ВСТУП

Стрімкий розвиток мобільних технологій та зростаюча залежність сучасного суспільства від бездротових засобів зв’язку зумовлюють потребу у забезпеченні їхньої високої надійності, сталості та захищеності. Мобільний зв’язок сьогодні виконує роль критичної інфраструктури, яка забезпечує функціонування банківських систем, державних сервісів, транспортних мереж, оборонних структур та повсякденних комунікацій між громадянами. Разом з тим, зростання обсягів передаваних даних і кількості підключених пристроїв супроводжується одночасним ускладненням спектра кіберзагроз, спрямованих на перехоплення, модифікацію, блокування або фальсифікацію інформаційних потоків.

Класичні засоби криптографічного захисту, що широко застосовуються в мережах мобільного зв’язку, в перспективі можуть виявитися вразливими до атаки з використанням квантових комп’ютерів. Квантові обчислення здатні суттєво прискорити процес розв’язання задач, на яких базується стійкість сучасних алгоритмів шифрування, таких як RSA та ECC. Це ставить під загрозу конфіденційність та цілісність інформаційних потоків у майбутніх поколіннях мобільних мереж, зокрема 5G та 6G.

У цьому контексті особливої актуальності набуває дослідження підходів до оптимізації та підвищення безпеки мобільного зв’язку, які враховують не лише існуючі кіберзагрози, як-от атакування сигнальних протоколів, несанкціоноване підключення до мережі, використання IMSI-перехоплювачів та DDoS-атаки, але й перспективні ризики, пов’язані з розвитком квантових обчислювальних технологій. Перехід до постквантових криптографічних алгоритмів, впровадження квантового розподілу ключів, побудова мережевих архітектур із принципом "нульової довіри", застосування штучного інтелекту для моніторингу аномальної мережевої активності — усе це формує основу майбутніх стандартів

інформаційної безпеки.

Таким чином, дослідження механізмів захисту та оптимізації мобільного зв’язку в умовах сучасних і перспективних кіберзагроз є важливим науково-практичним завданням, спрямованим на забезпечення національної та технологічної безпеки. Результати роботи можуть бути використані під час модернізації телекомунікаційних систем, розробки стандартів інформаційної безпеки та впровадження нових інфраструктурних рішень у сфері бездротових комунікацій.

Актуальність даної роботи зумовлена зростанням ролі мобільного зв’язку як критичної інформаційної інфраструктури та одночасним ускладненням спектра кіберзагроз, що спрямовані на порушення цілісності, конфіденційності та доступності переданих даних. Сучасні мобільні мережі, включно з технологіями 4G/5G, широко використовуються у фінансовому секторі, державному управлінні, транспортних системах, службах безпеки та у повсякденній комунікації, що робить їх потенційною мішенню для високотехнологічних атак.

Крім того, швидкий розвиток квантових обчислювальних технологій створює ризик суттєвого зниження ефективності традиційних криптографічних методів, які на даний момент забезпечують захист даних у мобільних мережах. Імовірність появи квантових комп’ютерів, здатних зламувати сучасні алгоритми шифрування, вимагає завчасної адаптації телекомунікаційних систем до нової парадигми захисту інформації. У зв’язку з цим постає необхідність аналізу існуючих вразливостей мобільного зв’язку та розробки підходів до його оптимізації із використанням постквантових криптографічних алгоритмів, захищених протоколів сигналізації та інтелектуальних механізмів моніторингу.

Таким чином, дослідження безпеки та оптимізації мобільного зв’язку в умовах кіберзагроз і розвитку квантових технологій є важливим для забезпечення надійності телекомунікаційної інфраструктури, стабільності державних та комерційних сервісів, а також для побудови перспективних моделей захищених

мереж наступних поколінь.

Мета даної роботи є аналіз сучасних та перспективних кіберзагроз, що впливають на безпеку мобільного зв’язку, а також обґрунтування рекомендацій щодо оптимізації та підвищення стійкості мобільних мереж із урахуванням розвитку квантових технологій.

Об’єкт дослідження - є системи та інфраструктура мобільного зв’язку в контексті їхньої інформаційної безпеки.

Предметом дослідження є методи, моделі та технології забезпечення безпеки і оптимізації мобільного зв’язку в умовах кіберзагроз та впливу квантових технологій.

