозволяв багатьом абонентам одночасно використовувати той самий частотний діапазон, розрізняючи сигнали за допомогою унікальних кодів.

Такий підхід мав важливу перевагу з точки зору безпеки та доступності. Обмеження на кількість жорстко виділених каналів фактично зникло, що значно ускладнило реалізацію атак типу відмови в обслуговуванні, характерних для мереж 1G і частково 2G. Водночас CDMA привніс нову проблему: зі збільшенням кількості активних абонентів зростала ймовірність помилок декодування сигналів, що призводило до поступового погіршення якості зв'язку. Однак, на відміну від повного блокування доступу, це виражалося у зниженні швидкості або якості, а не в повному припиненні обслуговування.

Загалом архітектура мережі 3G залишилася еволюційним розвитком 2G. Уже в другому поколінні з'явилася мережа GPRS, яка надала абонентам доступ до інтернету, і саме вона стала фундаментом для пакетної передачі даних у 3G. Основні зміни полягали у перейменуванні компонентів мережі радіодоступу та розширенні їх функціональності, що дало змогу забезпечити вищі швидкості передачі даних, стабільніші з'єднання та кращу якість сервісів.

Еволюція підходів до безпеки та двостороння аутентифікація

Концепції безпеки, закладені у другому поколінні, не були відкинуті, а навпаки — збережені та суттєво вдосконалені. Саме в мережах третього покоління відбувся принциповий злам у підходах до аутентифікації. Якщо в 2G аутентифікувався лише абонент, то в 3G було впроваджено двосторонню (взаємну) аутентифікацію, за якої мобільний пристрій також перевіряв справжність мережі оператора.

Це нововведення стало відповіддю на поширені атаки типу Fake BTS, які активно використовувалися проти мереж другого покоління. Суть механізму залишилася подібною до схеми *challenge–response*, однак реалізація стала значно складнішою і криптографічно стійкішою.

Аутентифікаційний центр оператора більше не використовував застарілі алгоритми A3, A5 та A8. Натомість застосовувалися спеціальні криптографічні функції, на основі яких формувався так званий аутентифікаційний вектор. Цей вектор передавався мобільному пристрою, який, використовуючи власні

криптографічні механізми та спільний секретний ключ, генерував очікуване значення аутентифікаційного коду.

Отриманий результат порівнювався з кодом, надісланим мережею. Якщо значення не збігалися, це означало, що мережа не володіє закритим ключем, а отже може бути підробленою базовою станцією або частиною атаки. У такому разі з'єднання розривалося. Якщо ж коди збігалися, мобільний пристрій визнавав мережу автентичною і довіряв їй. Таким чином, двостороння аутентифікація суттєво підвищила рівень захисту користувачів.

Шифрування та контроль цілісності в мережах 3G

Для забезпечення конфіденційності та цілісності передаваних даних у 3G було впроваджено алгоритм KASUMI, який використовувався як для шифрування, так і для захисту від модифікації даних. Проте з часом з'ясувалося, що криптографічна стійкість KASUMI є недостатньою для довгострокового використання.

У відповідь на це був розроблений новий алгоритм SNOW 3G, який значно перевершував попередника за рівнем безпеки. Цей алгоритм виявився настільки успішним, що продовжує використовуватися й сьогодні, зокрема в мережах LTE, поряд з іншими криптографічними механізмами.

Водночас варто зазначити, що внутрішні канали зв'язку всередині мережі оператора, зокрема між контролером радіомережі та іншими компонентами ядра, часто не мали належного криптографічного захисту. Це означало, що загрози внутрішніх атак, пов'язаних із компрометацією інфраструктури оператора, залишалися актуальними навіть у мережах третього покоління.

IPsec і збереження проблем SS7

Консорціум 3GPP також запропонував використовувати IPsec для захисту з'єднань між підсистемою GPRS оператора та зовнішніми інтернет-провайдерами. IPsec дозволяв забезпечити взаємну аутентифікацію сторін і шифрування передаваних даних, що суттєво підвищувало рівень безпеки пакетної передачі інформації. Проте впровадження IPsec не було обов'язковим, і остаточне рішення щодо його використання залишалося за оператором мобільного зв'язку.

При цьому взаємодія між мережами різних операторів, зокрема у процесі роумінгу, продовжувала ґрунтуватися на протоколах SS7. Оскільки SS7 був спроєктований ще в епоху, коли питання безпеки не вважалися критичними, усі відомі загрози, пов’язані з цими протоколами, перейшли і в мережі третього покоління. Таким чином, попри значний прогрес у сфері аутентифікації та шифрування, повністю усунути системні вразливості сигналізаційної інфраструктури в 3G не вдалося.

Отже, мережі третього покоління стали важливим етапом еволюції мобільного зв’язку, поєднавши масштабованість, вищі швидкості передачі даних і суттєво вдосконалені механізми безпеки. Створення консорціуму 3GPP, впровадження двосторонньої аутентифікації та нових криптографічних алгоритмів заклали фундамент для подальшого розвитку мобільних мереж. Водночас спадкові проблеми, зокрема обмежений захист внутрішніх каналів і вразливості SS7, продемонстрували необхідність ще глибших змін, які згодом були реалізовані в мережах четвертого покоління (4G/LTE).

4G — четверте покоління мобільного зв’язку: повна IP-архітектура та нові алгоритми захисту

Мережі четвертого покоління (4G) почали масово розгортатися наприкінці 2000-х років і стали логічним результатом багаторічної еволюції мобільних телекомунікацій. На сьогодні стандарт LTE (Long Term Evolution) є найбільш поширеною та домінуючою технологією мобільного зв’язку у світі. Його ключовою особливістю стало повне переосмислення архітектури мережі: на відміну від попередніх поколінь, 4G із самого початку будувалося як повністю пакетна, IP-орієнтована система.

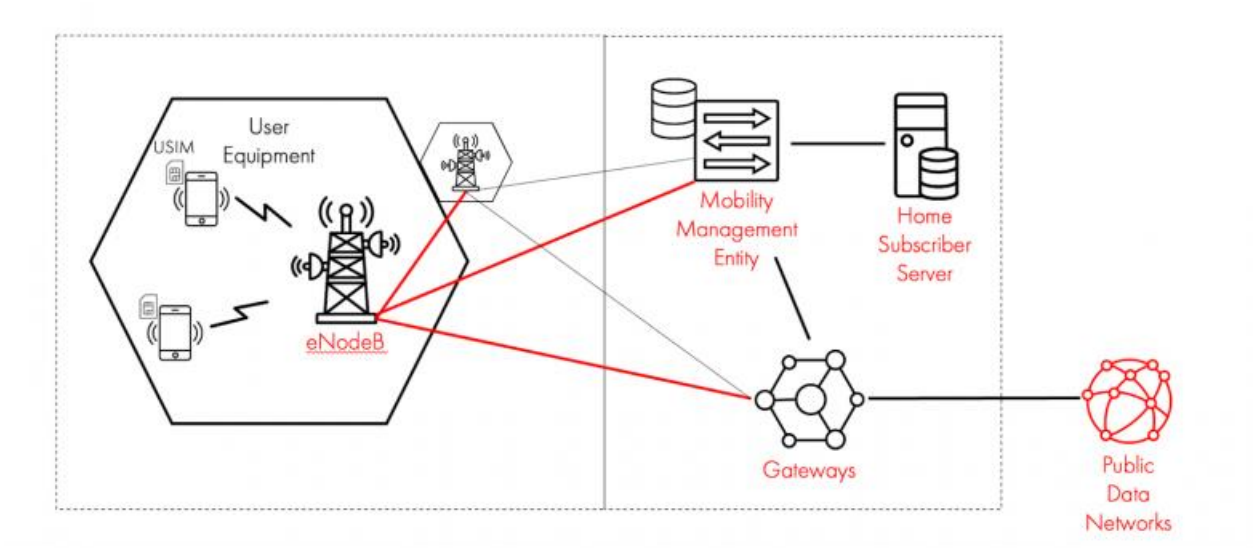


Рис. 1.4 Схема побудови мереж 4 покоління

У мережах LTE відсутній класичний комутаційний голосовий домен. Голосовий трафік більше не передається окремими комутаційними каналами, а інкапсулюється в IP-пакети та передається так само, як і будь-які інші дані. Для цього використовується технологія Voice over LTE (VoLTE), яка дозволяє передавати голос поверх IP-мереж із високою якістю, низькою затримкою та підтримкою сучасних мультимедійних сервісів.

Однією з принципових змін у сфері сигналізації стала відмова від застарілих протоколів SS7, які супроводжували мобільні мережі ще з епохи 2G та 3G. Їм на зміну прийшов протокол Diameter, розроблений з урахуванням сучасних вимог до безпеки. Diameter забезпечує аутентифікацію, авторизацію та облік (AAA), а також дозволяє захищати сигнальні повідомлення всередині мережі оператора, значно знижуючи ризики атак, притаманних SS7.

Трансформація архітектури мережі LTE

Архітектура мереж четвертого покоління зазнала радикальних змін порівняно з попередніми стандартами. По-перше, у 4G було повністю виключено контролер базових станцій, який у 2G та 3G відігравав центральну роль в управлінні радіоресурсами. Його функціональність була перерозподілена між самими базовими станціями та опорною мережею.

Базові станції нового покоління (eNodeB) стали значно «розумнішими». Вони отримали можливість:

- самостійно керувати радіоресурсами,
- виконувати процедури хендоверу,
- обмінюватися інформацією безпосередньо між собою через спеціальні інтерфейси.

З’явилися прямі канали зв’язку між базовими станціями, а також захищені канали між базовими станціями та опорною мережею оператора. Уся мережа була зведена до єдиного IP-простору, що дозволило суттєво спростити маршрутизацію та зменшити кількість точок виходу у зовнішні мережі.

Оскільки 4G є чисто пакетною мережею, традиційні комутаційні канали для з’єднання з іншими операторами були замінені IP-каналами. Це дозволило організувати один універсальний вихід до всіх зовнішніх мереж — як мобільних, так і фіксованих. Такий підхід підвищив масштабованість, спростив керування мережею та водночас створив передумови для більш уніфікованих механізмів захисту даних.

Нові підходи до захисту даних у 4G

Перехід до повністю IP-орієнтованої архітектури вимагав суттєвого перегляду механізмів безпеки. У мережах LTE було значно ускладнено систему ключів і підвищено рівень розмежування захисту різних типів трафіку.

Під час встановлення з’єднання між мобільним пристроєм і мережею оператора в 4G генерується одразу п’ять криптографічних ключів:

- два ключі використовуються для захисту контрольної (сигнальної) інформації з боку мережі оператора,
- ще два — для захисту контрольних даних з боку базової станції,
- окремий ключ призначений безпосередньо для шифрування користувацьких даних у радіоканалі між мобільним пристроєм і базовою станцією.

Такий поділ дозволив чітко ізолювати різні типи трафіку та мінімізувати наслідки компрометації окремих елементів мережі. Навіть у разі часткового порушення безпеки зловмисник не отримує доступ до всіх даних одразу.

Криптографічні алгоритми в мережах четвертого покоління

Для реалізації механізмів шифрування та контролю цілісності в LTE використовуються сучасні та добре досліджені криптографічні алгоритми, серед яких:

- SNOW 3G,
- AES (Advanced Encryption Standard),
- ZUC.

Особливе місце серед них займає AES — глобальний стандарт симетричного шифрування, який широко застосовується у банківських системах, захисті даних, VPN-технологіях та багатьох інших критично важливих сферах. Його впровадження в мобільних мережах четвертого покоління суттєво підвищило загальний рівень криптографічної стійкості. На сьогодні AES є найбільш поширеним алгоритмом для захисту мобільного трафіку, що робить 4G значно безпечнішим порівняно з попередніми поколіннями.

IPsec та захист інфраструктури базових станцій

У межах стандартів 3GPP також було запропоновано використовувати протокол IPsec для захисту з’єднань:

- між базовими станціями,
- між базовою станцією та опорною мережею оператора.

IPsec забезпечує взаємну аутентифікацію, шифрування та захист цілісності даних, що є критично важливим у повністю IP-орієнтованій архітектурі LTE. Окрім цього, 3GPP сформулював вимоги до так званої захищеної середовища базової станції, яке має гарантувати фізичний і програмний захист елементів мережі.

Втім, ці вимоги описані досить узагальнено, і конкретна реалізація значною мірою залежить від виробника обладнання. Такий підхід залишає простір для помилок реалізації та потенційних уразливостей, які можуть відрізнятися від вендора до вендора.

Атаки через даунгрейд до мереж попередніх поколінь

Попри значне підвищення рівня безпеки, мережі четвертого покоління не стали абсолютно невразливими. Одним із небагатьох практичних векторів атак залишився даунгрейд до мереж старших поколінь (2G або 3G).

Суть такої атаки полягає в особливостях роботи мобільних пристроїв. Телефон постійно надсилає базовій станції measurement reports — звіти про поточну якість сигналу. Зловмисник може підробити або інжектувати повідомлення, які вказують на погану якість зв’язку. У відповідь базова станція автоматично переводить абонента в мережу нижчого покоління, де доступні менш захищені механізми зв’язку.

Після цього зловмисник може експлуатувати відомі уразливості 2G або 3G, які вже давно вивчені. Водночас атаки через даунгрейд є складними в реалізації. Вони потребують точного таргетування конкретного абонента, глибокого розуміння мережевих протоколів та подальшого використання уразливостей старих стандартів, багато з яких сучасні оператори вже навчилися частково або повністю мітігувати.

Саме тому атаки через даунгрейд трапляються рідко і не є масовими, але вони наочно демонструють важливий принцип: загальний рівень безпеки мобільної мережі визначається найслабшою ланкою, якою часто залишаються застарілі технології.

Мережі четвертого покоління стали якісно новим етапом у розвитку мобільного зв’язку, поєднавши повністю IP-архітектуру, сучасні криптографічні алгоритми та значно вдосконалені механізми аутентифікації й захисту даних. Відмова від SS7, впровадження Diameter, AES та IPsec зробили 4G набагато стійкішим до атак. Водночас спадкові механізми сумісності з попередніми поколіннями зберегли окремі вектори загроз, що згодом стало одним із стимулів для подальшого розвитку мереж п’ятого покоління (5G).

1.3 Максимальна модернізація зв’язку в мережах 5 покоління

5G — п’яте покоління мобільного зв’язку: хмарна архітектура, мікросервіси та новий рівень безпеки

Мережі п’ятого покоління (5G) почали активно розгортатися на початку 2010-х років і стали найбільш технологічно складним етапом розвитку мобільного

зв’язку. На відміну від усіх попередніх поколінь, 5G проєктувалося не як еволюція класичної телекомунікаційної інфраструктури, а як повноцінна IT-платформа, орієнтована на хмарні обчислення, віртуалізацію та сервісну модель.

В основі 5G лежить мікросервісна архітектура, концепція network functions virtualization (NFV) та можливість розгортання елементів мережі в хмарному середовищі. Такий підхід дозволяє гнучко масштабувати мережу, швидко впроваджувати нові сервіси та адаптувати інфраструктуру під різні сценарії використання — від масового мобільного інтернету до індустріального IoT, автономного транспорту та критично важливих сервісів.

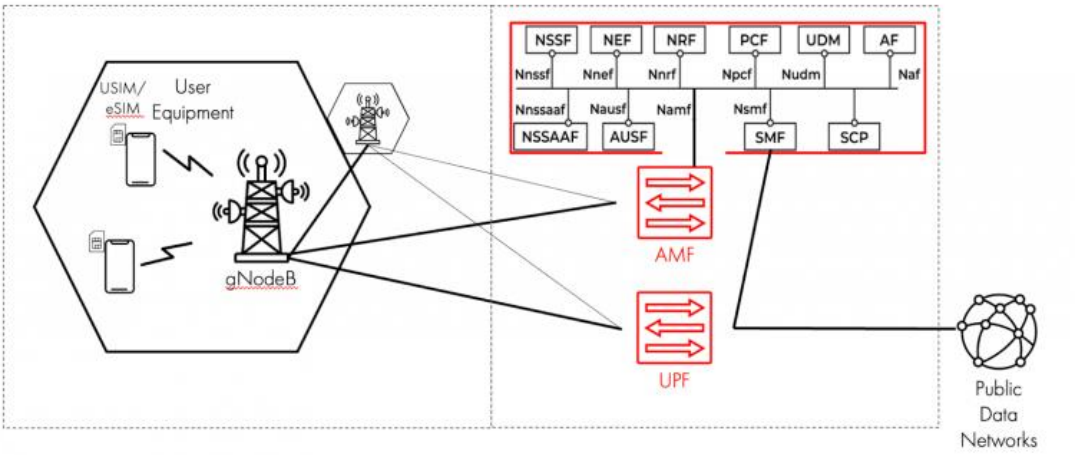


Рис. 1.5 Схема побудови мереж 5 покоління

Трансформація ядра мережі 5G

Ядро мережі п’ятого покоління зазнало кардинальних змін. Монолітні елементи попередніх поколінь були замінені на набір незалежних мережевих функцій (Network Functions, NF), кожна з яких відповідає за чітко визначену роль і може розгортатися окремо.

Зокрема:

- AMF (Access and Mobility Management Function) відповідає за керування доступом абонентів до мережі, реєстрацію пристроїв і мобільність користувачів;
- SMF (Session Management Function) керує сесіями користувачів, маршрутами передавання даних і потоками трафіку;

- PCF (Policy Control Function) забезпечує виконання політик оператора, контроль якості обслуговування та дотримання угод рівня сервісу (SLA);
- AUSF (Authentication Server Function) реалізує механізми аутентифікації абонентів і є ключовим елементом безпеки доступу до мережі.

Такий розподіл дозволив досягти високої модульності, спростити оновлення окремих компонентів і зменшити ризик каскадних відмов у разі збоїв.

Еволюція базової станції та концепція Open RAN

У специфікаціях Open RAN базову станцію 5G було логічно розділено на три окремі функціональні складові, що ще більше наблизило телекомунікаційну інфраструктуру до класичних IT-систем.

- Radio Unit (RU) безпосередньо взаємодіє з мобільними пристроями, приймає та передає радіосигнали;
- Distributed Unit (DU) виконує обробку даних на рівні стеку протоколів, забезпечує низьку затримку та роботу з радіоінтерфейсом;
- Central Unit (CU) керує потоками даних, визначає маршрути передавання пакетів і взаємодіє з ядром мережі.

Консорціум 3GPP і спільнота Open RAN рекомендують розгортати DU та CU у хмарній або віртуалізованій інфраструктурі, що дозволяє операторам використовувати стандартне серверне обладнання та зменшувати залежність від конкретних вендорів.

Безпека 5G: нові механізми та підходи

Безпека мереж п’ятого покоління регламентується великою кількістю стандартів і специфікацій. Лише в межах 3GPP було розроблено понад 30 нормативних документів, присвячених захисту даних, аутентифікації, сигналізації та внутрішніх взаємодій компонентів мережі.

Серед ключових нововведень варто виділити наступні.

По-перше, ідентифікатор абонента між мобільним пристроєм і базовою станцією передається в зашифрованому вигляді. Це означає, що пасивне прослуховування ефіру більше не дозволяє зловмиснику визначати або

відстежувати місцезнаходження конкретного користувача, що було серйозною проблемою в мережах попередніх поколінь.

По-друге, поява network functions, які можуть працювати як на одному фізичному сервері, так і в розподіленому хмарному середовищі, потенційно створювала нові вектори атак. Проте ці ризики були враховані ще на етапі проєктування. Взаємодія між мережевими функціями захищається за допомогою взаємної аутентифікації на основі Mutual TLS, а також механізмів авторизації, реалізованих через Open Authentication 2.0 (OAuth 2.0). OAuth визначає, які саме дані або API-ендпоїнти одна мережна функція має право використовувати щодо іншої.

Хмарні ризики та реальний стан загроз

Хоча архітектура 5G є cloud-friendly, вона не зобов'язує операторів обов'язково використовувати публічні хмари. Проте ті мережі, які все ж були розгорнуті в хмарному середовищі, зіткнулися з новими таргетованими атаками, характерними для сучасних IT-систем.

У цьому сенсі 5G не є винятком: протистояння між розробниками, операторами та зловмисниками є безперервним процесом, який ніколи не завершиться остаточно. Водночас варто підкреслити, що рівень безпеки мереж п'ятого покоління незрівнянно вищий, ніж у перших поколінь мобільного зв'язку.

На сьогодні існують теоретичні та експериментальні атаки на 5G, здебільшого реалізовані в лабораторних умовах. Публічної інформації про масштабні або успішні таргетовані атаки на комерційні 5G-мережі в медіапросторі не зафіксовано, що дозволяє зробити обережний висновок: на даному етапі рівень захисту 5G випереджає практичні можливості зловмисників.

Перехідний період мобільних мереж в Україні

В Україні, як і в більшості країн світу, мобільна інфраструктура перебуває у перехідному стані — від застарілих поколінь зв'язку до сучасних стандартів 4G та 5G. Оператори поступово відмовляються від мереж третього покоління, а в перспективі — і від 2G, водночас інвестуючи значні кошти в модернізацію безпеки там, де повна відмова від старих технологій поки що неможлива.

Такий підхід є економічно виправданим, адже нехтування безпекою призводить до серйозних фінансових втрат, репутаційних ризиків і втрати довіри абонентів.

Практичні рекомендації для підвищення безпеки користувачів

Поки триває перехідний період і смартфони все ще можуть автоматично перемикатися на 3G або навіть 2G, доцільно дотримуватися кількох простих, але ефективних рекомендацій:

1. Обмежте використання старих поколінь зв’язку. У налаштуваннях телефону варто обрати режим роботи лише в мережах 4G (LTE) та 5G, якщо така можливість доступна.
2. Використовуйте Voice over LTE (VoLTE) замість класичних голосових викликів через мережі другого покоління. За наявності такої опції її можна активувати в налаштуваннях мобільного зв’язку.
3. Віддавайте перевагу захищеним месенджерам із наскрізним шифруванням для обміну повідомленнями, замість використання SMS.
4. Не використовуйте SMS як другий фактор аутентифікації, якщо є альтернатива. Краще застосовувати спеціалізовані застосунки або push-повідомлення, які забезпечують значно вищий рівень захисту.

Мережі п’ятого покоління є найбільш захищеними та технологічно досконалими за всю історію мобільного зв’язку. Хмарна архітектура, мікросервіси, взаємна аутентифікація мережевих функцій і шифрування ідентифікаторів абонентів вивели безпеку на принципово новий рівень. Водночас спадковість поколінь і необхідність підтримки старих стандартів зберігають окремі ризики, що вимагає як зусиль з боку операторів, так і усвідомленої поведінки самих користувачів.

2 МЕРЕЖІ NGN ЯК ОСНОВА МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

2.1 Архітектура NGN та механізми керування сервісами і трафіком

Мережі наступного покоління (Next Generation Networks, NGN) являють собою концептуально новий етап у розвитку телекомунікаційних систем, який поєднує перевірені часом принципи класичних мереж зв’язку з можливостями сучасних IP-технологій та програмно-керованих мереж. Перехід до NGN зумовлений зростаючими вимогами до пропускної здатності, гнучкості, надійності та якості обслуговування, а також необхідністю підтримки різноманітних мультимедійних сервісів у межах єдиної інфраструктури.

Основною метою впровадження NGN є створення універсальної, масштабованої та адаптивної телекомунікаційної платформи, здатної забезпечувати надання широкого спектра послуг із гарантованими параметрами якості незалежно від типу мережі доступу та фізичного середовища передавання даних. Така платформа повинна ефективно підтримувати як традиційні сервіси, зокрема голосовий зв’язок, так і сучасні мультимедійні та інтерактивні застосунки, включно з передаванням відео високої роздільної здатності, хмарними сервісами та сервісами реального часу.

На відміну від традиційних телекомунікаційних мереж, у яких кожен тип сервісу реалізовувався на основі окремої спеціалізованої інфраструктури (виділені мережі для голосу, передачі даних і відео), архітектура NGN базується на принципі конвергенції сервісів і транспортних ресурсів. Усі види інформації — голос, дані, відео та сигнальний трафік — передаються у вигляді пакетів у межах єдиної IP-орієнтованої транспортної мережі. Це дозволяє уніфікувати механізми маршрутизації, керування та обробки трафіку, істотно підвищуючи ефективність використання мережевих ресурсів.

Важливою особливістю NGN є відокремлення логіки надання сервісів від транспортного рівня мережі. Функції керування викликами, сесіями та сервісами

реалізуються на окремих рівнях керування та сервісних платформах, що забезпечує незалежний розвиток прикладних сервісів без необхідності внесення змін у базову транспортну інфраструктуру. Такий підхід значно спрощує модернізацію мереж, скорочує час впровадження нових послуг і знижує експлуатаційні витрати операторів зв'язку.

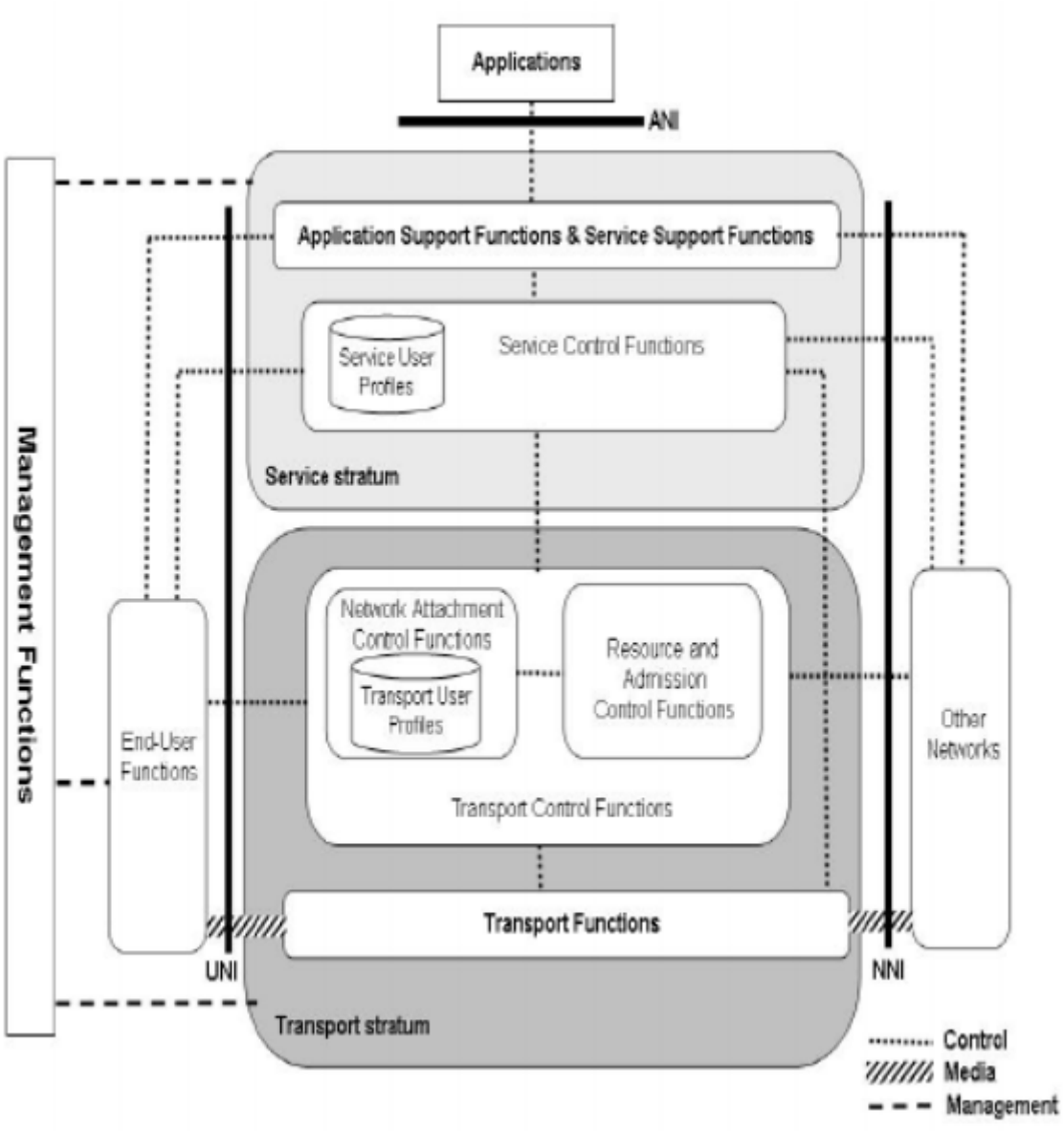


Рис. 2.1 Схема мережі NGN

Завдяки використанню пакетної передачі даних та стандартизованих IP-протоколів мережі NGN забезпечують високий рівень масштабованості та технологічної нейтральності. Це означає, що до мережі можуть інтегруватися різні технології доступу — фіксовані, мобільні та бездротові — без зміни загальних принципів функціонування системи. Така властивість є особливо важливою в

умовах поетапної модернізації телекомунікаційних мереж, коли необхідно забезпечити сумісність нових рішень із уже наявною інфраструктурою.

Узагальнюючи, впровадження концепції NGN створює передумови для:

- уніфікації телекомунікаційної інфраструктури та скорочення кількості спеціалізованих мереж;
- підвищення ефективності використання пропускної здатності та обчислювальних ресурсів;
- спрощення процесів керування мережею та надання сервісів;
- швидкого впровадження нових послуг і підтримки інноваційних бізнес-моделей;
- забезпечення гарантованої якості обслуговування для різних класів користувачів і сервісів.

Таким чином, мережі наступного покоління слугують фундаментальною основою модернізації сучасних телекомунікаційних систем, забезпечуючи їхню адаптацію до зростаючих вимог цифрового суспільства та створюючи єдину платформу для подальшого розвитку послуг зв’язку.

Загальні принципи побудови архітектури NGN

Архітектура мереж наступного покоління ґрунтується на чіткому функціональному розподілі телекомунікаційної системи на логічні рівні, кожен з яких виконує визначений набір завдань і має власну зону відповідальності. Такий підхід дозволяє спростити проєктування, експлуатацію та подальшу модернізацію мережі, а також забезпечує її гнучкість і масштабованість. На відміну від традиційних мереж, де функції доступу, передавання та керування були тісно пов’язані між собою, NGN реалізує модульну архітектуру, що дає змогу незалежно розвивати окремі компоненти системи.

Ключовим принципом побудови NGN є відокремлення транспортної функції від функцій керування та надання сервісів. Транспортна мережа відповідає виключно за передавання пакетів даних, тоді як логіка керування з’єднаннями, сесіями та сервісами реалізується на вищих рівнях архітектури. Такий поділ забезпечує незалежність розвитку транспортної інфраструктури від сервісних

платформ і дозволяє впроваджувати нові послуги без необхідності змінювати базові механізми передавання даних.

У загальному вигляді архітектура NGN включає такі основні логічні рівні:

• **рівень доступу**;

• **транспортний рівень**;

• **рівень керування**;

• **сервісний рівень**.

Кожен із цих рівнів виконує власні функції, однак їхня спільна робота забезпечує цілісність і узгодженість функціонування всієї мережі.

Рівень доступу призначений для підключення абонентів до мережі NGN незалежно від використовуваної технології. Він охоплює широкий спектр технологій фіксованого та бездротового доступу, зокрема мережі мобільного зв’язку, волоконно-оптичні лінії передачі даних, xDSL-технології, а також різні варіанти радіодоступу. Основним завданням цього рівня є забезпечення надійного фізичного та канального з’єднання між абонентським обладнанням і транспортною мережею.

Важливою характеристикою NGN є технологічна нейтральність рівня доступу, що означає можливість інтеграції різних технологій без необхідності змінювати принципи роботи ядра мережі. Завдяки цьому оператори зв’язку можуть поетапно модернізувати інфраструктуру, поєднуючи нові рішення з уже наявними мережами доступу. Такий підхід знижує капітальні витрати та забезпечує плавний перехід до сучасних технологій.

Транспортний рівень NGN реалізує пакетну передачу даних на основі IP-протоколу і є основою для функціонування всієї мережі. Саме на цьому рівні відбувається маршрутизація та комутація пакетів, формування транспортних шляхів і передавання даних між різними сегментами мережі. Використання IP як універсального транспортного протоколу дозволяє уніфікувати механізми передавання інформації та забезпечити сумісність із глобальними мережами передачі даних.

Крім базових функцій передавання, транспортний рівень забезпечує реалізацію початкових механізмів якості обслуговування, таких як класифікація трафіку, пріоритизація пакетів і керування пропускною здатністю. Це особливо важливо в умовах конвергенції сервісів, коли в межах однієї мережі передаються потоки з різними вимогами до затримки, надійності та пропускної здатності.

Відмова від комутації каналів на користь пакетної передачі даних дозволила суттєво підвищити ефективність використання пропускної здатності мережі. На відміну від традиційних телефонних мереж, де канал резервується на весь час з'єднання незалежно від фактичного використання, у NGN ресурси транспортної мережі динамічно розподіляються між активними потоками даних. Це забезпечує кращу адаптацію до змінного навантаження та підвищує загальну продуктивність системи.

Таким чином, загальні принципи побудови архітектури NGN — модульність, функціональний поділ, пакетна передача даних і технологічна нейтральність — створюють основу для гнучкої та ефективної телекомунікаційної інфраструктури.

Рівень керування в архітектурі NGN

Центральним елементом архітектури NGN є **рівень керування**, який відповідає за встановлення, підтримку та завершення з'єднань, а також за координацію роботи мережевих ресурсів. Саме на цьому рівні реалізуються механізми керування сесіями, мобільністю користувачів і взаємодією між різними сервісами.

На рівні керування функціонують такі ключові компоненти:

- системи керування викликами та сесіями;
- сервери сигналізації;
- платформи керування політиками та ресурсами.

У NGN широко застосовується **сигнальний протокол SIP (Session Initiation Protocol)**, який забезпечує ініціацію, модифікацію та завершення мультимедійних сесій. SIP дозволяє відокремити сигналізацію від транспортної частини мережі, що є важливою умовою масштабованості та гнучкості системи.

Рівень керування взаємодіє з транспортним рівнем через спеціалізовані інтерфейси, отримуючи інформацію про поточне завантаження мережі та доступні ресурси. На основі цих даних приймаються рішення щодо маршрутизації трафіку та допустимості надання певного сервісу конкретному абоненту.

Сервісний рівень та платформи надання послуг

Сервісний рівень NGN відповідає за **реалізацію прикладних сервісів** і логіку їх надання користувачам. До таких сервісів належать голосові виклики, відеозв'язок, мультимедійні повідомлення, інтерактивні послуги та сервіси доданої вартості.

Особливістю NGN є те, що сервіси реалізуються **незалежно від транспортної інфраструктури**, що дозволяє швидко змінювати або доповнювати функціональність мережі без втручання в її базову архітектуру. Це досягається шляхом використання сервісних платформ і програмних серверів додатків, які взаємодіють із рівнем керування через стандартизовані інтерфейси.

Такий підхід забезпечує **гнучке масштабування сервісів**, можливість персоналізації для окремих груп користувачів і підтримку нових бізнес-моделей операторів зв'язку.

Керування трафіком у мережах NGN

Оскільки NGN базується на пакетній передачі даних, ефективне керування трафіком є критично важливим завданням. У межах однієї мережі можуть одночасно передаватися потоки даних із різними вимогами до затримки, надійності та пропускної здатності.

Для формального опису трафіку часто використовуються параметри середньої інтенсивності та пропускної здатності. Наприклад, середню швидкість передавання даних можна описати співвідношенням:

$$R = \frac{B}{T} \tag{2.1}$$

де B — обсяг переданих даних, T — час передавання.

У NGN застосовуються механізми **класифікації та маркування трафіку**, що дозволяє розподіляти пакети за пріоритетами. Після класифікації трафік

обробляється відповідно до заданих політик, які визначають допустиму затримку, максимальну швидкість або рівень втрат.

Моделі керування трафіком і ресурсами

Однією з поширених моделей керування трафіком у NGN є **диференційоване обслуговування**, за якого трафік поділяється на класи з різними характеристиками обслуговування. Для кожного класу визначаються допустимі параметри якості, що дозволяє ефективно використовувати ресурси мережі.

Взаємозв'язок між затримкою, джитером та втратою пакетів можна узагальнено представити як залежність якості сервісу від завантаження мережі:

$$QoS = f(D, J, L) \tag{2.2}$$

де D — затримка, J — варіація затримки, L — ймовірність втрати пакетів.

Для оцінювання ефективності використання ресурсів транспортної мережі також застосовується коефіцієнт завантаження каналу.

Роль політик керування в мережах NGN

Політики керування відіграють ключову системоутворюючу роль у функціонуванні мереж наступного покоління, оскільки саме вони забезпечують узгоджену взаємодію між усіма компонентами NGN та визначають логіку використання мережевих ресурсів. У контексті NGN політики керування можна розглядати як набір формалізованих правил і механізмів прийняття рішень, які регламентують доступ користувачів і сервісів до транспортних, обчислювальних та мережевих ресурсів залежно від поточних умов роботи мережі.

На відміну від традиційних телекомунікаційних мереж, де параметри обслуговування були здебільшого статичними, NGN реалізує динамічний підхід до керування, за якого політики формуються з урахуванням типу користувача, класу сервісу, поточного стану мережі, а також вимог щодо якості обслуговування та рівня пріоритету. Це дозволяє мережі адаптувати свою поведінку в реальному часі, реагуючи на зміни навантаження, відмови окремих елементів або появу нових потоків трафіку.

Централізоване керування політиками забезпечує єдиний контрольний механізм для всієї мережі, що особливо важливо в умовах конвергенції сервісів. За

допомогою таких політик оператор може визначати, які сервіси мають отримувати пріоритетний доступ до ресурсів, які потоки даних підлягають обмеженню швидкості, а які — можуть бути тимчасово відкладені або перенаправлені альтернативними маршрутами. Це дозволяє динамічно перерозподіляти ресурси мережі без необхідності ручного втручання та зміни конфігурації окремих вузлів.

Важливою функцією політик керування є запобігання перевантаженню мережі. У разі зростання трафіку система керування може автоматично знижувати пріоритет менш критичних сервісів, наприклад фонових передач даних або завантаження великих файлів, одночасно гарантуючи стабільну роботу сервісів реального часу. Такий підхід дозволяє уникати ситуацій, коли різке збільшення навантаження призводить до деградації всіх сервісів без винятку.

Політики керування також забезпечують стабільну роботу критично важливих сервісів, до яких належать голосовий зв’язок, відеоконференції, служби екстреного виклику та корпоративні сервіси з підвищеними вимогами до надійності. Наприклад, у мережі NGN виклики екстрених служб можуть оброблятися за спеціальними політиками, що гарантують їм найвищий пріоритет незалежно від загального стану мережі. Навіть у разі значного перевантаження транспортної інфраструктури такі з’єднання зберігатимуть допустимі параметри затримки та втрат пакетів.

Практичним прикладом реалізації політик керування є сценарій обслуговування корпоративних користувачів у мережі оператора зв’язку. Для бізнес-клієнтів можуть бути визначені окремі політики, які забезпечують гарантовану пропускну здатність і мінімальні затримки для доступу до корпоративних сервісів, тоді як трафік масових абонентів обробляється за стандартними правилами. У такому випадку навіть під час пікових навантажень корпоративні сервіси продовжують працювати стабільно, що безпосередньо впливає на рівень довіри до оператора та якість наданих послуг.

Ще одним прикладом є керування мультимедійним трафіком. Відеопотоки високої роздільної здатності мають значні вимоги до пропускної здатності, однак можуть бути менш чутливими до затримки, ніж голосові сервіси. Політики

керування дозволяють коректно розмежовувати такі потоки, забезпечуючи оптимальний баланс між якістю зображення та загальною стабільністю мережі.

Завдяки впровадженню політик керування мережі NGN здатні підтримувати гарантовану якість сервісів навіть за умов значних і нерівномірних коливань навантаження. Такий підхід не лише підвищує ефективність використання мережевих ресурсів, але й створює основу для впровадження нових сервісів і бізнес-моделей, орієнтованих на індивідуальні потреби користувачів. У результаті політики керування стають одним із ключових інструментів модернізації телекомунікаційних систем у рамках концепції NGN, забезпечуючи їхню гнучкість, масштабованість і стійкість до зростаючих вимог сучасних сервісів.