1. Мобільний зв’язок, та кібер загрози

1.1 Визначення мобільного зв’язку

Мобільний зв’язок — це сукупність технологій, методів і технічних засобів, що забезпечують передавання інформації (голосу, даних, мультимедійного контенту) між абонентами за допомогою радіохвиль у бездротовому середовищі. На відміну від фіксованих мереж, мобільний зв’язок дозволяє користувачу переміщуватися у просторі, зберігаючи доступ до комунікаційних послуг.



Основою мобільних мереж є стільниковий принцип, згідно з яким територія поділяється на зони покриття — комірки (cell), кожна з яких обслуговується власною базовою станцією. Це дозволяє багаторазово використовувати той самий частотний ресурс, забезпечувати широку зону покриття та ефективно масштабувати мережу.

Мобільний зв’язок функціонує на трьох ключових рівнях:

- Радіодоступ — передавання сигналу між мобільним пристроєм і базовою

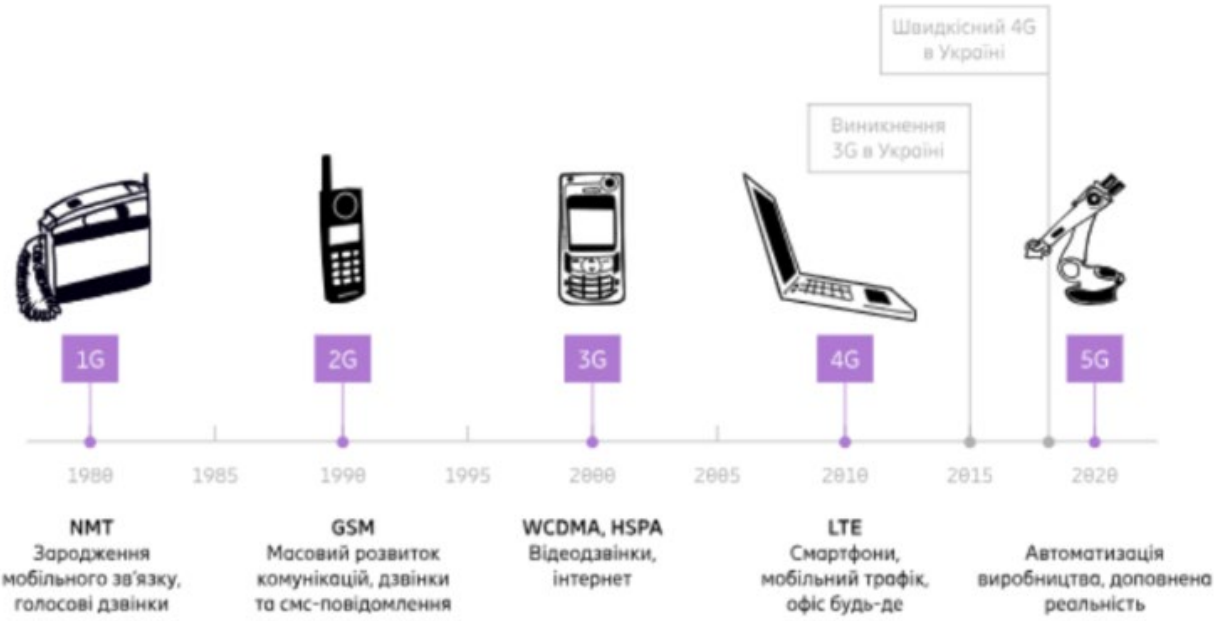
станцією.

- Транспортна мережа — маршрутизація трафіку всередині оператора.
- Ядро мережі — керування з’єднаннями, безпекою, автентифікацією, доступом до послуг.

З розвитком технологій мобільний зв'язок пройшов кілька поколінь — від 1G до 5G, кожне з яких забезпечило суттєвий стрибок у швидкості, надійності та функціональності.

1.2 Покоління мобільного зв'язку, та їх недоліки

Покоління мобільного зв’язку, які позначаються літерою G (від англійського Generation), являють собою послідовні стандарти розвитку бездротових телекомунікаційних систем. Кожне нове покоління не є просто збільшенням швидкості передавання даних, а відображає глибокі технологічні зміни в архітектурі мережі, методах модуляції, способах доступу до радіоресурсу, рівні цифровізації та спектрі підтримуваних сервісів. Перехід від одного



покоління до іншого зазвичай зумовлений зростанням потреб користувачів, розвитком обчислювальних технологій і появою нових сценаріїв застосування мобільного зв’язку.