З урахуванням наведеного, основні функції політик керування в мережах NGN можна узагальнити наступним чином:

- **керування доступом до мережевих ресурсів**, що передбачає автентифікацію користувачів і сервісів, визначення їхніх прав доступу та обмежень відповідно до заданих політик;
- **класифікація та пріоритизація трафіку** залежно від типу сервісу, що дозволяє забезпечувати першочергове обслуговування трафіку реального часу та критично важливих застосунків;
- **динамічний розподіл пропускної здатності**, який забезпечує ефективне використання мережевих ресурсів за змінних умов навантаження;
- **підтримка заданих параметрів якості обслуговування (QoS)** шляхом контролю затримок, втрат пакетів та варіації затримок для різних класів трафіку;
- **запобігання перевантаженню мережі та деградації сервісів** за рахунок адаптивного зниження пріоритету другорядних потоків трафіку;
- **підтримка надання гарантованих сервісів відповідно до угод рівня обслуговування (SLA)** для корпоративних та спеціалізованих користувачів;
- **забезпечення масштабованості мережі**, що дозволяє інтегрувати нові сервіси та збільшувати кількість абонентів без суттєвого зниження якості обслуговування.

2.2 Забезпечення якості обслуговування та безпеки в мережах NGN

Однією з ключових вимог до мереж наступного покоління є здатність забезпечувати гарантовану якість обслуговування та належний рівень інформаційної безпеки в умовах конвергенції сервісів і використання пакетної передачі даних. У мережах NGN в єдиній інфраструктурі одночасно функціонують сервіси з принципово різними вимогами до затримки, надійності та пропускної здатності, що суттєво ускладнює процес керування трафіком і ресурсами мережі.

На відміну від традиційних телекомунікаційних мереж, де параметри обслуговування визначалися жорсткою комутацією каналів і ресурси резервувалися на весь час з'єднання, мережі NGN працюють у режимі спільного використання ресурсів. Передавання даних здійснюється у вигляді пакетів, які динамічно маршрутизуються мережею залежно від поточного навантаження та доступності каналів. У таких умовах мережа функціонує в середовищі зі змінним трафіком, що вимагає застосування складних і адаптивних механізмів керування як якістю обслуговування, так і безпекою передавання інформації.

Якість обслуговування в NGN зазвичай характеризується низкою кількісних параметрів, до яких належать затримка передавання пакетів, варіація затримки (джитер), ймовірність втрати пакетів та доступна пропускна здатність. Наприклад, для сервісів голосового зв'язку допустима затримка зазвичай не повинна перевищувати 150–200 мс, а джитер має залишатися на мінімальному рівні, тоді як для передачі файлів або веб-доступу основним критерієм є пропускна здатність каналу. Таким чином, мережа NGN повинна не лише передавати дані, а й гарантувати дотримання визначених параметрів QoS для кожного класу сервісів.

Безпека в мережах NGN є не менш важливим аспектом, оскільки IP-орієнтована архітектура розширює поверхню потенційних атак. Порушення доступності сервісів, наприклад унаслідок атак типу відмови в обслуговуванні, безпосередньо призводить до зниження якості обслуговування. Аналогічно, компрометація цілісності або конфіденційності даних, зокрема перехоплення або

модифікація пакетів, негативно впливає на довіру користувачів і сприйняття сервісу як надійного.

У зв'язку з цим якість обслуговування та безпека в NGN розглядаються як взаємопов'язані складові єдиного процесу керування мережею. Неможливо забезпечити стабільні параметри QoS без належного рівня захисту від зовнішніх і внутрішніх загроз, так само як і засоби безпеки втрачають ефективність у разі неконтрольованого перевантаження мережі. Саме тому концепція NGN передбачає комплексний інтегрований підхід, за якого механізми забезпечення QoS та засоби інформаційної безпеки впроваджуються та узгоджено функціонують на всіх рівнях архітектури мережі — від доступу й транспорту до рівня керування та сервісних платформ.

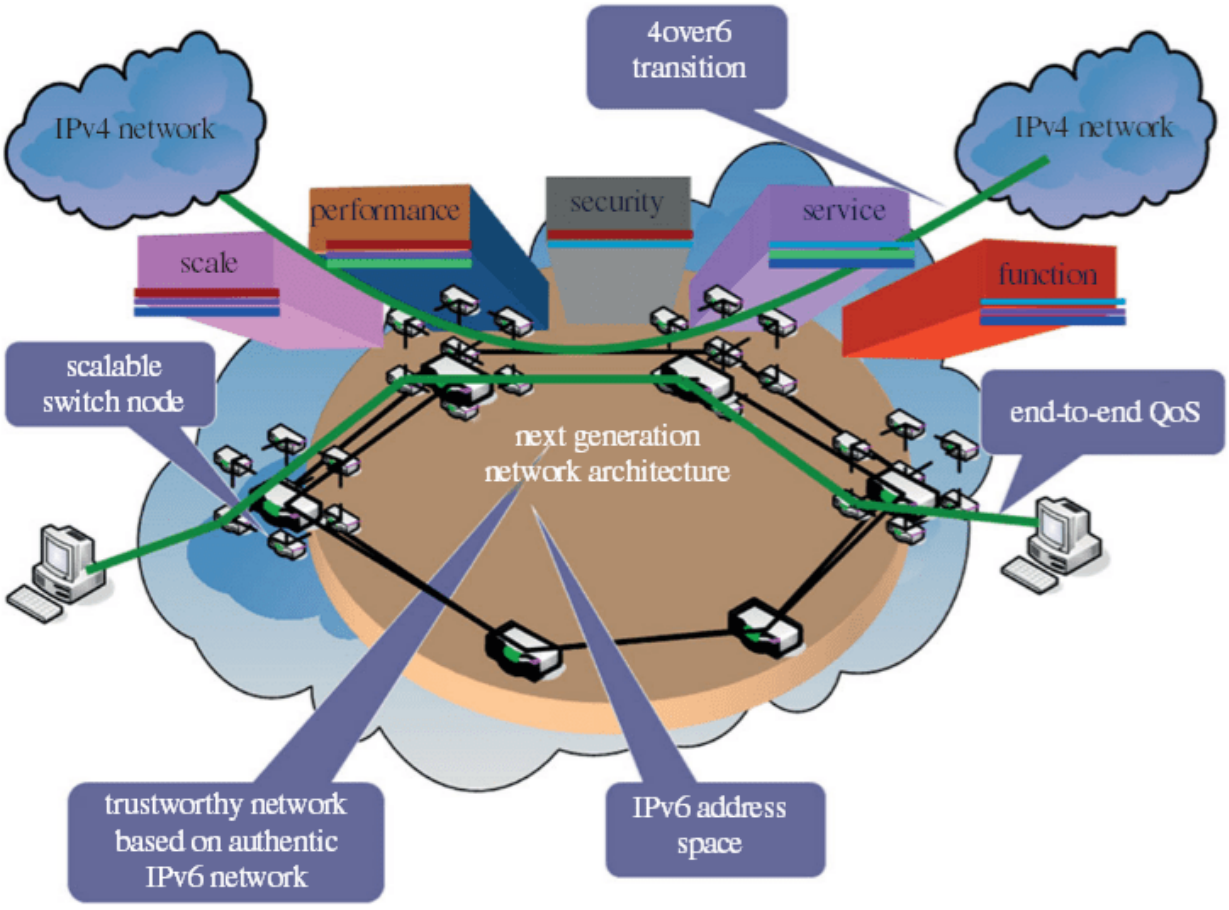


Рис. 2.2 Інтеграція "performance/QoS", "security" і "service" як взаємопов'язані складові в архітектурі мережі наступного покоління

Такий підхід дозволяє NGN підтримувати стабільну роботу конвергентних сервісів навіть у складних умовах змінного навантаження, забезпечуючи при цьому захист інформації та відповідність вимогам сучасних телекомунікаційних систем.

Поняття якості обслуговування в мережах NGN

Під якістю обслуговування (Quality of Service, QoS) у мережах NGN розуміють сукупність кількісних і якісних параметрів, що характеризують здатність мережі передавати інформацію з наперед заданими характеристиками, необхідними для коректного функціонування конкретного сервісу. У межах однієї мережі NGN одночасно можуть функціонувати сервіси з принципово різними вимогами до швидкодії, надійності та стабільності передавання даних — від передачі голосу та відео в реальному часі до асинхронного обміну даними, веб-доступу або передавання великих файлів.

Особливістю NGN є те, що всі ці сервіси використовують спільну пакетну IP-інфраструктуру, що унеможливлює застосування універсального підходу до обслуговування трафіку. Саме тому забезпечення QoS у таких мережах базується на диференційованому підході, за якого кожному типу сервісу надаються ресурси відповідно до його вимог.

До основних показників якості обслуговування в мережах NGN належать затримка передавання пакетів, варіація затримки (джитер), ймовірність втрати пакетів і доступна пропускна здатність. Затримка характеризує час проходження пакета від джерела до приймача і є критичним параметром для сервісів реального часу. Для голосового зв’язку зазвичай вважається допустимою затримка не більше 150–200 мс, тоді як для відеоконференцій верхня межа може сягати 300 мс без істотного погіршення якості сприйняття.

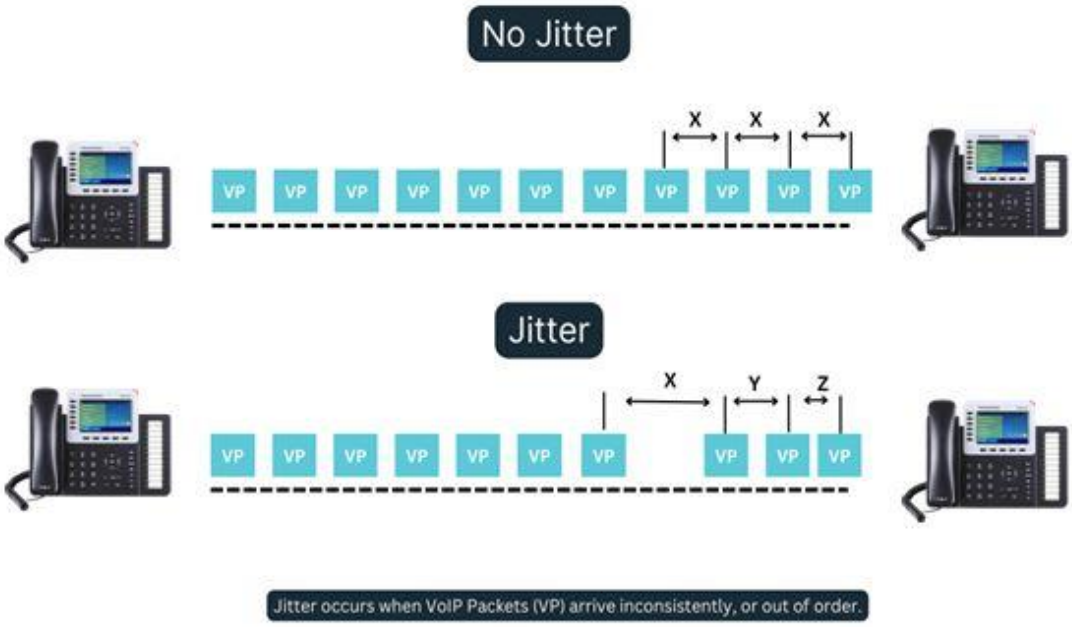


Рис. 2.3 Візуальне пояснення нерівномірного приходу VoIP-пакетів

Варіація затримки, або джитер, відображає коливання часу доставки послідовних пакетів. Навіть за прийнятної середньої затримки надмірний джитер може призводити до спотворення голосу або збоїв у відтворенні відео. Для голосових сервісів допустиме значення джитера зазвичай не перевищує 20–30 мс, тоді як для потокового відео допускаються дещо більші значення за умови використання буферизації.

Ймовірність втрати пакетів є ще одним важливим показником QoS. Для сервісів реального часу втрата пакетів навіть на рівні 1–2 % може бути помітною для користувача, тоді як для сервісів передачі даних така втрата може бути компенсована механізмами повторної передачі. У мережах NGN для критичних сервісів прагнуть забезпечити рівень втрат не вище 0,1 %.

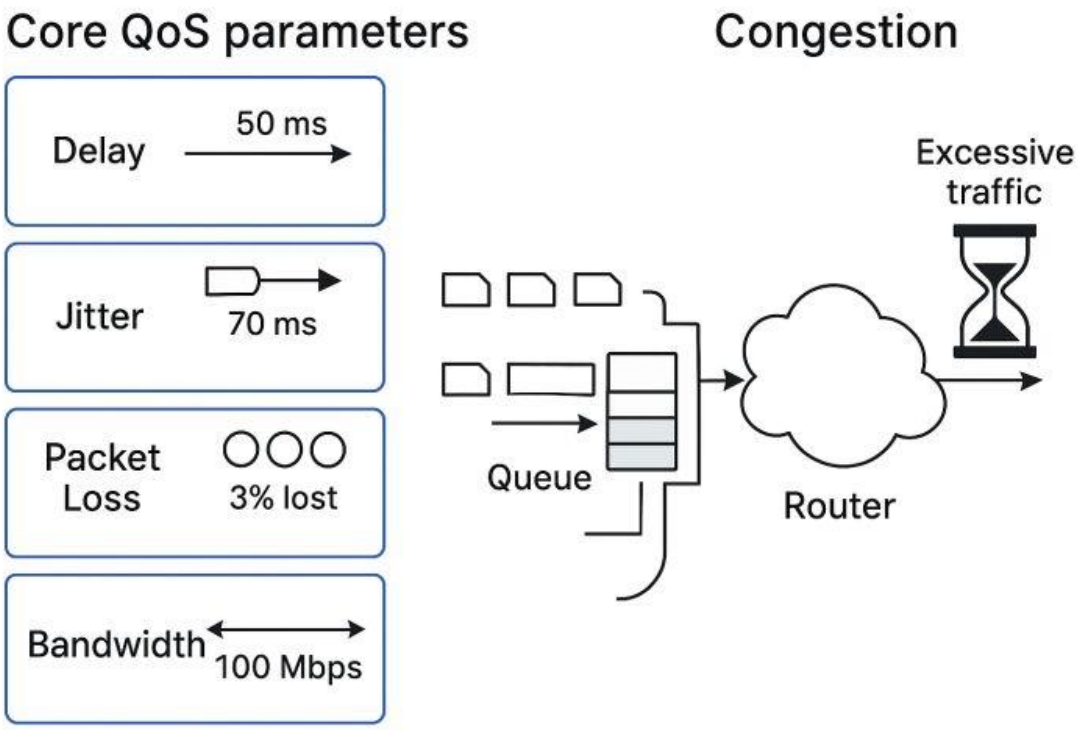


Рис. 2.4 Параметри QoS

Пропускна здатність визначає максимальний обсяг даних, який може бути переданий за одиницю часу, і є ключовим параметром для сервісів передачі даних. Наприклад, для стандартного веб-доступу достатньо кількох мегабіт за секунду, тоді як для передавання відео високої роздільної здатності або хмарних сервісів потрібні значно вищі значення пропускної здатності. У NGN цей параметр динамічно керується залежно від класу сервісу та поточного навантаження мережі.

Таким чином, для сервісів реального часу, зокрема голосового зв’язку та відеоконференцій, критичними є затримка та джитер, тоді як для сервісів передачі даних визначальну роль відіграє пропускна здатність і надійність доставки інформації. Це зумовлює необхідність підтримки в NGN диференційованого обслуговування трафіку, що дозволяє адаптувати параметри передавання даних до вимог конкретного сервісу.

Здатність мереж NGN забезпечувати різні рівні QoS для різних класів трафіку є однією з фундаментальних відмінностей від мереж попередніх поколінь і

водночас ключовою умовою ефективного функціонування конвергентних телекомунікаційних систем.

Механізми забезпечення QoS у мережах NGN

Забезпечення якості обслуговування в NGN реалізується на основі поєднання механізмів класифікації, маркування, пріоритизації та керування трафіком. На етапі надходження трафіку до мережі здійснюється його ідентифікація за типом сервісу, після чого пакети відносяться до відповідного класу обслуговування.

Одним із найбільш поширених підходів є використання моделі диференційованого обслуговування, у межах якої трафік поділяється на кілька класів із різними пріоритетами. Високопріоритетний трафік реального часу отримує гарантовані ресурси, тоді як фоновий трафік обслуговується за залишковим принципом. Такий підхід дозволяє ефективно використовувати пропускну здатність транспортної мережі без суттєвого погіршення якості критичних сервісів.

У NGN важливу роль відіграють системи керування політиками, які визначають правила розподілу ресурсів залежно від типу користувача, сервісу та поточного стану мережі. Ці системи дозволяють динамічно змінювати параметри обслуговування в реальному часі, адаптуючись до змін навантаження та запобігаючи перевантаженню окремих сегментів мережі.

Угоди рівня обслуговування та їх роль у мережах NGN

У практичній діяльності операторів зв’язку забезпечення якості обслуговування (Quality of Service, QoS) нерозривно пов’язане з реалізацією угод рівня обслуговування (Service Level Agreement, SLA). Такі угоди є формалізованим інструментом взаємодії між оператором і споживачем послуг та визначають гарантовані параметри якості, яких має дотримуватися мережа під час надання конкретних сервісів або обслуговування певних категорій користувачів.

SLA, як правило, містять чітко визначені допустимі значення ключових показників якості, зокрема затримки передавання даних, варіації затримки (джитера), рівня втрат пакетів, доступної пропускної здатності, часу відновлення сервісу та показників доступності мережі. Для різних типів сервісів ці параметри

можуть суттєво відрізнятися: наприклад, для голосових і відеосервісів критичними є затримка та джитер, тоді як для сервісів передачі даних пріоритет надається пропускній здатності та стабільності з’єднання.

В умовах мереж наступного покоління (NGN) роль SLA значно зростає у зв’язку з конвергенцією сервісів і спільним використанням мережевих ресурсів. Оскільки різнорідні сервіси — голос, відео, дані, мультимедіа та спеціалізовані корпоративні застосунки — функціонують у межах єдиної пакетної інфраструктури, необхідно забезпечити гнучкий і керований розподіл ресурсів відповідно до умов SLA. Саме SLA стають основою для формування політик керування трафіком і пріоритизації сервісів у NGN.

Реалізація механізмів SLA в NGN здійснюється за допомогою автоматизованих систем моніторингу та керування, які безперервно збирають статистичні дані про стан мережі та параметри трафіку. Отримані показники порівнюються із заданими значеннями, визначеними в угодах SLA, що дозволяє оперативно виявляти відхилення та потенційні порушення якості обслуговування. Такий підхід забезпечує прозорість і об’єктивність оцінювання роботи мережі як для оператора, так і для споживача послуг.

У разі виявлення порушень умов SLA системи керування NGN можуть автоматично ініціювати коригувальні дії. До таких дій належать зміна маршрутів передавання трафіку, перерозподіл пропускної здатності між сервісами, зміна пріоритетів обслуговування або залучення резервних ресурсів мережі. Завдяки цьому NGN здатні не лише фіксувати порушення, а й динамічно адаптувати свою поведінку, мінімізуючи вплив несприятливих факторів на кінцевих користувачів.

Крім технічного аспекту, SLA виконують і економічну та організаційну функцію, оскільки визначають відповідальність оператора за якість наданих послуг та можуть містити механізми компенсації у разі невиконання договірних зобов’язань. Це стимулює операторів до впровадження сучасних технологій керування трафіком, оптимізації архітектури NGN та підвищення загального рівня надійності мережі.

Таким чином, угоди рівня обслуговування є ключовим елементом управління якістю в NGN, що поєднує технічні механізми QoS із бізнес-вимогами та очікуваннями користувачів. Використання SLA дозволяє забезпечити передбачувану якість сервісів, ефективно управляти мережевими ресурсами та створює основу для надання диференційованих послуг у межах сучасних телекомунікаційних систем.

Загрози безпеці в мережах NGN

Перехід до IP-орієнтованої архітектури значно розширює функціональні можливості мережі, але водночас збільшує кількість потенційних загроз безпеці. Мережі NGN успадковують типові загрози комп'ютерних мереж, зокрема несанкціонований доступ, перехоплення трафіку, атаки типу відмови в обслуговуванні та спроби підміни мережевих елементів.

Особливу небезпеку становлять атаки, спрямовані на порушення доступності сервісів, оскільки навіть короткочасна деградація якості може призвести до значних фінансових втрат і зниження довіри користувачів. Крім того, у мережах NGN актуальними залишаються загрози, пов'язані з сигналізацією та керуванням сесіями, оскільки компрометація цих компонентів може мати системний характер.

Механізми забезпечення безпеки в NGN

Забезпечення безпеки в NGN реалізується на основі багаторівневого підходу, який охоплює всі елементи архітектури — від рівня доступу до сервісних платформ. Основними напрямами захисту є автентифікація користувачів і мережевих елементів, контроль доступу, шифрування переданих даних і забезпечення цілісності інформації.

На рівні доступу застосовуються механізми автентифікації абонентів, що дозволяють запобігти несанкціонованому підключенню до мережі. На транспортному рівні використовуються криптографічні методи захисту каналів зв'язку, які унеможливлюють перехоплення або модифікацію даних. Рівень керування захищається за допомогою механізмів взаємної автентифікації та контролю прав доступу між мережевими компонентами.

Особливу увагу в NGN приділено захисту сигналізації, оскільки саме вона визначає логіку встановлення та завершення з’єднань. Використання сучасних протоколів керування та захищених інтерфейсів значно знижує ризик атак, характерних для попередніх поколінь телекомунікаційних мереж.

Взаємозв’язок якості обслуговування та безпеки в мережах NGN

Якість обслуговування (Quality of Service, QoS) та інформаційна безпека в мережах наступного покоління (NGN) не можуть розглядатися як незалежні складові, оскільки між ними існує тісний і багатовимірний взаємозв’язок. Порушення одного з цих аспектів неминуче призводить до деградації іншого, що безпосередньо впливає на стабільність функціонування мережі та сприйняття якості сервісів кінцевими користувачами.

З одного боку, загрози безпеці мають прямий вплив на показники QoS. Класичним прикладом є атаки типу відмови в обслуговуванні (Denial of Service, DoS / Distributed DoS), які призводять до перевантаження мережевих ресурсів, зростання затримок, підвищення рівня втрат пакетів і зниження доступної пропускної здатності. У результаті навіть легітимний трафік не може бути обслуговий із заданими параметрами якості, що порушує умови SLA та знижує довіру користувачів до мережі.

З іншого боку, неефективні або неправильно налаштовані механізми QoS самі по собі можуть створювати передумови для реалізації кібератак. Наприклад, відсутність чіткої класифікації та пріоритизації трафіку дозволяє зловмисникам маскувати шкідливі потоки під легітимний трафік або використовувати фонові сервіси для прихованого виснаження мережевих ресурсів. У таких умовах мережа стає вразливою до атак типу *low-and-slow*, які важко виявити традиційними засобами моніторингу.

В умовах конвергентної архітектури NGN, де голосові, відео- та дані-сервіси передаються спільною пакетною інфраструктурою, інтеграція механізмів QoS і безпеки набуває особливої актуальності. Комплексний підхід до проєктування NGN передбачає використання єдиних політик керування, які одночасно враховують вимоги до якості обслуговування та критерії безпеки. Це дозволяє реалізувати

динамічне керування трафіком із урахуванням як пріоритетності сервісів, так і рівня довіри до джерел трафіку.

Сучасні NGN-мережі використовують інтелектуальні системи керування та моніторингу, здатні аналізувати стан мережі в реальному часі. Такі системи можуть не лише виявляти аномалії, що свідчать про можливі атаки, а й автоматично застосовувати коригувальні дії, зберігаючи прийнятний рівень QoS для критично важливих сервісів. Наприклад, у разі виявлення підозрілої активності трафік може бути обмежений або ізольований без істотного впливу на роботу пріоритетних сервісів.

Інтеграція QoS і безпеки також має важливе значення для виконання угод рівня обслуговування (SLA). Захисні механізми, такі як фільтрація трафіку, автентифікація та шифрування, повинні впроваджуватися таким чином, щоб не погіршувати параметри QoS нижче допустимих значень. Водночас механізми QoS мають бути здатними адаптуватися до дій систем безпеки, забезпечуючи стабільну роботу мережі навіть у разі підвищеного рівня загроз.

Таким чином, інтеграція механізмів якості обслуговування та безпеки є однією з ключових переваг мереж NGN порівняно з традиційними телекомунікаційними системами. Саме цей підхід дозволяє забезпечити не лише високу якість надання сервісів, а й стійкість мережі до зовнішніх і внутрішніх загроз, що є критично важливим у сучасних умовах зростаючої складності та динамічності телекомунікаційних середовищ.

3 ВИКОРИСТАННЯ ПОТУЖНИХ ЦОД ДЛЯ МОДЕРНІЗАЦІЇ NGN

3.1 Технологія 400GE в ЦОД

У 2020 році провідні міжнародні вендори оголосили про початок ери інтерфейсів 400 GE, що ознаменувало новий етап розвитку високошвидкісних мереж передачі даних. Проте ринок сприйняв цю заяву з певною обережністю та здоровим скепсисом. У професійному середовищі на той момент активно обговорювалося поняття digital disrupt — цифровий злам або потрясіння, якого галузь намагалася уникнути. Існувало переконання, що наявні технологічні рішення ще мають потенціал для подальшої еволюційної модернізації без різких змін.

Крім того, не для всіх учасників ринку було очевидно, що саме є першопричиною цього технологічного стрибка: зростання швидкості як самоціль чи реальна об’єктивна потреба, зумовлена новими типами навантажень і сервісів. Щоб краще зрозуміти передумови таких змін, доцільно коротко повернутися до стану інфраструктури наприкінці 2010-х років.

Багато центрів обробки даних (ЦОД) у той період будувалися з використанням класичної архітектури DCN, яка вважалася перевіреною та зручною з точки зору експлуатації. Такі мережі відзначалися відносною простотою проєктування та реалізації резервних з’єднань, що забезпечувало необхідний рівень надійності. Типовими для того часу були мережеві підключення зі швидкостями 10–25 Гбіт/с, які відповідали більшості прикладних задач.

Паралельно відбувався поступовий перехід від трирівневої архітектури до архітектури Clos, яка дозволяла ефективніше обробляти горизонтальний трафік між серверами. Такий підхід ставав дедалі актуальнішим у зв’язку зі зростанням ролі віртуалізації та розподілених обчислень у датацентрах.

Разом із тим існували стримувальні чинники технологічного характеру. Найбільш поширеним стандартом системного інтерфейсу на той момент залишався PCI Express 3.0, з яким працювало відповідне покоління процесорів. Хоча вже

з’являлися нові версії — PCIe 4.0 та PCIe 5.0, — їх масове впровадження ще не відбулося. Це обмежувало можливості ефективного використання надшвидкісних мережевих адаптерів.

Крім того, підсистема зберігання даних у більшості випадків базувалася на інтерфейсах SATA або SAS, які не були розраховані на високі швидкості введення-виведення. Перехід до більш продуктивних NVMe-накопичувачів лише починався і ще не став стандартом для більшості ЦОД.

В інженерній інфраструктурі датацентрів того часу переважали серверні стійки з питомою потужністю 5–7 кВт, що відповідало типовим вимогам обладнання кінця 2010-х років. Для побудови фізичної мережі широко застосовувалися структуровані кабельні системи (СКС), оптимізовані під базові топології та тодішні швидкості передачі даних. Така інфраструктура добре відповідала поточним потребам, однак не завжди була готова до різкого зростання пропускної здатності, яке передбачала поява 400 GE.

Розглянемо вимоги до технічної складової інформаційно-комунікаційної інфраструктури (ІКІ), які сформувалися протягом останніх п’яти років. В основу подальших міркувань доцільно покласти твердження, що вимоги до мережевої інфраструктури визначаються не безпосередньо бізнесом, а насамперед рівнем розвитку прикладних застосунків і цифрових сервісів. Саме еволюція програмних рішень, їх архітектурна складність і зростаючі вимоги до продуктивності та надійності формують запити до мережі.

Такий підхід узгоджується з положеннями класичної організаційної моделі TOGAF та референсної архітектури IT4IT, запропонованої консорціумом The Open Group, відповідно до яких інформаційні технології розглядаються як цілісна система, орієнтована на підтримку життєвого циклу цифрових продуктів і сервісів. У межах цих моделей саме прикладний рівень визначає функціональні та нефункціональні вимоги до інфраструктурних компонентів, зокрема до мереж зв’язку, систем зберігання та обчислювальних ресурсів.

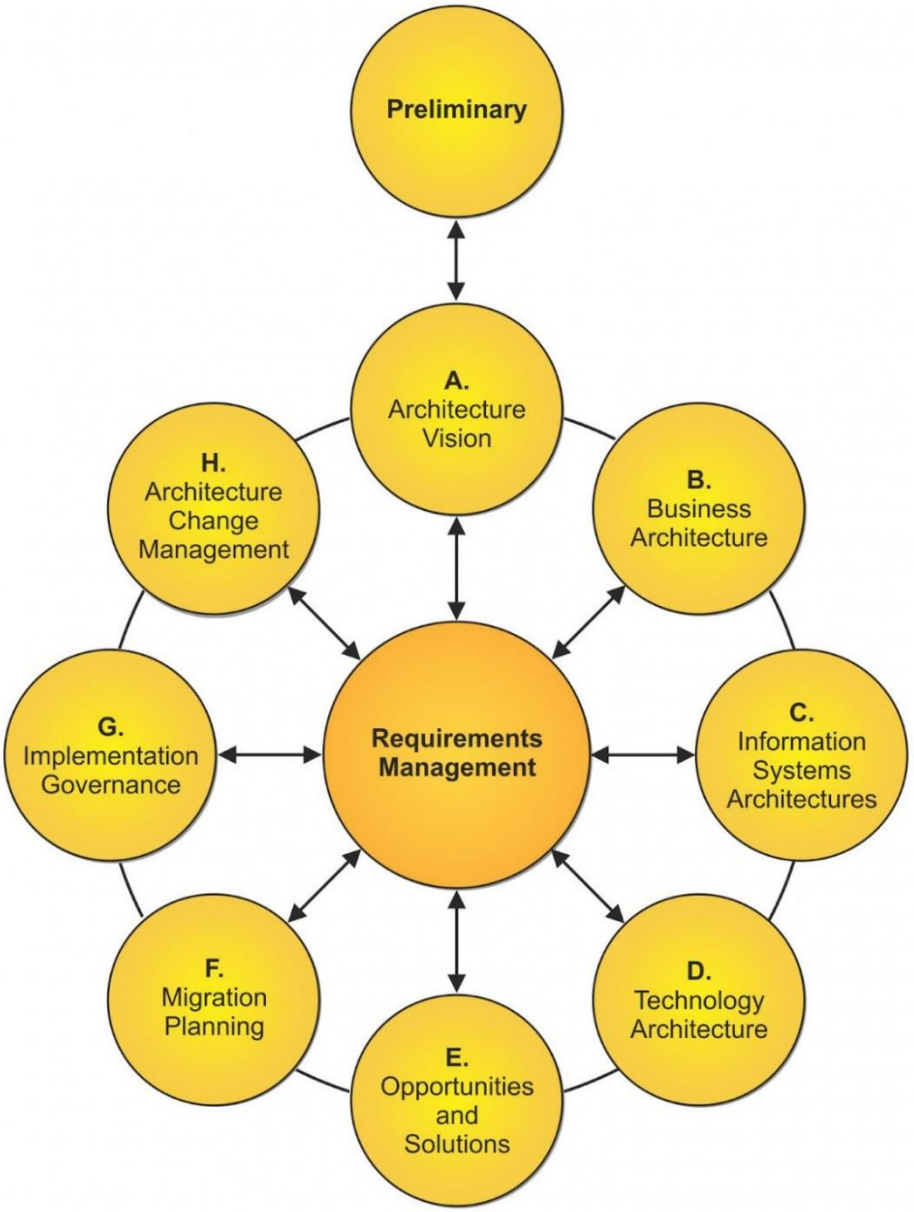


Рис. 3.1 Структура референсної архітектури IT4IT від The Open Group

Стрімке зростання зрілості цифрових технологій, а також їх поступовий перехід від етапу інформаційного ажіотажу до стадії реального практичного впровадження, змусили замовників із бізнес-середовища по-новому переосмислити підходи до якісної трансформації всієї мережевої та інформаційно-комунікаційної інфраструктури. Якщо раніше ключовим фактором розвитку були окремі технологічні інновації, то сьогодні в центрі уваги опинилася системна модернізація мереж, орієнтована на довгострокову стабільність, масштабованість і відповідність вимогам сучасних застосунків.

Особливо чітко ця тенденція проявилася в прагненні компаній орієнтуватися на архітектурні моделі технологічних лідерів світового ринку, які першими зіткнулися з проблемами масштабування, обробки великих обсягів даних і забезпечення безперервності цифрових сервісів. Саме їхній досвід показав, що подальший розвиток неможливий без переходу до уніфікованих, пакетних і програмно-керованих мереж, концептуально близьких до ідей NGN.

Аналізуючи сукупність драйверів розвитку різних галузей, можна виділити кілька ключових тенденцій. По-перше, активне формування нових бізнес-моделей та цифрових екосистем призводить до консолідації й трансформації ІКІ-ландшафту великих організацій. Об’єднання сервісів, платформ і даних вимагає створення єдиної мережевої інфраструктури, здатної підтримувати різнорідні сервіси з гарантованими параметрами якості, що безпосередньо відповідає принципам NGN.

По-друге, практичні приклади реалізації довгострокових ІТ-стратегій демонструють, що надійність і відмовостійкість мережі стають критично важливими характеристиками. Саме ці вимоги стимулюють перехід від фрагментованих рішень до централізованих і стандартизованих мережевих платформ, де функції керування, транспорту та сервісів чітко розділені, як це передбачено в архітектурі NGN.

По-третє, поширюється практика консолідації обчислювальних і мережевих ресурсів шляхом створення приватних хмарних середовищ для груп компаній або великих організаційних структур. Такий підхід дозволяє відмовитися від ізольованих локальних рішень і перейти до єдиного інфраструктурного ядра, що потребує високопродуктивних, масштабованих і гнучких мереж передачі даних — ще одного ключового елементу концепції NGN.

Застосування зазначених підходів дає змогу поступово відійти від фрагментованої (“лоскутної”) побудови ІКІ та перейти до її якісного оновлення. У цьому контексті можна з високим ступенем упевненості стверджувати, що провідні споживачі цифрових послуг — телекомунікаційна та фінансова сфери, енергетичний сектор, а також державні цифрові сервіси — почали усвідомлювати необхідність прискореного розвитку мережевої інфраструктури.

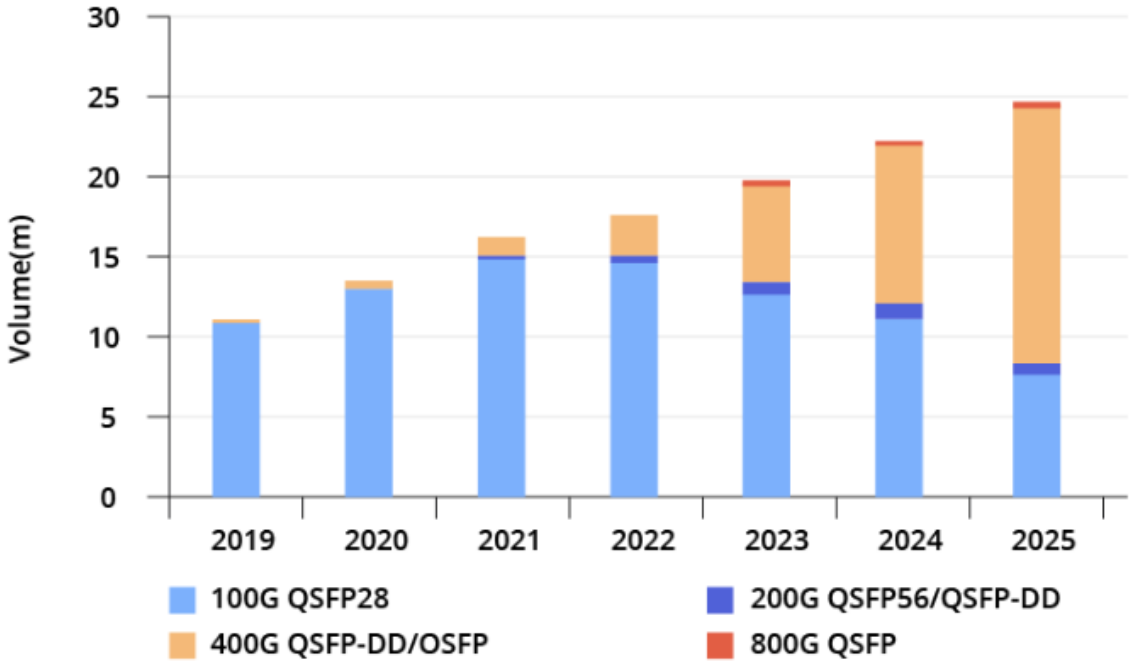


Рис. 3.2 Зміна швидкості мереж за п'ять років та прогноз на найближче майбутнє (на осі Y показаний обсяг відвантажень мережевих пристроїв різних стандартів у мільйонах штук)

Саме мережа, побудована за принципами NGN, здатна перестати бути стримувальним фактором і перетворитися на активний елемент цифрової трансформації, який відповідає зростаючим вимогам бізнесу та високонавантажених сучасних застосунків. Динаміка цих процесів знаходить своє відображення у статистичних показниках розвитку ринку та підтверджує актуальність модернізації мережевої інфраструктури на основі концепції NGN.

3.2 Характеристики 400GE

Основні переваги технології 400GE

Використання 400-гігабітного Ethernet (400GE) забезпечує низку технічних та економічних переваг, які роблять цю технологію доцільною для модернізації сучасних мереж центрів обробки даних і транспортної інфраструктури.

- **Значне збільшення пропускної здатності мережі.** Технологія 400GE дозволяє суттєво підвищити сумарну пропускну здатність

мережі, що забезпечує ефективну обробку великих обсягів трафіку. Це є особливо важливим для центрів обробки даних, хмарних платформ, систем зберігання та сервісів, які працюють з великими масивами даних і потребують високої швидкості обміну інформацією.

- **Підвищення продуктивності прикладних сервісів.** Завдяки зменшенню затримок і збільшенню доступної пропускної здатності забезпечується швидший доступ до застосунків і сервісів, що позитивно впливає на загальну продуктивність інформаційних систем та якість обслуговування користувачів.
- **Оптимізація витрат на мережеву інфраструктуру.** Консолідація кількох з'єднань з нижчими швидкостями в один канал 400GE дозволяє зменшити кількість портів, кабельних з'єднань і мережевого обладнання. Це сприяє зниженню капітальних і експлуатаційних витрат, а також спрощує адміністрування мережі.
- **Зниження енергоспоживання та вимог до фізичної інфраструктури.** Менша кількість активного обладнання призводить до скорочення енергоспоживання, тепловиділення та потреби в додаткових площах для розміщення мережевих пристроїв, що є важливим чинником для масштабних датацентрів.
- **Масштабованість і готовність до зростання навантажень.** Технологія 400GE забезпечує можливість поступового нарощування пропускної здатності без повної заміни існуючої мережевої інфраструктури. Це робить її ефективним рішенням для довгострокового розвитку мереж і підтримки зростаючих потреб бізнесу та цифрових сервісів.

Сфери застосування технології 400GE

Технологія 400-гігабітного Ethernet (400GE) знаходить широке застосування в різних сегментах сучасної інформаційно-комунікаційної інфраструктури, де необхідна передача великих обсягів даних із високою швидкістю та мінімальними затримками.

- **Центри обробки даних (ЦОД).**

У датацентрах технологія 400GE забезпечує значно вищу швидкість обміну даними між серверами, системами зберігання та мережевими комутаторами. Це створює необхідні умови для підтримки масштабної віртуалізації, розподілених обчислень і аналітики великих даних, а також для ефективної роботи сучасних хмарних платформ.