Перше покоління мобільного зв’язку, відоме як 1G, базувалося на аналогових технологіях і було призначене виключно для передавання голосу. Такі системи, як AMPS або TACS, не підтримували шифрування, мали низьку якість звуку, обмежену ємність мережі та були вразливими до перехоплення розмов. Проте саме 1G заклав основу стільникової архітектури, де територія поділяється на зони обслуговування з базовими станціями, що дозволило забезпечити мобільність абонентів.

Друге покоління, 2G, стало переломним етапом завдяки переходу від аналогового до цифрового зв’язку. Найвідомішим стандартом цього покоління є GSM. Оцифрування сигналу дало змогу значно підвищити якість голосу, ефективніше використовувати радіочастотний спектр і вперше впровадити базові механізми шифрування та аутентифікації абонентів. Окрім голосового зв’язку, 2G забезпечило підтримку простих сервісів передачі даних, таких як SMS та низькошвидкісний пакетний доступ (GPRS, EDGE), що стало початком мобільного інтернету.

Третє покоління, 3G, зосередилося на розвитку мобільної передачі даних. Технології на кшталт UMTS/WCDMA та CDMA2000 забезпечили значно вищі швидкості в порівнянні з 2G, що зробило можливим доступ до вебсайтів, використання електронної пошти, відеодзвінків і мультимедійних сервісів. 3G вперше інтегрувало голос і дані в єдину мережеву архітектуру, заклавши основу для масового використання смартфонів та мобільних додатків.

Четверте покоління, 4G, представлене насамперед технологією LTE, ознаменувало повний перехід до пакетної передачі даних на основі IP. У мережах 4G голосовий зв’язок реалізується через технології типу VoLTE, а мобільний інтернет досягає швидкостей, співставних із дротовими широкосмуговими мережами. LTE використовує передові методи модуляції, OFDMA, багатоантенні системи MIMO та оптимізовану архітектуру ядра мережі, що забезпечує високу пропускну здатність, менші затримки та кращу якість обслуговування. Саме 4G зробило можливими потокове відео високої якості, хмарні сервіси, онлайн-ігри та масове використання мобільного інтернету.

П’яте покоління, 5G, виходить далеко за межі традиційного уявлення про мобільний зв’язок як сервіс для смартфонів. Воно орієнтоване на підтримку надвисоких швидкостей передачі даних, наднизьких затримок і одночасного підключення величезної кількості пристроїв. 5G відкриває шлях до нових застосувань, таких як автономний транспорт, промислова автоматизація, віддалена медицина, доповнена і віртуальна реальність, масовий Інтернет речей. Архітектура 5G є гнучкою та програмно керованою, використовує network slicing,

edge-обчислення та інтеграцію з хмарними сервісами, що дозволяє адаптувати мережу під різні сценарії використання.

Таким чином, еволюція поколінь мобільного зв'язку від 1G до 5G відображає поступовий перехід від простого аналогового голосового зв'язку до складних, інтелектуальних і високошвидкісних цифрових мереж. Кожне нове покоління не лише підвищує швидкість і пропускну здатність, а й змінює роль мобільного зв'язку в суспільстві, перетворюючи його на базову інфраструктуру для цифрової економіки та майбутніх технологій.

1G, або перше покоління мобільного зв'язку, є початковим етапом розвитку стільникових телекомунікаційних систем і охоплює аналогові мобільні мережі, що почали впроваджуватися на початку 1980-х років. Саме в цей період уперше було реалізовано ідею стільникової архітектури, коли велика територія поділяється на окремі зони обслуговування — стільники, кожен з яких обслуговується власною базовою станцією. Такий підхід дозволив багаторазово використовувати одні й ті самі радіочастоти в різних географічних зонах і став фундаментом для всіх наступних поколінь мобільного зв'язку.

Технологічно мережі 1G базувалися виключно на аналоговій передачі голосу. Голосовий сигнал передавався у вигляді безперервної електричної хвилі без цифрового кодування, що робило зв'язок чутливим до шумів, перешкод і спотворень. Будь-яка втрата якості радіосигналу одразу відображалася на чутності розмови. Передача даних у сучасному розумінні була відсутня — мережі 1G не підтримували ні текстові повідомлення, ні доступ до Інтернету. Фактично єдиним сервісом був голосовий зв'язок, а обмін службовою інформацією між телефоном і мережею здійснювався з дуже низькою швидкістю, еквівалентною приблизно 2,4 кбіт/с.

Перші стандарти 1G, такі як AMPS у США, TACS у Європі та NMT у скандинавських країнах, стали основою для комерційних мобільних мереж. Вони забезпечували базову мобільність абонентів, зокрема можливість здійснювати дзвінки під час руху на високій швидкості — до приблизно 250 км/год, що було важливо для використання зв'язку в автомобілях, поїздах або інших транспортних засобах. Саме в 1G були реалізовані базові механізми handover, тобто автоматичного перемикання абонента між базовими станціями під час руху, що стало ключовою характеристикою стільникового зв'язку.

Разом із тим мережі першого покоління мали суттєві обмеження. Через відсутність цифрового кодування вони не мали ефективних механізмів захисту інформації, що робило голосові розмови легко вразливими до перехоплення за

допомогою простих радіоприймачів. Ємність мережі була низькою, оскільки кожному дзвінку виділявся окремий частотний канал на весь час розмови, що швидко призводило до перевантаження мереж у густонаселених районах. Крім того, якість зв'язку значно погіршувалася з віддаленням від базової станції або за наявності перешкод.

Попри ці недоліки, 1G відіграло надзвичайно важливу історичну роль. Воно стало першим практичним кроком до створення глобальних мобільних мереж і сформувало базові принципи, які збереглися у всіх наступних поколіннях: стільникову структуру, мобільність абонента, автоматичне керування з'єднаннями та централізоване управління мережею. Саме обмеження й недоліки 1G стимулювали розвиток цифрових технологій і призвели до появи 2G, яке усунуло більшість проблем аналогового зв'язку та відкрило шлях до сучасних мобільних комунікацій.

1G — Перше покоління мобільного зв'язку. 1G — це аналогові стільникові системи, що з'явилися на початку 1980-х років. Перші комерційні впровадження стали основою для створення глобальних мобільних мереж. Швидкість передачі даних: лише голос, фактично 2,4 кбіт/с для службових сигналів. Максимальна швидкість руху абонента: до 250 км/год

Основні технології:

- AMPS (Advanced Mobile Phone System) — США
- NMT (Nordic Mobile Telephone) — Скандинавія
- **TACS** (Total Access Communications System) — Європа

TACS — це один із перших (1G) аналогових стандартів стільникового зв'язку, адаптація американської системи AMPS для Європи й деяких інших регіонів. Він був запроваджений у 1980-х роках (особливо в Великій Британії) і забезпечував мобільний голосовий зв'язок у діапазоні ~900 МГц.

Ключові особливості:

- Аналогова передача голосу (FM-модуляція)
- Відсутність шифрування - легко перехоплювався сигнал
- Низька ємність мереж
- Погана якість зв'язку (перешкоди, шум)
- Відсутність підтримки SMS чи будь-яких даних

- Обмежена швидкість handover та радіопокриття

Недоліки, що призвели до появи 2G:

- Відсутність цифрової безпеки
- Низька спектральна ефективність
- Відсутність сервісів передачі даних
- Великі й енергозатратні телефони

2G, або друге покоління мобільного зв’язку, стало важливим етапом еволюції стільникових систем, оскільки саме воно здійснило перехід від аналогового зв’язку першого покоління до повністю цифрової передачі інформації. Цей перехід докорінно змінив якість, надійність і функціональність мобільного зв’язку, зробивши його масовим, стандартизованим і більш захищеним. На відміну від 1G, де передавався лише аналоговий голосовий сигнал, 2G дозволило кодувати голос у цифрову форму, що забезпечило кращу якість дзвінків, зменшення рівня шумів і перешкод, а також ефективніше використання радіочастотного спектра.

Технологічною основою 2G стали стандарти на кшталт GSM, IS-95 (cdmaOne) та D-AMPS. Найпоширенішим із них став GSM, який запровадив чітку архітектуру мережі, міжнародний роумінг і уніфіковані принципи роботи мобільних систем у різних країнах. Цифрова обробка сигналу дала змогу розділяти радіоканал між багатьма абонентами, що значно підвищило ємність мережі та дозволило операторам обслуговувати набагато більше користувачів у порівнянні з аналоговими мережами.