- **Хмарні сервіси та платформи.**

  З розвитком хмарних обчислень 400GE дозволяє оперативно передавати дані між фізичними пристроями та хмарними сервісами. Це суттєво підвищує продуктивність для користувачів застосунків, які потребують великої пропускної здатності, зокрема мереж доставки контенту (CDN), потокових відеосервісів, а також корпоративних інформаційних систем типу ERP.

- **Телекомунікаційні мережі.**

  У телекомунікаційних інфраструктурах базові мережі та периферійні вузли потребують значного збільшення пропускної здатності. Використання Ethernet-каналів зі швидкістю 400 Гбіт/с дозволяє обробляти інтенсивний трафік, зумовлений зростанням абонентської бази та впровадженням нових сервісів, зокрема мереж мобільного зв’язку п’ятого покоління (5G).

- **Високопродуктивні обчислення (HPC) та системи штучного інтелекту.**

  У середовищах високопродуктивних обчислень, де критично важливими є мінімальні затримки та висока швидкість обміну даними, технологія 400GE використовується для з’єднання обчислювальних кластерів у межах однієї або кількох серверних стійок. Це забезпечує ефективну взаємодію між вузлами та дає змогу виконувати складні обчислення, зокрема моделювання та аналіз великих масивів наукових даних, зібраних із розподілених джерел.

- **Магістральні та транспортні мережі.**

  У зв’язку з постійним експоненційним зростанням обсягів інтернет-трафіку провайдери послуг змушені впроваджувати нові високошвидкісні технології. Використання портів Ethernet 400G на магістральних маршрутизаторах дозволяє ефективно передавати пакети на великі відстані, задовольняючи

зростаючий попит на пропускну здатність, зокрема з урахуванням активного розвитку мереж доставки контенту (CDN).

Еволюція стандартів Ethernet: від 10 до 400 Гбіт/с

Стандарт 10 Gigabit Ethernet (10GE), який почав активно впроваджуватися на початку 2000-х років, став важливим етапом у розвитку високошвидкісних мереж і суттєво розширив можливості мережевих застосунків у центрах обробки даних. Перехід до швидкостей 10 Гбіт/с дозволив значно підвищити продуктивність серверних з'єднань, оптимізувати обмін даними між обчислювальними ресурсами та створити основу для подальшого розвитку віртуалізації й розподілених систем.

У міру зростання обсягів мережевого трафіку та ускладнення цифрових сервісів Інститут інженерів з електротехніки та електроніки (IEEE) ініціював розробку наступних стандартів — 40G та 100G Ethernet. Їх поява була зумовлена стрімким збільшенням потреб у пропускній здатності, зокрема з боку великих датацентрів, хмарних платформ і провайдерів інтернет-послуг. Нові стандарти дали змогу істотно підвищити швидкість передавання даних, водночас зберігши принцип зворотної сумісності з наявною мережевою інфраструктурою, що значно спростило їх інтеграцію в існуючі мережі.

Наступним важливим кроком в еволюції Ethernet стало ухвалення у 2017 році специфікації 400 Gigabit Ethernet (400GE), закріпленої в стандарті IEEE 802.3bs. Запровадження 400GE ознаменувало суттєвий технологічний стрибок і було безпосередньо пов'язане з потребами сучасних цифрових середовищ. Надвисокі швидкості передавання даних стали необхідними для підтримки хмарних обчислень, аналітики великих даних, сервісів штучного інтелекту та потокового відео високої роздільної здатності, які формують основне навантаження на мережі нового покоління.

Показовим є те, що еволюцію стандартів Ethernet від 10 до 400 Гбіт/с у наочній формі проілюстрував автор теорії обмежень (Theory of Constraints, TOC) Еліяху Голдратт у своїй праці *«Критичний ланцюг»*. Наведені ним узагальнюючі таблиці та схеми не лише містять довідкову інформацію щодо зростання

швидкостей, а й демонструють зміну підходів до обґрунтування необхідності нових стандартів.

Зокрема, з аналізу цих матеріалів видно, що IEEE поступово змістив акценти з абстрактної «датацентрової» орієнтації на чітко визначені прикладні сфери, які стали основними драйверами прискорення розробки нових стандартів Ethernet. До таких сфер належать хмарні платформи, глобальні мережі доставки контенту, високопродуктивні обчислення та телекомунікаційні магістралі. Саме їхні зростаючі вимоги до пропускної здатності, затримок і масштабованості зумовили перехід від поступової еволюції до стрибкоподібного збільшення швидкостей передавання даних.

Таким чином, розвиток стандартів Ethernet від 10 до 400 Гбіт/с відображає загальну логіку еволюції мережевих технологій — від задоволення локальних потреб датацентрів до підтримки глобальних цифрових екосистем, що є невід'ємною складовою сучасної інформаційно-комунікаційної інфраструктури.

Таблиця 3.1

Параметри стандартів Ethernet

Стандарт Ethernet	**Рік ратифікації**	**Коротка характеристика стандарту**
1GE (1GbE)	1998	Стандарт **1 Gigabit Ethernet (IEEE 802.3z)** був ратифікований у 1998 році та став основою для масового поширення Ethernet-мереж у 2000-х роках. Забезпечував пропускну здатність 1 Гбіт/с з використанням мідних і волоконно-оптичних кабелів.
10GE (10GbE)	2002	Стандарт **10 Gigabit Ethernet (IEEE 802.3ae)** затверджено у 2002 році. Він забезпечив суттєве зростання швидкості передавання даних, необхідне для серверних рішень і центрів обробки даних. Підтримує як мідні, так і оптичні інтерфейси.
25GE (25GbE)	2016	Стандарт **25 Gigabit Ethernet (IEEE 802.3by)** був ратифікований у 2016 році як ефективне рішення для серверів і систем зберігання даних. Забезпечує підвищену пропускну здатність за нижчої вартості порівняно з 40GbE.

Продовження таблиці 3.1

Стандарт Ethernet	**Рік ратифікації**	**Коротка характеристика стандарту**
100GE (100GbE)	2010	Стандарт **100 Gigabit Ethernet (IEEE 802.3ba)** прийнято у 2010 році. Орієнтований на високошвидкісні з'єднання всередині та між дата-центрами, підтримує хмарні сервіси, обробку великих даних і високопродуктивні обчислення.
200GE (200GbE)	2017	Стандарт **200 Gigabit Ethernet (IEEE 802.3bs)** був затверджений у 2017 році. Став важливим етапом розвитку масштабованих датацентрових мереж, забезпечивши подвоєння пропускної здатності порівняно зі 100GbE.
400GE (400GbE)	2017	Стандарт **400 Gigabit Ethernet (IEEE 802.3bs)** ратифіковано у 2017 році одночасно з 200GbE. Розроблений для задоволення зростаючих вимог до пропускної здатності в великих хмарних та високопродуктивних дата-центрах.
800GE (800GbE)	2020	Стандарт **800 Gigabit Ethernet (IEEE 802.3df)** був прийнятий у 2020 році. Забезпечує подвоєння пропускної здатності 400GbE та призначений для надвисокошвидкісних з'єднань у масштабних хмарних інфраструктурах.
1600GE (1.6TbE)	2023	Стандарт **1600 Gigabit Ethernet (IEEE 802.3dj)** був запропонований і ратифікований у 2023 році. Орієнтований на найбільші хмарні та наукові дата-центри, зокрема для задач штучного інтелекту та обробки надвеликих обсягів даних.

Варіанти трансиверів та методів модуляції

Вибір конкретного типу мережевого обладнання, як правило, визначається поставленими технічними завданнями та архітектурою наявної інфраструктури, яка вже функціонує в центрі обробки даних. Значну роль при цьому відіграє сумісність нового обладнання з існуючими мережевими компонентами, що безпосередньо впливає на складність і вартість модернізації.

Особливості роботи зі спадковим обладнанням доцільно розглядати окремо, оскільки оцінка співвідношення переваг і ризиків у таких сценаріях потребує детального аналізу та може бути предметом окремого дослідження. У межах даного

розгляду зосередимося на ключовому технічному аспекті — інтеграції нових і наявних сегментів мережі в єдину інфраструктуру.

Для вирішення цього завдання застосовуються трансивери — спеціалізовані пристрої, призначені для перетворення електричних або оптичних сигналів з одного формату в інший. Використання трансиверів дає змогу передавати дані різними типами фізичних середовищ, зокрема мідними та волоконно-оптичними кабелями, забезпечуючи взаємодію між мережевими елементами з різними інтерфейсами та параметрами передавання.

Таблиця 3.2

Характеристики обладнання

Тип трансивера	**Швидкість**	**Тип кабелю**	**Дальність передавання**	**Кількість ліній**	**Метод модуляції**	**Сфера застосування**
CFP8	400 Гбіт/с	SMF, MMF	SMF: до 100 км; MMF: до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Високошвидкісні з'єднання у великих дата-центрах, хмарні інфраструктури
QSFP-DD	400 Гбіт/с	SMF, MMF	SMF: до 100 км; MMF: до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Сервери, комутатори та маршрутизатори в центрах обробки даних
OSFP	400 Гбіт/с	SMF, MMF	SMF: до 100 км; MMF: до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Високощільні підключення в центрах обробки даних

Продовження таблиці 3.2

Тип трансивера	**Швидкість**	**Тип кабелю**	**Дальність передавання**	**Кількість ліній**	**Метод модуляції**	**Сфера застосування**
400G SR8	400 Гбіт/с	MMF	до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Короткі з’єднання в межах одного дата-центра
400G DR4	400 Гбіт/с	SMF	до 500 м (MMF) / до 2 км (SMF)	4 (4×100G)	DP-QPSK (квадратурна фазова маніпуляція з подвійною поляризацією)	Міжсегментні та міждатацентрові з’єднання
400G FR4	400 Гбіт/с	SMF	до 2 км	4 (4×100G)	DP-QPSK (квадратурна фазова маніпуляція з подвійною поляризацією)	Довгі з’єднання між дата-центрами та міжмережеві канали

Вибір трансиверів для проєктів, що реалізуються за стандартом 400GE, значною мірою визначається типом ASIC-чипа мережевого обладнання та використовуваною схемою модуляції. Зокрема, модуляція PAM4 застосовується в режимах 100/200/400GE, тоді як модуляція NRZ характерна для режимів 50/100/200GE. Ці схеми модуляції є взаємно несумісними, що необхідно обов’язково враховувати під час підбору обладнання. Окрім цього, вибір трансиверів здійснюється з урахуванням конкретного сценарію використання та технічних рекомендацій, наведених у відповідних таблицях сумісності й коментарів виробників.

Окрему увагу доцільно приділити можливості використання брейкаут-режиму (breakout mode). У цьому режимі один фізичний порт із високою

пропускною здатністю може бути логічно розділений на кілька портів з меншою швидкістю передавання даних. Наприклад, порт 400GE може працювати у конфігурації 2×200GE або 4×100GE. Такий підхід є корисним у разі поетапного переходу до вищих швидкостей обчислень і передавання інформації, оскільки дозволяє ефективно використовувати наявну інфраструктуру.

Водночас слід враховувати, що для роботи в брейкаут-режимі мережеве обладнання має підтримувати відповідну функціональність на апаратному та програмному рівнях. Крім того, для підключення можуть знадобитися спеціалізовані кабелі або адаптери, сумісні з обраною конфігурацією портів.

Мережеві мікросхеми та їх роль у забезпеченні технологічної незалежності

Постійне зростання вимог користувачів до продуктивності та масштабованості мереж змушує виробників і постачальників мережевого обладнання висувати дедалі вищі вимоги до розробників мікросхем — чипмейкерів. Їхня готовність брати участь у створенні сучасних мережевих чипів за моделлю Merchant Silicon відіграє важливу роль у налагодженні виробництва високотехнологічної продукції на національному рівні та зменшенні залежності від закордонних рішень.

Мережевий комутатор є складним інженерним пристроєм, у якому реалізуються різні алгоритми обробки даних, що зумовлює використання кількох типів мікросхем. Зокрема, застосовується центральний процесор (CPU), який є універсальним, але відносно повільним і енергоємним; спеціалізований ASIC-чип, що забезпечує надвисоку швидкість обробки пакетів і фактично є «серцем» комутатора; а також FPGA, який може бути адаптований користувачем або виробником під специфічні задачі та нестандартні сценарії роботи.

Слід зазначити, що виробники ASIC-мікросхем є одними з найвибагливіших і найпослідовніших партнерів у процесі співпраці. Вони чітко усвідомлюють цінність своїх рішень, адже саме ASIC визначає ключові технічні характеристики мережевого обладнання. За аналогією, ASIC-чип можна порівняти з двигуном автомобіля: завдання виробника комутатора полягає в тому, щоб спроєктувати всю

систему навколо цього «двигуна», інтегрувати його в загальну архітектуру та підготувати технічну документацію для серійного виробництва.

Цей процес є складним і потребує глибокої експертизи, тому формування портфеля продуктів здійснюється з урахуванням обраної технологічної платформи, а також доступності конкретних типів мікросхем на ринку. Водночас ринок мережевих чипів сьогодні пропонує широкий вибір рішень, що наочно демонструє суттєве зростання можливостей мікросхем починаючи з 2010 року, як за продуктивністю, так і за енергоефективністю та функціональністю.

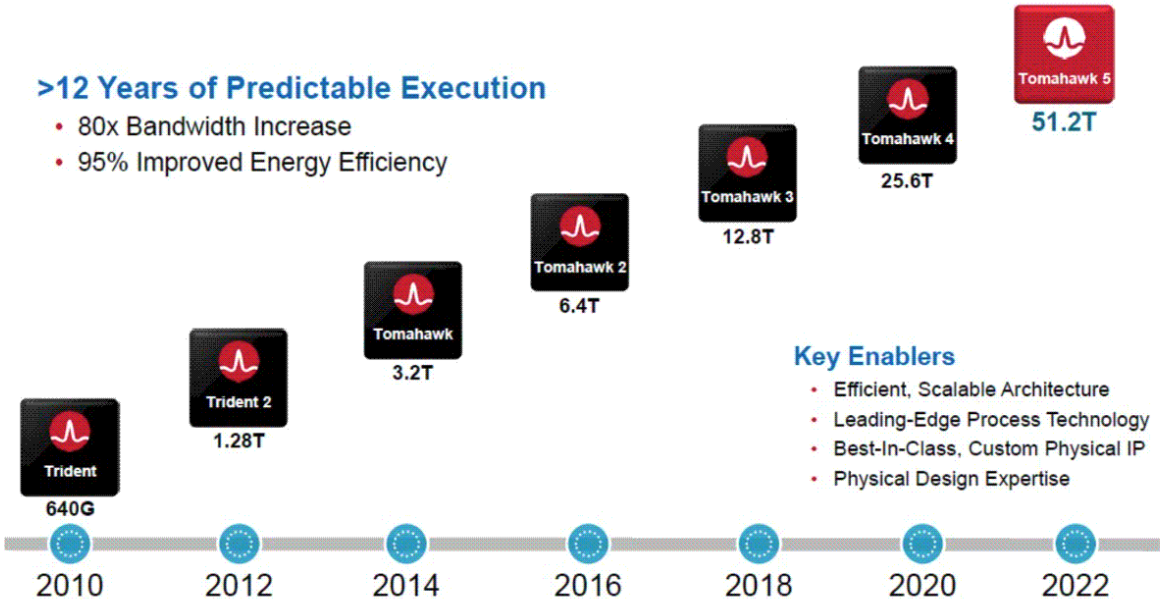


Рис. 3.3 Зростання швидкості передачі даних у міру вдосконалення чіпів на прикладі одного з вендорів Merchant Silicon

3.3 Ethernet 400GE як компонент для апгрейду в мережах NGN

Застосування складних методів сигналізації та сучасних технологій передавання даних дозволяє стандарту 400GE суттєво підвищити пропускну здатність центрів обробки даних — у деяких сценаріях до п’яти разів порівняно з попередніми поколіннями інтерфейсів. Такий ефект досягається за рахунок більш ефективної організації передавання інформації по каналах із надвисокою пропускною здатністю.

У контексті мереж наступного покоління (NGN) технологія 400GE виступає ключовим інфраструктурним компонентом апгрейду транспортного рівня, забезпечуючи необхідний резерв пропускної здатності для підтримки конвергентних сервісів, хмарних платформ і високонавантажених прикладних систем. Завдяки об'єднанню великої кількості потоків даних в один канал із використанням оптичних волокон і сучасних високощільних роз'ємів, 400GE дозволяє зменшити кількість фізичних з'єднань у мережі. Це, у свою чергу, сприяє зниженню затримок, спрощенню кабельної інфраструктури та підвищенню енергоефективності операцій у центрах обробки даних.

Збільшення пропускної здатності ЦОД

Перехід від застарілої схеми модуляції NRZ до більш сучасних методів, таких як PAM4 та DP-QPSK, створює значний технологічний задел для подальшого зростання продуктивності мереж. Саме ці підходи лежать в основі стандартів 400GE та дозволяють реалізувати високі швидкості передавання даних без пропорційного збільшення кількості фізичних ліній.

Водночас використання складніших схем модуляції має і зворотний бік. Сучасні мережеві пристрої, що підтримують 400GE, за рівнем енергоспоживання та тепловиділення вже наближаються до повноцінних серверних систем. У зв'язку з цим у найближчій перспективі при проєктуванні мережевого обладнання для NGN першочергового значення набуватимуть питання оптимізації енергоспоживання та ефективного відведення тепла.

Розв'язання цих задач здійснюватиметься насамперед на рівні фізичного шару, зокрема шляхом удосконалення конструкції трансиверів, підбору матеріалів, оптимізації оптичних компонентів і зменшення втрат сигналу. Такий підхід дозволяє інтегрувати технологію 400GE в архітектуру NGN як еволюційний, але водночас стратегічно важливий крок у модернізації телекомунікаційних мереж.

Застосування 400GE в машинному навчанні, штучному інтелекті та модернізації NGN

У середовищах штучного інтелекту (ШІ) та машинного навчання (ML) впровадження технології 400 Gigabit Ethernet (400GE) набуває особливого

значення, оскільки ці системи працюють з надзвичайно великими обсягами даних і потребують їх швидкої передачі та обробки в режимі, близькому до реального часу. Високошвидкісні мережеві інтерфейси дозволяють ефективно об’єднувати обчислювальні ресурси та забезпечувати інтенсивний обмін даними між вузлами кластерів.

Під час виконання задач у режимі GPU-to-GPU мережа стає критичним елементом загальної продуктивності системи. Якщо архітектура мережі не передбачає механізмів перепідписки або балансування трафіку, потоки даних можуть концентруватися на окремих повільних або нестабільних маршрутах. У результаті це призводить до виникнення вузьких місць і суттєвого зниження ефективності всього обчислювального кластера, незалежно від потужності окремих GPU.

Саме тому на рівні 400GE сьогодні застосовуються не лише класичні підходи до побудови мережевих фабрик, які вже широко використовуються в центрах обробки даних у всьому світі, але й додаткові практики оптимізації. Вони охоплюють як рівні моделі OSI в цілому, так і окремі забезпечувальні шари, зокрема транспортний і канальний, де реалізуються механізми керування потоками, пріоритизації трафіку та мінімізації затримок.