Однією з ключових інновацій 2G стала поява сервісу коротких текстових повідомлень — SMS. Ця функція спочатку розглядалася як допоміжна, проте з часом стала надзвичайно популярною і перетворилася на важливий канал комунікації. SMS дозволили користувачам обмінюватися текстовою інформацією без встановлення голосового з’єднання, що зменшувало навантаження на мережу та розширювало можливості мобільного зв’язку. Саме в 2G сформувалася концепція мобільного телефону як багатофункціонального засобу спілкування, а не лише пристрою для дзвінків.

Ще одним суттєвим досягненням другого покоління стало покращення безпеки зв’язку. У 2G були впроваджені механізми аутентифікації абонентів за допомогою SIM-карт, а також базові алгоритми шифрування голосового трафіку.

Це зробило несанкціоноване прослуховування значно складнішим у порівнянні з 1G і підвищило рівень довіри користувачів до мобільного зв’язку. Хоча з сучасної точки зору ці механізми мають обмежену криптостійкість, на момент впровадження вони були серйозним кроком уперед.

Важливим аспектом розвитку 2G стало також зародження мобільної передачі даних. Хоча початкові швидкості були дуже низькими, з’явилася можливість передавати прості цифрові дані, що стало фундаментом для подальшого розвитку мобільного інтернету. З удосконаленням 2G у вигляді технологій GPRS і EDGE мережі другого покоління почали підтримувати пакетну передачу даних, що дозволило користувачам переглядати прості вебсторінки, користуватися електронною поштою та іншими базовими онлайн-сервісами. Саме ці розширення стали перехідним етапом між традиційним голосовим зв’язком і повноцінним мобільним інтернетом.

У загальному контексті розвитку телекомунікацій 2G відіграло ключову роль у формуванні сучасного мобільного зв’язку. Воно не лише замінило застарілий аналоговий підхід, а й створило технологічну та концептуальну основу для наступних поколінь. Цифрова передача, масовість, стандартизація, базова безпека та перші кроки до мобільного інтернету зробили 2G фундаментом, на якому згодом були побудовані 3G, 4G і 5G мережі.

2G (друге покоління) – це цифрова технологія мобільного зв'язку, яка замінила аналоговий зв'язок 1G і дозволила передавати не тільки голос, але й дані. Вона забезпечила можливість надсилати короткі текстові повідомлення (SMS), покращила якість та безпеку дзвінків, а також поклала початок мобільному інтернету

Основні технології**:**

- **GSM** (Global System for Mobile Communications) — наймасовіший
- **cdmaOne (IS-95)**
- **D-AMPS**

GSM — це цифрова система мобільного зв’язку другого покоління (2G), створена в Європі й запущена на початку 1990-х. Вона стала глобальним стандартом, яким користувалися більшість країн світу. GSM був розроблений для того, щоб замінити несумісні аналогові 1G системи (AMPS, NMT, TACS) і забезпечити безпечний, масштабований та уніфікований мобільний зв’язок.

Однією з ключових особливостей GSM став перехід до цифрової модуляції та цифрової обробки сигналів, що дозволило ввести шифрування, високу якість

голосу, захист від клонування та можливість масштабного міжнародного роумінгу.

Технологічно GSM використовує TDMA у поєднанні з FDMA. Територія поділена на частотні канали шириною 200 kHz, і кожен канал поділений на 8 часових слотів, що дозволяє обслуговувати до восьми абонентів на одному частотному каналі. Усе це робить систему набагато ефективнішою, ніж аналогові стандарти.

Ще однією революцією стала поява SMS, а згодом — GPRS та EDGE, які дали можливість мобільного доступу до інтернету (хоч і повільного) і перетворили GSM у платформу 2.5G.

GSM зберіг свою актуальність понад 20 років і став базою для переходу до 3G та 4G. Більшість країн досі підтримують його для голосу та простих IoT-пристроїв.

CdmaOne, або **IS-95**, — це цифровий стандарт 2G, створений компанією Qualcomm. Його головна особливість — використання CDMA (Code Division Multiple Access), тобто розподіл доступу за кодами, а не за часом або частотою.