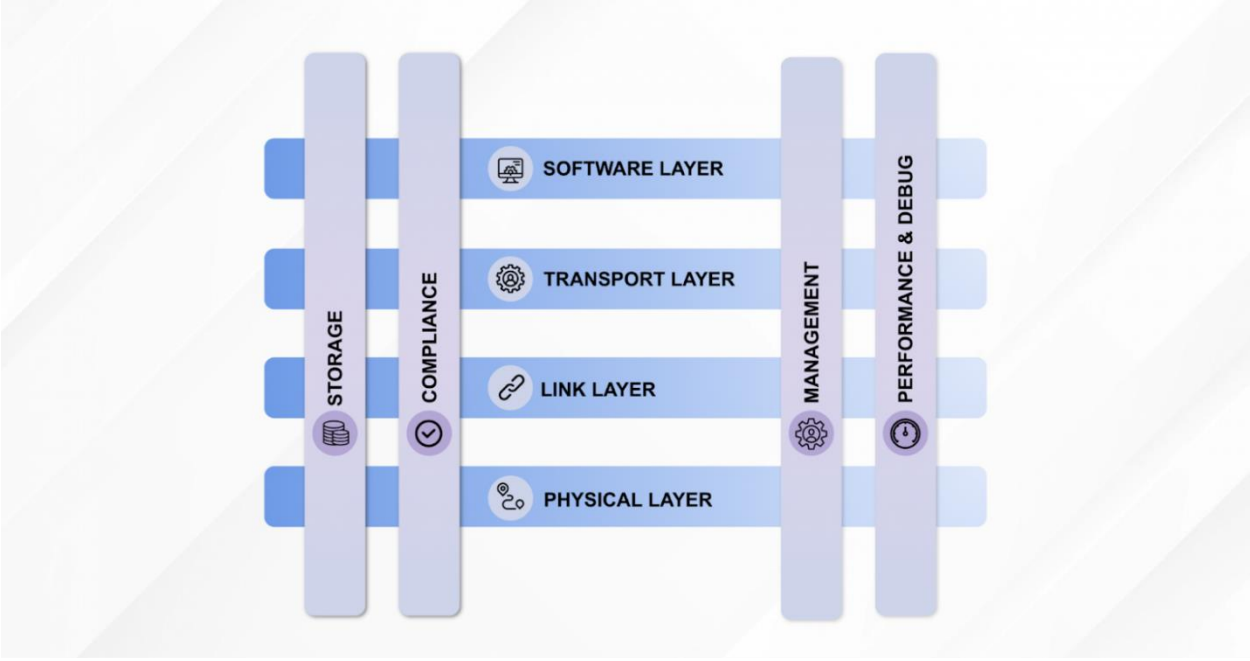


Рис. 3.4 Структура моделі OSI

Технологія 400GE виступає важливим елементом адаптації транспортної інфраструктури до потреб ШІ та ML-навантажень. Висока пропускна здатність, підтримка сучасних методів сигналізації та можливість гнучкого керування трафіком дозволяють інтегрувати 400GE в NGN як основу для побудови масштабованих, відмовостійких і високопродуктивних мереж. Таким чином, поєднання принципів NGN і можливостей 400GE створює технологічний фундамент для ефективної підтримки інтелектуальних обчислювальних систем нового покоління.

Перспективи розвитку мережевих технологій у контексті модернізації NGN

Говорячи про найближче майбутнє мережевих технологій, варто відзначити стандарт PCI Express 6.0, масове впровадження якого очікується, починаючи з 2025 року, а також появу нових класів мережевих прискорювачів, зокрема рішень типу SuperNIC від NVIDIA Mellanox. Ці технології безпосередньо впливають на еволюцію транспортної інфраструктури та формують нові вимоги до мереж наступного покоління.

У матеріалах провідних виробників уже розглядаються сценарії практичного застосування нових стандартів. Так, 400GE планується широко використовувати в мультитенантних дата-центрах, а також у середовищах навчання моделей штучного інтелекту з характерними потоками трафіку East–West та North–South. Водночас для нових високопродуктивних обчислювальних платформ, зокрема NVIDIA Blackwell DGX B200, для досягнення оптимальної ефективності обміну даними між вузлами вже розглядається необхідність застосування 800GE для трафіку типу East–West. Усе це свідчить про те, що мережі NGN мають бути готовими до подальшого кратного зростання пропускної здатності.

Варто зазначити, що сучасні обчислення не обмежуються виключно складними моделями штучного інтелекту. Увесь клас інфраструктур IaaS/PaaS, що використовується гіперскейлерами — великими хмарними провайдерами з десятками тисяч серверів, — активно проходить етап оновлення мережевої інфраструктури. Паралельно відбувається оптимізація частоти та кількості ядер

процесорів, що сприяє підвищенню щільності обчислювальних ресурсів і загальній компактності платформ. У межах NGN це означає зростання ролі високопродуктивного транспортного рівня, здатного обслуговувати інтенсивні міжсерверні потоки даних.

Що стосується фізичного розміщення обладнання в центрах обробки даних, то кількість місць у серверних стійках зростає повільніше, ніж вимоги до щільності обчислювальних потужностей. Це дозволяє й надалі використовувати перевірені архітектурні рішення. Хоча 10–12 років тому моделі розміщення комутаторів EoR/MoR поступилися місцем архітектурі ToR, сучасні чипи Merchant Silicon із пропускною здатністю 25,6–51,2 Тбіт/с створюють можливості для повторного використання окремих елементів існуючої мережевої архітектури в процесі модернізації NGN.

Окремо слід відзначити зростання популярності NVMe та NVMe over Fabrics (NVMeoF) у рамках програмно-визначених систем зберігання даних (SDS). Наприклад, система CEPH, навіть при використанні одного NVMe-накопичувача з двома OSD, здатна забезпечувати швидкість у межах 3–7 ГБ/с. Проте за умов інтенсивного навантаження, зокрема при використанні серверів із 24 NVMe-накопичувачами та синхронною реплікацією даних, критично важливо уникнути виникнення вузьких місць. Для цього необхідно забезпечити наявність щонайменше двох мережевих портів по 400 Гбіт/с, що дозволяє підтримувати стабільну та передбачувану роботу системи.

У сукупності ці тенденції демонструють, що подальший розвиток мережевих технологій тісно пов’язаний із модернізацією мереж NGN, де високошвидкісні інтерфейси 400GE і вище, програмно-керовані механізми та масштабована архітектура стають базовими елементами інфраструктури, здатної підтримувати майбутні цифрові сервіси та обчислювальні навантаження.

4 ПРОБЛЕМИ ТРАФІКА ПРИ МОДЕРНІЗАЦІЇ МЕРЕЖ

4.1 Виявлення слабих місць

Експерти компанії Trend Micro Incorporated у межах дослідження *Securing 5G Through Cyber-Telecom Identity Federation* зосередили увагу на аналізі потенційних уразливостей мереж п’ятого покоління та пошуку підходів, які можуть підвищити рівень їх кібербезпеки. Метою роботи було не лише виявлення слабких місць у сучасних 5G-мережах, а й формування практичних рекомендацій щодо їх усунення з урахуванням особливостей конвергентних телекомунікаційних середовищ.

Як об’єкт дослідження була обрана локальна непублічна мережа NPN (Non-Public Network), розгорнута для умовного гуртожитку з підтримкою технології 5G. Така мережа є прикладом закритої мережі п’ятого покоління, яка обслуговує обмежене коло користувачів, але водночас взаємодіє з «зовнішнім світом» через загальнодоступні телекомунікаційні канали. Подібні сценарії розглядаються як перспективні для застосування на виробничих об’єктах, промислових підприємствах, кампусах і в офісах великих компаній, де потрібен контрольований доступ до мережі з високими вимогами до надійності та безпеки.

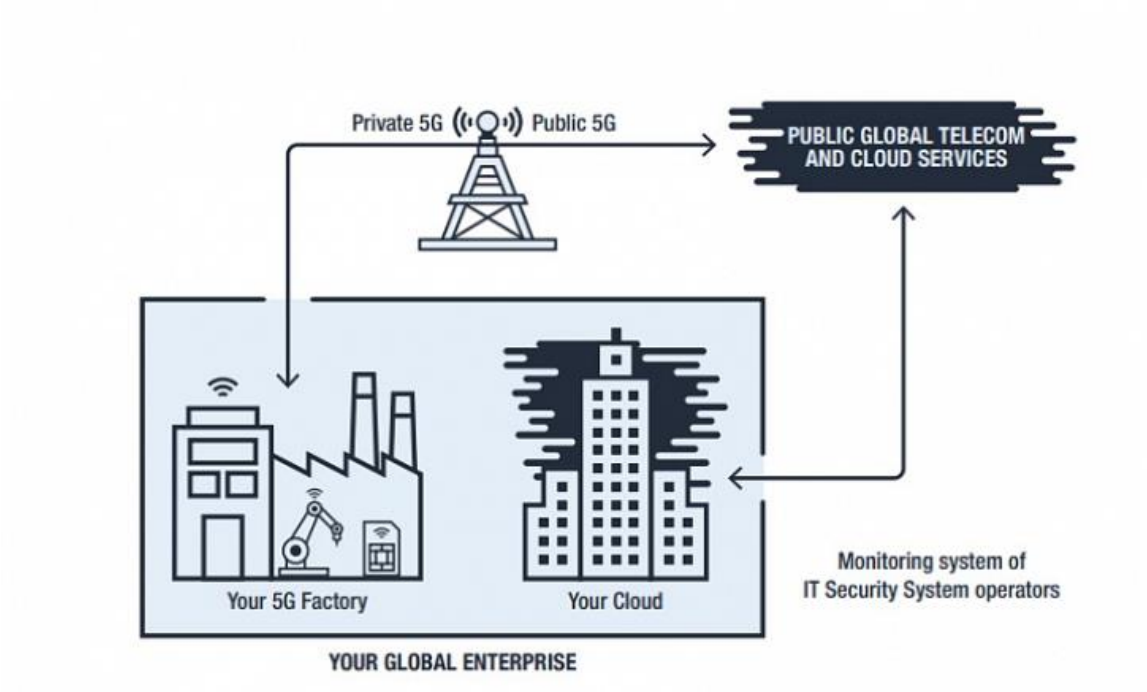


Рис. 4.1 Досліджувана NPN-мережа

У досліджуваній NPN-мережі для автентифікації користувачів і пристроїв застосовуються SIM-карти, які містять унікальні ідентифікаційні дані абонентів, підтримують механізми шифрування та оснащені базовим програмним забезпеченням. Крім того, такі SIM-карти мають можливість віддаленого оновлення програмного забезпечення та мікропрограм, що є важливою функцією для підтримки актуального рівня безпеки без фізичного доступу до обладнання.

З точки зору архітектури мереж наступного покоління (NGN), подібні NPN-рішення є логічним продовженням ідей конвергенції, віртуалізації та сервісно-орієнтованого підходу. NGN передбачає інтеграцію різних типів мереж і сервісів у межах єдиної IP-орієнтованої інфраструктури, а 5G-NPN можна розглядати як спеціалізований випадок такої інтеграції, адаптований під конкретні бізнес- або виробничі сценарії.

Водночас дослідження Trend Micro показало, що поєднання закритих 5G-мереж із відкритими транспортними каналами NGN створює додаткову поверхню атаки. Це вимагає посиленої уваги до питань керування ідентифікацією, автентифікацією та авторизацією, а також до захисту сигнального та користувацького трафіку. Саме тому запропонована концепція федерації ідентичностей у кібер-телекомунікаційному середовищі розглядається як один із перспективних напрямів підвищення безпеки мереж NGN і 5G.

Таким чином, результати цього дослідження підтверджують, що модернізація телекомунікаційних систем у межах NGN має супроводжуватися не лише впровадженням нових технологій доступу та передачі даних, а й розвитком комплексних механізмів безпеки. Особливо це актуально для непублічних 5G-мереж, які дедалі частіше стають частиною загальної NGN-інфраструктури та відіграють важливу роль у цифровій трансформації підприємств і організацій.

Однією з ключових уразливостей досліджуваної архітектури, на думку дослідників, є те, що більшість наявних засобів ТК-безпеки зосереджені виключно на захисті кінцевого об’єкта та його хмарного середовища, але практично не охоплюють трафік, який передається через зовнішні публічні та закриті телекомунікаційні мережі. У мережах NGN де відбувається тісна інтеграція

телекомунікаційних і ТК-систем, така фрагментація підходів до безпеки створює серйозні ризики.

За відсутності наскрізного захисту трафіку стає можливим цілий спектр кібератак, спрямованих на компрометацію телекомунікаційних каналів і самої мережі 5G. Ці атаки можуть мати різні цілі: апаратну частину мережі, дані користувачів або їхні цифрові посвідчення (ідентичності). У середовищі NGN, де мережа є основою для надання критично важливих сервісів, наслідки таких атак можуть виходити далеко за межі суто телекомунікаційної сфери.

Атаки на апаратному рівні

На апаратному рівні однією з найбільш небезпечних загроз є віддалені маніпуляції з SIM-картами, відомі як SIMjacking, особливо в сценаріях роумінгу, тобто під час роботи пристрою поза «домашньою» мережею. У такому випадку зловмисники можуть змінювати налаштування SIM-карти таким чином, що кінцевий пристрій підключатиметься не до легітимної публічної мережі, а до контрольованої зловмисниками мережевої інфраструктури.

Після цього відкривається можливість:

- перехоплення та прослуховування голосових викликів;
- аналізу та модифікації сигнального і користувацького трафіку;
- віддаленого запуску шкідливого програмного забезпечення;
- цілеспрямованого втручання в алгоритми машинного навчання, що використовують дані з мобільних пристроїв або сенсорів.

Атаки на дані та мережеву інфраструктуру

У разі атак, спрямованих на дані та саму мережу, скомпрометована SIM-карта може негативно впливати не лише на роботу окремого пристрою, а й на продуктивність мережі загалом. Зловмисники здатні змінювати базові мережеві параметри, створювати нестабільні з’єднання або штучно підвищувати навантаження на окремі сегменти мережі.

Особливо небезпечними є так звані атаки типу salami та low-and-slow, які реалізуються одночасно з великої кількості пристроїв. За таких умов у мережевій інфраструктурі поступово формуються «сліпі зони», де аномальна активність

залишається непоміченою системами моніторингу. Ці зони можуть бути використані як плацдарм для подальших, значно масштабніших і руйнівніших кібератак, що загрожує стабільності всієї NGN-інфраструктури.

Компрометація посвідчень і міждоменної ідентичності

Окрему категорію становлять атаки, пов'язані з телекомунікаційними каналами та цифровими посвідченнями. Їхня ефективність значною мірою зумовлена невідповідністю підходів до обробки ідентичностей у телекомунікаційних і класичних ТК-системах. У телекомунікаційних мережах більшість посвідчень і облікових даних жорстко прив'язані до SIM-карти та обробляються на апаратному рівні, тоді як в ТК-інфраструктурі керування ідентичністю реалізується переважно на рівні програмного забезпечення.

У результаті, після викрадення або підміни цифрової ідентичності користувача шляхом компрометації SIM-карти, зловмисники можуть отримати доступ не лише до мережі 5G, а й до пов'язаних ТК-систем. У виробничих або корпоративних середовищах NGN це відкриває можливість втручання в бізнес-процеси, зміну параметрів кінцевих продуктів або порушення технологічних циклів.

Таблиця 4.1

Узагальнювальна таблиця типів атак

Тип атаки	**Рівень реалізації**	**Основна ціль**	**Потенційні наслідки для NGN/5G**
SIMjacking	Апаратний (SIM)	Кінцевий пристрій, мережеве підключення	Перехоплення трафіку, підміна мережі, запуск шкідливого ПЗ
Salami / Low-and-slow	Мережевий	Інфраструктура NGN	Формування «сліпих зон», деградація QoS, масштабні атаки
Компрометація ідентичності	Телеком + IT	Посвідчення користувача	Несанкціонований доступ до IT-систем і сервісів
Атаки на ML/AI	Дані та транспорт	Алгоритми ШІ	Спотворення результатів навчання, зниження ефективності

Таким чином, результати дослідження свідчать, що модернізація мереж NGN із використанням 5G повинна супроводжуватися наскрізним підходом до безпеки, який охоплює не лише кінцеві пристрої та хмарні сервіси, а й усі телекомунікаційні канали передавання даних. Лише інтеграція механізмів безпеки на апаратному, мережевому та програмному рівнях здатна забезпечити стійкість NGN-інфраструктури до сучасних і майбутніх кіберзагроз.

4.2 Оптимальні рішення при модернізації мереж

У рамках своїх досліджень фахівці Trend Micro запропонували комплексний підхід до забезпечення безпеки, який передбачає об’єднання механізмів контролю цілісності та захисту мереж передавання даних, SIM-карт, кінцевих пристроїв і зовнішніх телекомунікаційних мереж в єдину інтегровану систему. Такий підхід відповідає сучасним вимогам до мереж наступного покоління, де безпека має реалізовуватися не фрагментарно, а наскрізно — на всіх рівнях архітектури NGN.

Запропонована модель дозволяє здійснювати безперервний моніторинг стану пристроїв і мережевих з’єднань, що дає змогу своєчасно виявляти потенційно «заражені» або скомпрометовані пристрої навіть у межах так званої «домашньої» мережі. У контексті NGN, де велика кількість сервісів і користувачів працює в спільній інфраструктурі, раннє виявлення таких загроз є критично важливим для запобігання їх поширенню на інші сегменти мережі.

Окрему увагу в цій концепції приділено захисту SIM-карт, які в мережах 5G і NGN виступають ключовим елементом ідентифікації та автентифікації користувачів і пристроїв. Інтеграція SIM-карт у загальну систему безпеки дозволяє не лише запобігати їх несанкціонованому використанню, а й захищати від атак, пов’язаних із підміною або перезаписом мікропрограмного забезпечення. Це особливо актуально для сценаріїв використання SIM-карт у промислових мережах, IoT-середовищах та непублічних 5G-мережах.

Крім того, запропонований підхід відкриває можливість застосування елементів блокчейн-технологій для підвищення рівня безпеки SIM-карт і

пов’язаних з ними процесів. Зокрема, розподілені реєстри можуть використовуватися для зберігання та перевірки інформації про стан SIM-карт, їхню автентичність і історію оновлень. Це дозволяє забезпечити незмінність і прозорість даних, а також підвищити довіру до процесів автентифікації, особливо в ситуаціях, коли SIM-карта працює поза межами «домашньої» мережі, наприклад у роумінгу або в гібридних NGN-середовищах.

У результаті реалізація такої інтегрованої системи безпеки дає змогу перейти від ізольованого захисту окремих компонентів до єдиного, узгодженого механізму кіберзахисту, який охоплює як телекомунікаційні, так і IT-складові інфраструктури. Для мереж NGN це означає підвищення стійкості до складних багатовекторних атак, зниження ризиків компрометації ідентичностей і забезпечення надійної роботи конвергентних сервісів у довгостроковій перспективі.

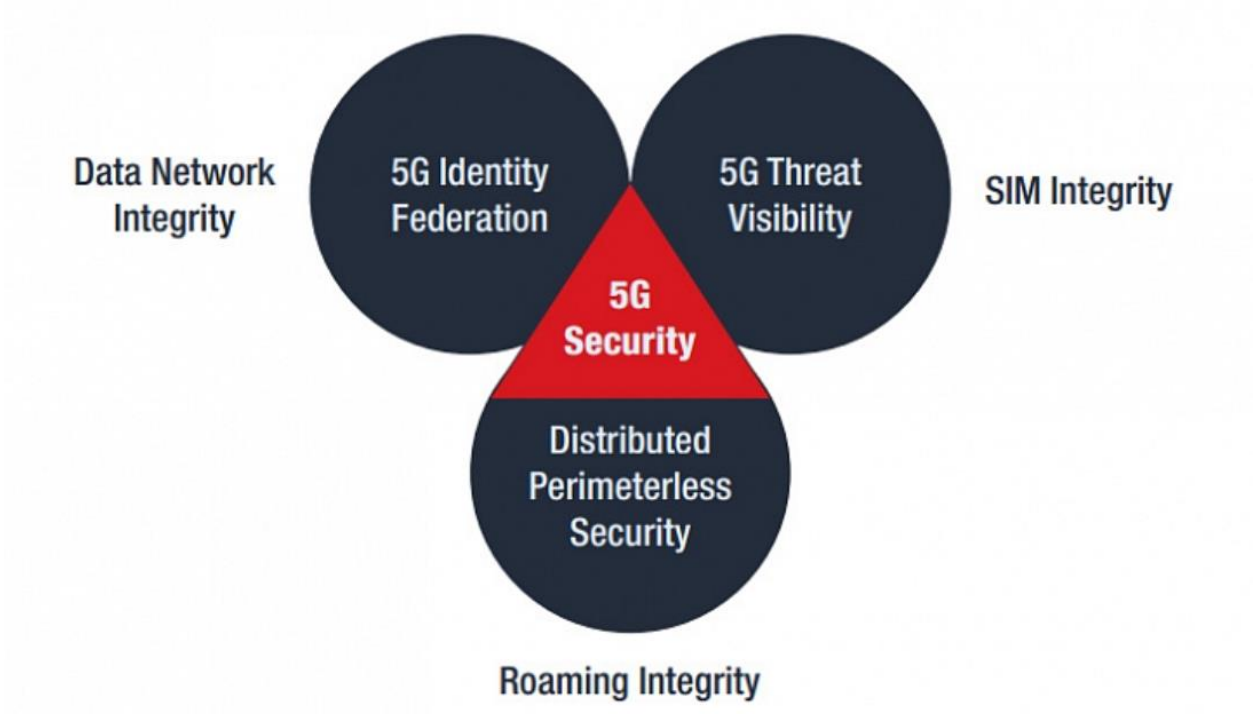


Рис. 4.2 Візуалізація підходу до забезпечення безпеки мереж

Загалом фахівці сходяться на думці, що значна частина компаній, а також цілі галузі економіки, прагнучи скористатися перевагами мереж п’ятого покоління (5G), часто не мають достатнього досвіду роботи з телекомунікаційними технологіями. На відміну від традиційних ТК-систем, мережі 5G і NGN характеризуються високою складністю архітектури, глибокою інтеграцією з транспортною

інфраструктурою та використанням спеціалізованих механізмів керування й безпеки. Це створює додаткові виклики для організацій, які раніше не експлуатували власні телекомунікаційні мережі або не взаємодіяли з ними на глибокому технічному рівні.

У таких умовах компанії можуть зіштовхуватися з труднощами у протидії кібератакам, оскільки зловмисники, у свою чергу, активно аналізують і використовують вразливості нових мережевих технологій. Особливу небезпеку становлять атаки, спрямовані на сигнальні протоколи, механізми автентифікації, керування ідентичністю та взаємодію між телекомунікаційною й ТК-інфраструктурою. У середовищі 5G та NGN навіть локальні порушення безпеки можуть мати системний характер і впливати на великі сегменти мережі.

Для України ці питання є особливо актуальними з огляду на перспективний розвиток 5G та поетапну модернізацію мереж NGN. У найближчі роки очікується розширення використання 5G не лише для масового мобільного доступу, а й для промислових мереж, приватних 5G (NPN), критичної інфраструктури, логістики, енергетики та державних сервісів. Усі ці сценарії передбачають підвищені вимоги до надійності, безперервності роботи та стійкості мереж.

Модернізація NGN в Україні передбачає перехід до пакетно-орієнтованих, програмно-керованих і віртуалізованих мереж, інтеграцію хмарних платформ, впровадження технологій SDN/NFV та використання високошвидкісних транспортних рішень (100GE, 400GE і вище). Водночас без належної підготовки персоналу, розвитку нормативної бази та впровадження комплексних механізмів безпеки такі зміни можуть супроводжуватися зростанням кіберризиків.

Саме тому ключовим напрямом подальшого розвитку має стати поєднання технологічної модернізації NGN із системним підходом до кібербезпеки. Це включає навчання спеціалістів, впровадження наскрізних моделей захисту, інтеграцію телекомунікаційної та IT-безпеки, а також адаптацію міжнародного досвіду до національних умов. Такий підхід дозволить не лише мінімізувати загрози, а й створити надійну основу для сталого розвитку 5G-екосистеми в Україні.

Таблиця 4.2

Виклики та перспективи розвитку 5G і NGN в Україні

Аспект	**Поточний стан / виклик**	**Перспективний напрям розвитку**
Досвід експлуатації	Обмежений досвід роботи з телеком-мережами у бізнесу	Підготовка фахівців, співпраця з операторами
Кібербезпека	Фрагментарний захист, розрив між IT і телеком	Наскрізна модель безпеки NGN + 5G
Архітектура мереж	Перехідний стан від legacy до NGN	SDN/NFV, хмарні ядра, приватні 5G
Транспортна інфраструктура	Обмежені резерви пропускної здатності	Впровадження 100GE/400GE
Сфери застосування	Переважно мобільний доступ	Промисловість, NPN, держсервіси
Регуляторне середовище	Формується	Адаптація європейських стандартів

Таким чином, успішне впровадження 5G в Україні можливе лише за умови синхронної модернізації мереж NGN і розвитку систем кібербезпеки. Без цього переваги нових технологій можуть бути нівельовані зростанням ризиків, тоді як комплексний підхід створює передумови для безпечного й ефективного використання 5G у довгостроковій перспективі.

ВИСНОВКИ

У даній кваліфікаційній роботі було розглянуто питання впровадження технології NGN (Next Generation Networks) при модернізації телекомунікаційних систем та мереж, що є одним із ключових напрямів розвитку сучасної інфраструктури зв'язку. Проведений аналіз показав, що перехід до NGN є об'єктивною необхідністю, зумовленою зростанням вимог до пропускної здатності, гнучкості, масштабованості та безпеки мереж, а також активною конвергенцією сервісів і технологій.

У роботі було простежено еволюцію телекомунікаційних і мобільних мереж від 1G до 5G, що дозволило виявити основні тенденції розвитку архітектур, механізмів керування та засобів захисту інформації. Показано, що якщо в ранніх поколіннях мереж пріоритет надавався доступності сервісів, то в мережах NGN ключового значення набули питання якості обслуговування, безпеки та ефективного використання ресурсів.

Особливу увагу приділено архітектурним принципам побудови NGN, зокрема розподілу мережі на рівні доступу, транспорту, керування та сервісів. Такий підхід забезпечує незалежний розвиток окремих компонентів, спрощує інтеграцію різних технологій доступу та створює умови для ефективної модернізації існуючих телекомунікаційних систем на основі пакетної IP-орієнтованої транспортної мережі.

У межах роботи детально розглянуто механізми забезпечення якості обслуговування (QoS) та їхній зв'язок з угодами рівня обслуговування (SLA). Показано, що використання автоматизованих систем моніторингу й керування дозволяє підтримувати гарантовані параметри якості для різних сервісів і категорій користувачів навіть за умов змінного навантаження.

Значну увагу приділено питанням інформаційної безпеки в NGN і мережах 5G. Аналіз сучасних загроз засвідчив необхідність наскрізного підходу до безпеки, який охоплює телекомунікаційні канали, SIM-карти, механізми ідентифікації та IT-

інфраструктуру. Обґрунтовано, що інтеграція механізмів безпеки та QoS є важливою умовою стабільної та надійної роботи NGN.

Також розглянуто роль високошвидкісних транспортних технологій Ethernet, зокрема 400GE, як важливого елементу модернізації NGN. Показано, що впровадження таких рішень є необхідним для підтримки зростаючих обсягів трафіку в дата-центрах, хмарних платформах, мережах 5G та системах штучного інтелекту, забезпечуючи масштабованість і енергоефективність мереж.

Окремо проаналізовано перспективи розвитку NGN і 5G в Україні, де модернізація телекомунікаційних мереж є важливою складовою цифрової трансформації економіки та розвитку державних і промислових сервісів. Зроблено висновок, що успішне впровадження NGN потребує комплексного підходу, який поєднує технологічне оновлення, розвиток фахових компетенцій і посилення кібербезпеки.

Таким чином, результати кваліфікаційної роботи підтверджують, що технологія NGN є ефективною основою для модернізації телекомунікаційних систем та мереж, забезпечуючи високу якість сервісів, гнучкість керування, масштабованість і стійкість до сучасних загроз. Отримані висновки можуть бути використані під час проєктування та розвитку телекомунікаційної інфраструктури, а також у подальших наукових дослідженнях у сфері мереж наступного покоління.

ПЕРЕЛІК ПОСИЛАНЬ

1. ITU-T Recommendation Y.2001. General overview of NGN. – Geneva : ITU-T, 2004. – 32 p.
2. ETSI ES 282 001. Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture. – Sophia Antipolis : ETSI, 2008.
3. 3GPP TS 23.501. System Architecture for the 5G System (5GS). – Release 17. – Sophia Antipolis : ETSI, 2023.
4. 3GPP TS 23.401. GPRS enhancements for E-UTRAN access (Evolved Packet Core). – Release 16. – Sophia Antipolis : ETSI, 2022.
5. 3GPP TS 33.501. Security architecture and procedures for the 5G System. – Release 17. – Sophia Antipolis : ETSI, 2023.
6. ETSI GS NFV-MAN 001. Network Functions Virtualisation (NFV); Management and Orchestration. – Sophia Antipolis : ETSI, 2014.
7. Bradner S., Nichols K. An Architecture for Differentiated Services : RFC 2475. – IETF, 1998.
8. Rosen E., Viswanathan A., Callon R. Multiprotocol Label Switching Architecture : RFC 3031. – IETF, 2001.
9. Kent S., Seo K. Security Architecture for the Internet Protocol : RFC 4301. – IETF, 2005.
10. Fajardo V. et al. Diameter Base Protocol : RFC 6733. – IETF, 2012.
11. IEEE Std 802.3bs-2017. IEEE Standard for Ethernet – Amendment 10: Media Access Control Parameters, Physical Layers, and Management Parameters for 200 Gb/s and 400 Gb/s Operation. – New York : IEEE, 2017.
12. Trend Micro Incorporated. Securing 5G Through Cyber-Telecom Identity Federation : White Paper. – Tokyo : Trend Micro, 2020.
13. Trend Micro Research. Private 5G Network Security Expectations. – Trend Micro Research Report, 2021.

14. Janevski T. NGN Architectures, Protocols and Services. – Chichester : John Wiley & Sons, 2014. – 480 p.
15. Salina J., Salina P. Next Generation Networks: Perspectives and Potentials. – Hoboken : Wiley, 2007. – 360 p.
16. Alvarez S. QoS for IP/MPLS Networks. – Indianapolis : Cisco Press, 2006. – 528 p.
17. Morreale P. A., Anderson J. M. Software Defined Networking: Design and Deployment. – Boca Raton : CRC Press, 2014. – 420 p.
18. Nadeau T., Gray K. SDN: Software Defined Networks. – Sebastopol : O'Reilly Media, 2013. – 384 p.
19. Russell T. The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations. – New York : McGraw-Hill, 2008. – 368 p.
20. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. – 8th ed. – Boston : Pearson, 2021. – 864 p.
21. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. – 5th ed. – Amsterdam : Elsevier, 2012. – 920 p.
22. Tanenbaum A. S., Wetherall D. J. Computer Networks. – 5th ed. – Boston : Pearson, 2011. – 960 p.
23. Stallings W. Network Security Essentials: Applications and Standards. – 6th ed. – Boston : Pearson, 2017. – 432 p.
24. 3GPP TS 23.228. IP Multimedia Subsystem (IMS); Stage 2. – Release 17. – Sophia Antipolis : ETSI, 2023.
25. ETSI TS 133 501. 5G Security Architecture. – Sophia Antipolis : ETSI, 2023.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Георгій ЖДАНОВИЧ

Назва: ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ NGN ПРИ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Координатор: Володимир РУЖИНСЬКИЙ

Підрозділ: ННІТ

Коефіцієнт подібності 1:0.3

Коефіцієнт подібності 2:0

Тривога: 1

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ NGN ПРИ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

ВИКОНАВ:
СТУДЕНТ ГРУПИ ТСДМ-62
ГЕОРГІЙ ЖДАНОВИЧ

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

- Мета роботи – дослідження принципів побудови та функціонування мереж наступного покоління (NGN) у процесі модернізації телекомунікаційних систем, а також аналіз механізмів керування сервісами, трафіком і забезпечення якості обслуговування та інформаційної безпеки в умовах конвергенції послуг.
- Об’єкт дослідження – телекомунікаційні системи та мережі зв’язку нового покоління, що базуються на пакетно-орієнтованих IP-архітектурах.
- Предмет дослідження – архітектурні рішення мереж NGN, механізми керування трафіком і сервісами, а також методи забезпечення якості обслуговування та інформаційної безпеки в процесі модернізації телекомунікаційних мереж.

Актуальність.

- Актуальність роботи зумовлена стрімким розвитком телекомунікаційних технологій, зростанням обсягів трафіку та переходом від традиційних мереж із комутацією каналів до пакетно-орієнтованих IP-архітектур. Мережі наступного покоління (NGN) забезпечують конвергенцію сервісів, гнучке керування трафіком, масштабованість і підтримку сучасних послуг, зокрема 4G/5G та хмарних сервісів. В умовах підвищених вимог до якості обслуговування й інформаційної безпеки, а також модернізації телекомунікаційної інфраструктури України, дослідження принципів побудови та функціонування NGN є своєчасним і практично значущим.

Архітектура NGN та механізми керування сервісами і трафіком

- Мережі наступного покоління (NGN) — це конвергентна IP-орієнтована телекомунікаційна архітектура, що поєднує різні сервіси (голос, дані, відео) в єдиній інфраструктурі з гарантованими параметрами якості. Основними принципами NGN є пакетна передача даних, модульна багаторівнева архітектура, відокремлення транспорту від керування та сервісів, а також технологічна нейтральність доступу. Ключову роль відіграють політики керування, які забезпечують класифікацію і пріоритизацію трафіку, динамічний розподіл ресурсів, підтримку QoS і виконання SLA. Це дозволяє NGN ефективно працювати за змінних навантажень, масштабуватися та підтримувати сучасні цифрові сервіси.

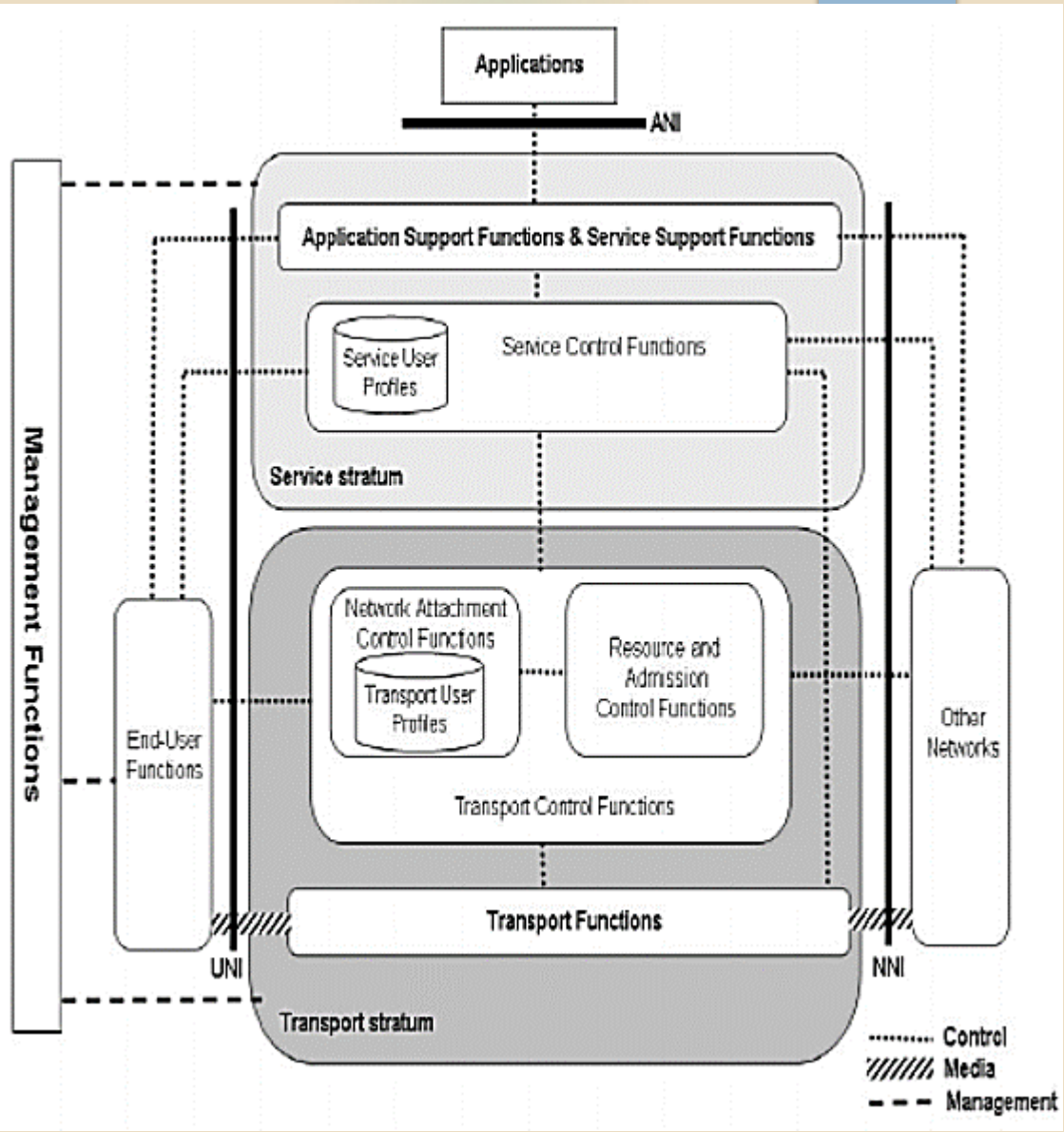
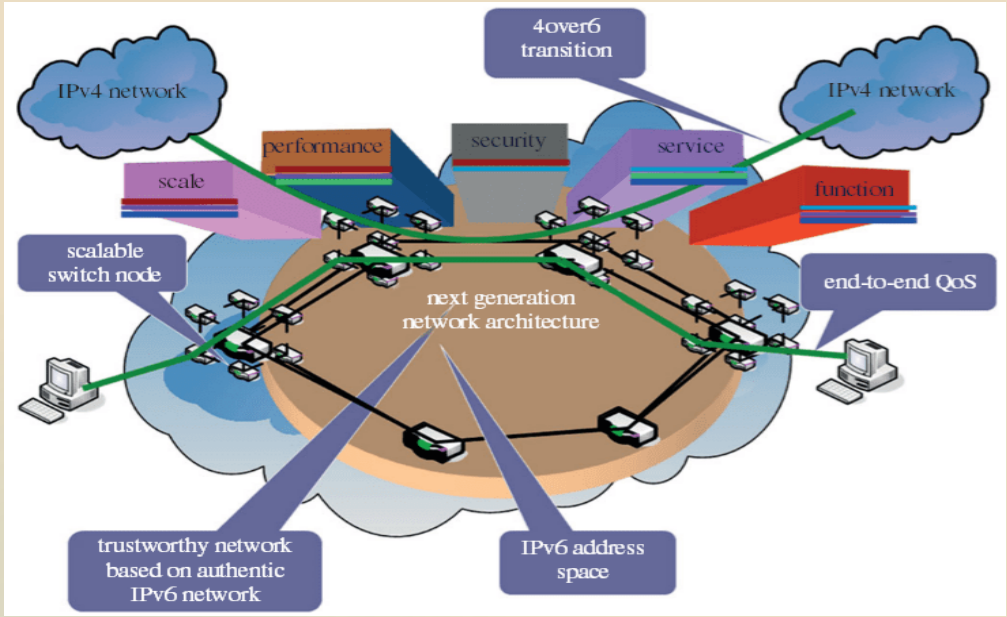
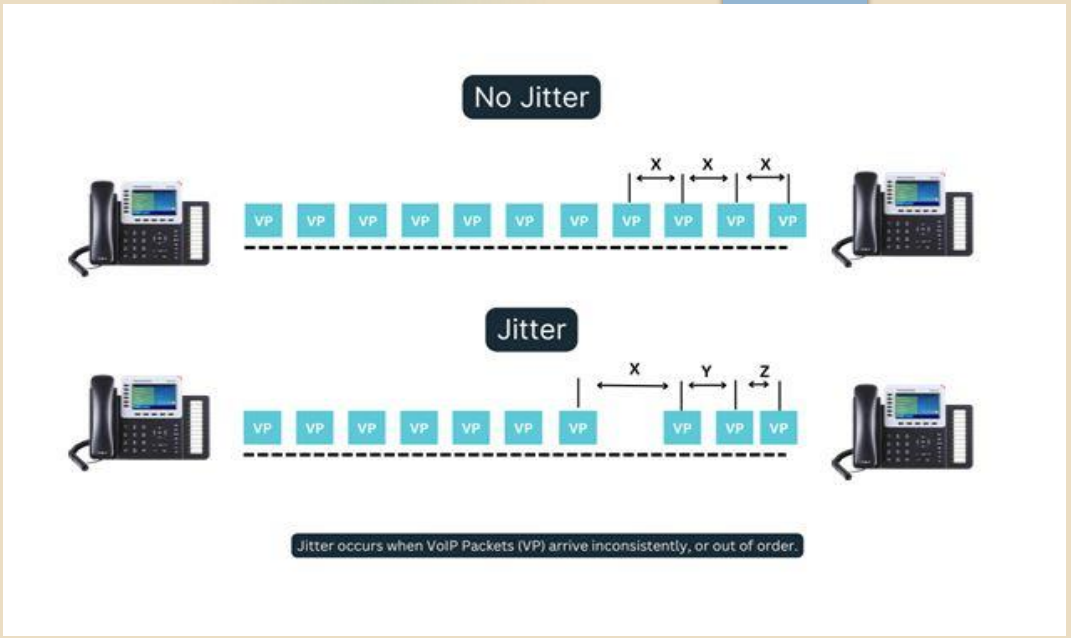


Схема мережі NGN

Забезпечення якості обслуговування та безпеки в мережах NGN

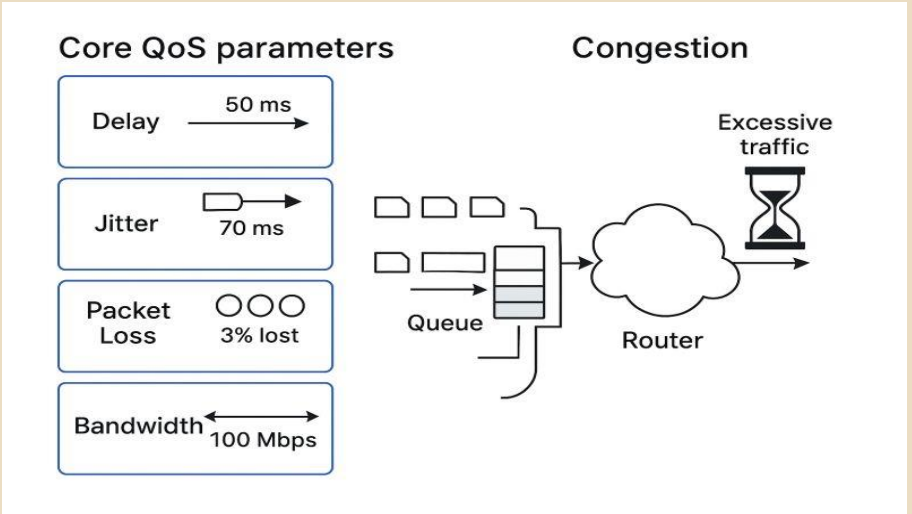
Інтеграція “performance/QoS” , “security” і “service” як взаємопов’язані складові в архітектурі мережі наступного покоління





Візуальне пояснення нерівномірного приходу VoIP-пакетів

- Мережі NGN повинні забезпечувати гарантовану якість обслуговування та інформаційну безпеку в умовах конвергенції сервісів і пакетної передачі даних. Різнорідні сервіси працюють у спільній IP-інфраструктурі, що вимагає диференційованого керування трафіком, політик QoS і контролю ресурсів. IP-архітектура підвищує кіберризики, тому QoS і безпека розглядаються як взаємопов’язані елементи. Їх інтеграція на всіх рівнях NGN забезпечує стабільну роботу сервісів, виконання SLA та стійкість мережі до атак.



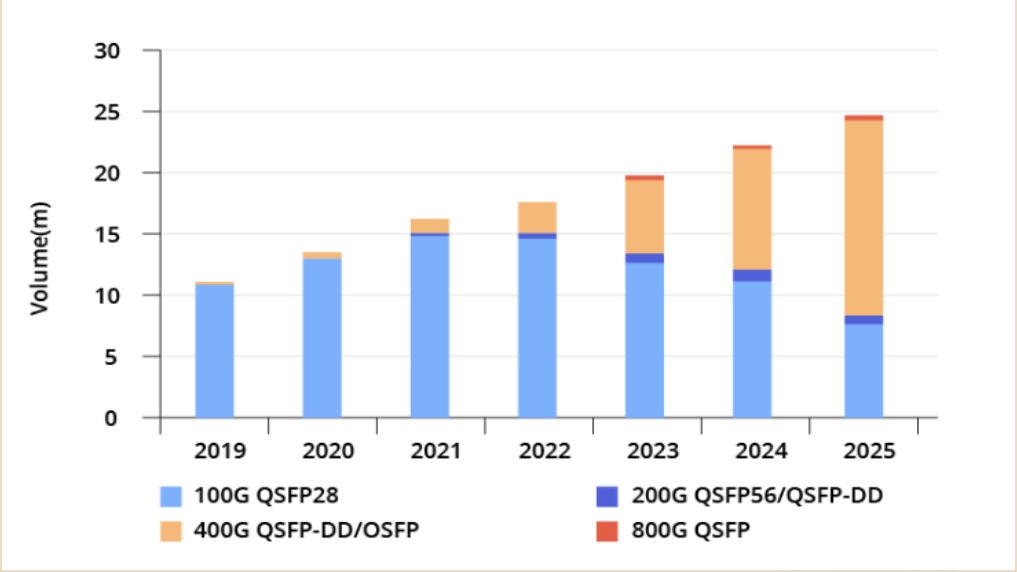
Параметри QoS

Технологія 400GE в ЦОД

- Оголошення у 2020 році про початок ери інтерфейсів 400GE спочатку було сприйняте ринком стримано, оскільки наявна інфраструктура кінця 2010-х років (10–25 Гбіт/с, класичні DCN-архітектури, PCIe 3.0, SATA/SAS) ще відповідала більшості прикладних задач. Проте стрімкий розвиток цифрових сервісів, віртуалізації, розподілених обчислень і хмарних платформ зумовив різке зростання вимог до продуктивності, надійності та масштабованості мереж.
- У межах сучасних архітектурних підходів (TOGAF, IT4IT) саме прикладний рівень формує вимоги до мережевої інфраструктури. Це призвело до переходу від фрагментованих рішень до уніфікованих, програмно-керованих мереж, близьких до концепції NGN, де високошвидкісні інтерфейси стають ключовим чинником цифрової трансформації.



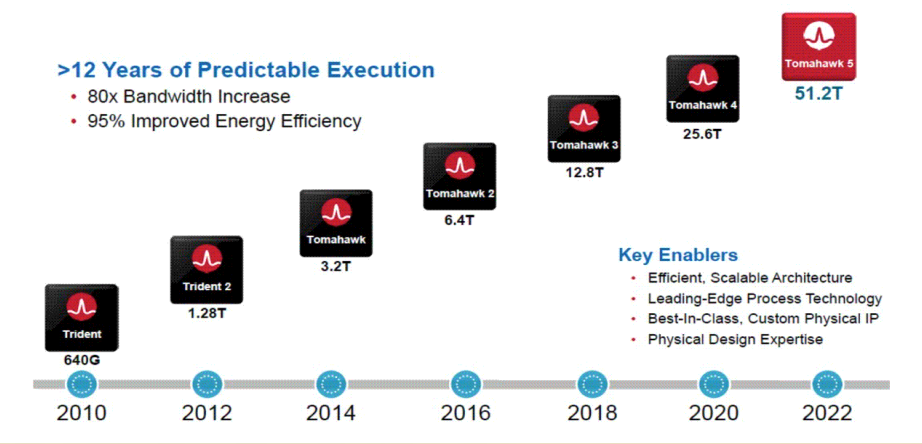
Структура референсної архітектури IT4IT від The Open Group



Зміна швидкості мереж за п'ять років та прогноз на найближче майбутнє (на осі Y показаний обсяг відвантажень мережевих пристроїв різних стандартів у мільйонах штук)

Характеристики 400GE

- Технологія 400GE забезпечує значне підвищення пропускної здатності мереж, продуктивності сервісів і ефективності використання інфраструктури за рахунок консолідації з'єднань і зменшення кількості обладнання. Вона знижує затримки, енергоспоживання та спрощує масштабування мереж. 400GE широко застосовується в центрах обробки даних, хмарних і телекомунікаційних мережах, системах штучного інтелекту та високопродуктивних обчисленнях. Еволюція стандартів Ethernet до 400 Гбіт/с відображає зростаючі вимоги сучасних цифрових сервісів і є важливою складовою модернізації мереж NGN.

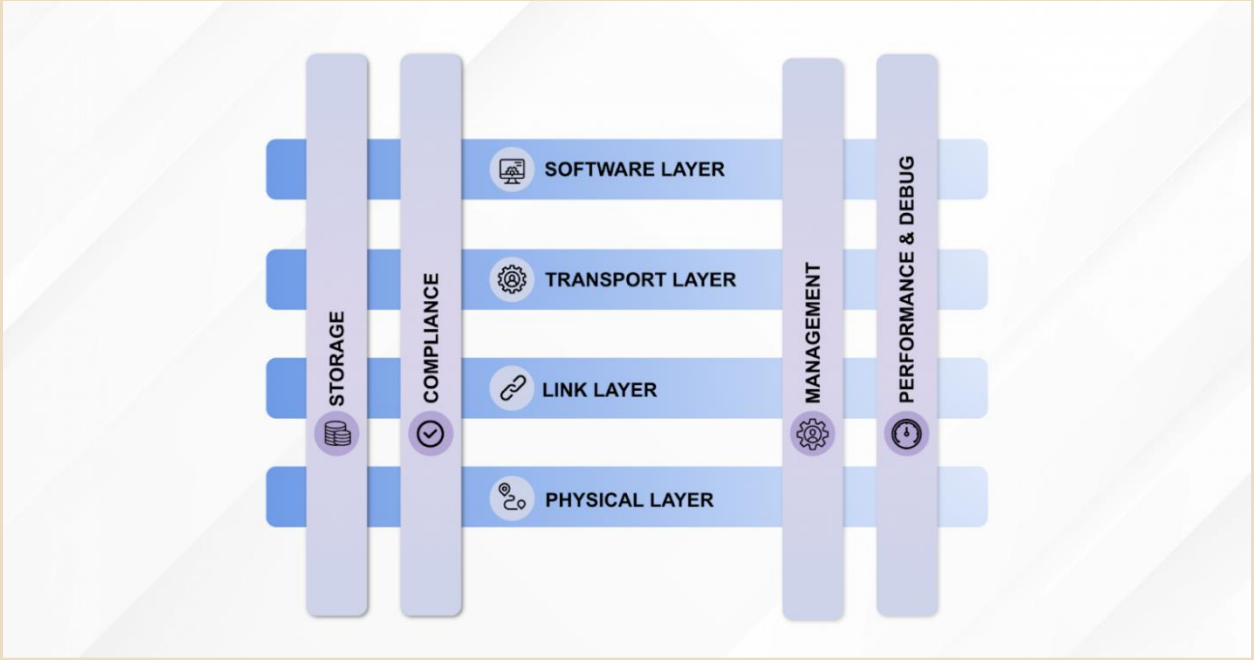


Зростання швидкості передачі даних у міру вдосконалення чіпів на прикладі одного з вендорів Merchant Silicon

Тип трансивера	Швидкість	Тип кабелю	Дальність передавання	Кількість ліній	Метод модуляції	Сфера застосування
CFP8	400 Гбіт/с	SMF, MMF	SMF: до 100 км; MMF: до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Високошвидкісні з'єднання у великих дата-центрах, хмарні інфраструктури
QSFP-DD	400 Гбіт/с	SMF, MMF	SMF: до 100 км; MMF: до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Сервери, комутатори та маршрутизатори в центрах обробки даних
OSFP	400 Гбіт/с	SMF, MMF	SMF: до 100 км; MMF: до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Високощільні підключення в центрах обробки даних
400G SR8	400 Гбіт/с	MMF	до 100 м	8 (8×50G)	PAM4 (4-рівнева амплітудна модуляція)	Короткі з'єднання в межах одного дата-центра
400G DR4	400 Гбіт/с	SMF	до 500 м (MMF) / до 2 км (SMF)	4 (4×100G)	DP-QPSK (квадратурна фазова маніпуляція з подвійною поляризацією)	Міжсегментні та міждатацентрові з'єднання
400G FR4	400 Гбіт/с	SMF	до 2 км	4 (4×100G)	DP-QPSK (квадратурна фазова маніпуляція з подвійною поляризацією)	Довгі з'єднання між дата-центрами та міжмережеві канали

Ethernet 400GE як компонент для апгрейду в мережах NGN

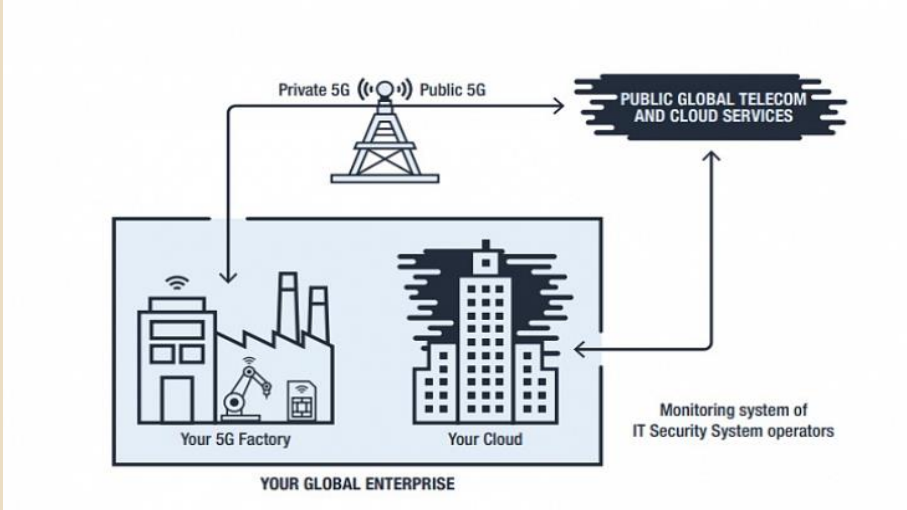
- Технологія 400GE забезпечує суттєве зростання пропускної здатності центрів обробки даних і є ключовим елементом модернізації транспортного рівня мереж NGN. Вона підтримує конвергентні сервіси, хмарні платформи та навантаження штучного інтелекту, зменшуючи затримки й кількість фізичних з’єднань. Використання сучасних схем модуляції підвищує продуктивність, водночас актуалізуючи питання енергоефективності. У перспективі NGN потребуватимуть ще швидших інтерфейсів і масштабованої мережевої інфраструктури для підтримки зростаючих обсягів трафіку.



Концептуальна модель багатошарової мережевої інфраструктури

Виявлення слабих місць

- Експерти Trend Micro у дослідженні *Securing 5G Through Cyber-Telecom Identity Federation* проаналізували уразливості мереж 5G та запропонували підходи до підвищення їх кібербезпеки. Об’єктом дослідження стала непублічна мережа 5G NPN, що використовує SIM-карти для автентифікації та взаємодіє з зовнішніми NGN-каналами. Показано, що поєднання закритих 5G-мереж з відкритою інфраструктурою NGN збільшує поверхню атак і потребує посиленого керування ідентифікацією та захисту трафіку.
- Виявлено ключові загрози, зокрема SIMjacking, мережеві атаки типу *salami* і *low-and-slow*, а також компрометацію цифрових ідентичностей. Зроблено висновок, що ефективна модернізація NGN і 5G можлива лише за умови наскрізного підходу до безпеки, який інтегрує апаратні, мережеві та програмні механізми захисту.

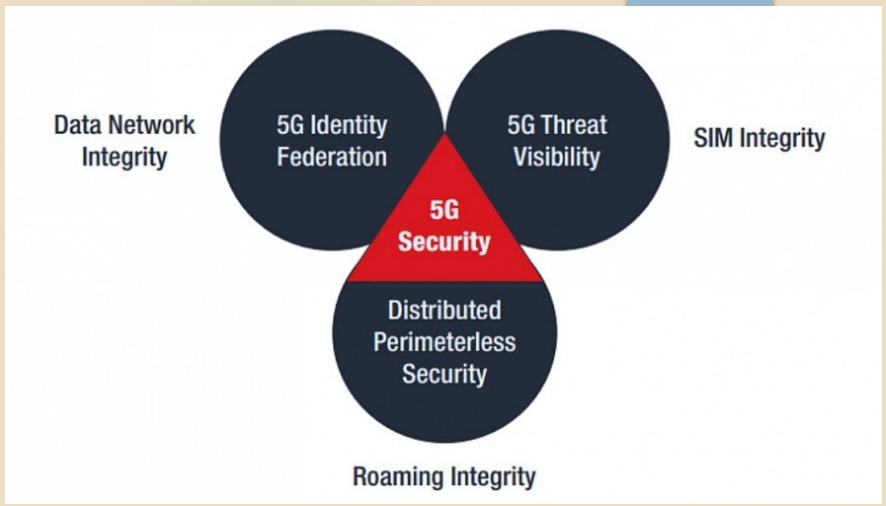


Досліджувана NPN-мережа

Узагальнювальна таблиця типів атак

Тип атаки	**Рівень реалізації**	**Основна ціль**	**Потенційні наслідки для NGN/5G**
SIMjacking	Апаратний (SIM)	Кінцевий пристрій, мережеве підключення	Перехоплення трафіку, підміна мережі, запуск шкідливого ПЗ
Salami / Low-and-slow	Мережевий	Інфраструктура NGN	Формування «сліпих зон», деградація QoS, масштабні атаки
Компрометація ідентичності	Телеком + IT	Посвідчення користувача	Несанкціонований доступ до IT-систем і сервісів
Атаки на ML/AI	Дані та транспорт	Алгоритми ШІ	Спотворення результатів навчання, зниження ефективності

Оптимальні рішення при модернізації мереж



Візуалізація підходу до забезпечення безпеки мереж

Фахівцями Trend Micro запропоновано наскрізний підхід до безпеки NGN, що об'єднує захист мереж, SIM-карт і кінцевих пристроїв в єдину систему. Така модель забезпечує постійний моніторинг, раннє виявлення загроз і захист механізмів ідентифікації, що є особливо важливим для 5G, IoT та приватних мереж. Підкреслено, що складність архітектури NGN і 5G підвищує кіберризики, особливо в Україні, тому успішне впровадження нових технологій можливе лише за умови поєднання мережевої модернізації з комплексною кібербезпекою та підготовкою фахівців.

Виклики та перспективи розвитку 5G і NGN в Україні

Аспект	Поточний стан / виклик	Перспективний напрям розвитку
Досвід експлуатації	Обмежений досвід роботи з телеком-мережами у бізнесу	Підготовка фахівців, співпраця з операторами
Кібербезпека	Фрагментарний захист, розрив між IT і телеком	Наскрізна модель безпеки NGN + 5G
Архітектура мереж	Перехідний стан від legacy до NGN	SDN/NFV, хмарні ядра, приватні 5G
Транспортна інфраструктура	Обмежені резерви пропускної здатності	Впровадження 100GE/400GE
Сфери застосування	Переважно мобільний доступ	Промисловість, NPN, держсервіси
Регуляторне середовище	Формується	Адаптація європейських стандартів

ВИСНОВКИ

- У кваліфікаційній роботі досліджено впровадження технології NGN (Next Generation Networks) у процесі модернізації телекомунікаційних систем і мереж.
- Показано, що перехід до NGN є об’єктивною необхідністю, зумовленою зростанням вимог до пропускної здатності, гнучкості, масштабованості та інформаційної безпеки, а також конвергенцією сервісів і технологій.
- Проаналізовано еволюцію телекомунікаційних мереж від 1G до 5G, що дозволило визначити ключові тенденції розвитку архітектур, механізмів керування та захисту інформації.
- Особливу увагу приділено архітектурним принципам NGN, механізмам забезпечення якості обслуговування (QoS), їх взаємозв’язку з угодами рівня обслуговування (SLA) та питанням інформаційної безпеки в мережах NGN і 5G.
- Розглянуто роль високошвидкісних транспортних технологій Ethernet у модернізації мереж. Проаналізовано перспективи розвитку NGN в Україні.
- Отримані результати підтверджують ефективність NGN як основи для подальшого розвитку сучасної телекомунікаційної інфраструктури.

Дякую за увагу!