На відміну від GSM, де кожному абоненту виділяється свій часовий слот, у CDMA всі користувачі передають одночасно в одному й тому самому частотному каналі шириною 1,25 MHz, але з різними унікальними псевдовипадковими кодами. Завдяки цьому сигнали абонентів не змішуються, а приймач «відокремлює» потрібний сигнал за кодом. CDMA дає значно вищу спектральну ефективність — у тому ж діапазоні можна обслуговувати більше абонентів. Якість голосу в cdmaOne часто була вищою, ніж у GSM, особливо в щільних мережах, бо CDMA менш чутлива до завад. Крім того, у CDMA застосовується розширення спектра, що робить сигнал стійким до перехоплення та завад — фактично шифрування було інтегроване в сам принцип роботи.

Ще одна унікальна властивість cdmaOne — м’який хендовер (soft handoff). Під час переходу між сотами телефон може одночасно підтримувати зв’язок з кількома базовими станціями. Це дає плавніший зв’язок і менший ризик обривів. Однак cdmaOne не став домінуючим стандартом через низку причин. Він був патентно залежний від Qualcomm, мав слабший міжнародний роумінг і був популярним переважно в США, Кореї, Японії та частині Латинської Америки.Проте саме CDMA технологічно лягла в основу 3G (CDMA2000, WCDMA).

D-AMPS, або IS-136, — це цифровий стандарт, створений як логічний наступник аналогового AMPS. Він мав забезпечити плавний перехід від 1G до 2G у Північній Америці без необхідності повної заміни інфраструктури. Головна ідея D-AMPS полягала в тому, щоб використати ті самі 30-кілогерцові канали, що й AMPS, але додати в них цифрову технологію TDMA. Таким чином у межах одного 30-kHz каналу з'явилося три часових слоти, що дало змогу збільшити ємність у три рази без зміни частотного плану.

Перевага D-AMPS полягала у зворотній сумісності: оператори могли одночасно підтримувати як старі аналогові телефони AMPS, так і нові цифрові. Це робило перехід технічно простим і дешевим.

Ключові нововведення:

- Цифровий голос (краща якість, менше шумів)
- SMS — вперше з'явилися короткі текстові повідомлення
- Безпечніші дзвінки (шифрування A5/1, A5/2)
- Можливість GPRS/EDGE → перший мобільний інтернет

Швидкості передачі даних:

- GSM (CSD): 9,6 кбіт/с
- GPRS (2.5G): до ~40–50 кбіт/с
- EDGE (2.75G): до ~200 кбіт/с

Переваги:

- Значно вища спектральна ефективність
- Краща безпека
- Масове покриття та міжнародний роумінг
- Підтримка простих інтернет-сервісів (WAP)

Обмеження:

- Дуже низька швидкість інтернету
- Перевантаження мережі при великій кількості абонентів

3G, або третє покоління мобільного зв'язку, є етапом розвитку стільникових мереж, який ознаменував перехід від обмеженого доступу до даних

у мережах 2G до повноцінного мобільного інтернету та мультимедійних сервісів. Основною метою впровадження 3G було забезпечення стабільної передачі даних зі значно вищими швидкостями, ніж у попередніх поколіннях, а також інтеграція голосового зв'язку й пакетних даних в єдину мережеву інфраструктуру. Саме 3G створило технічні умови для масового використання смартфонів і мобільних додатків.

На технологічному рівні 3G базується на цифрових методах передачі сигналу та нових радіоінтерфейсах, таких як UMTS із технологією WCDMA або CDMA2000. У порівнянні з 2G, ці системи використовують ширші смуги частот, складніші методи модуляції та кращі алгоритми управління радіоресурсами, що дозволяє одночасно обслуговувати більше абонентів і підтримувати вищу швидкість передавання даних. Теоретичні швидкості 3G у базових реалізаціях досягають кількох мегабіт за секунду, а з появою удосконалених версій, таких як HSPA та HSPA+, швидкість мобільного інтернету зросла до десятків мегабіт за секунду.

З точки зору послуг 3G значно розширило функціональність мобільного зв'язку. Окрім традиційних голосових викликів і текстових повідомлень, користувачі отримали можливість здійснювати відеодзвінки в реальному часі, переглядати вебсторінки, користуватися електронною поштою, соціальними мережами та потоковим відео. Це покоління вперше забезпечило достатню якість і швидкість з'єднання для мультимедійного контенту, що стало основою для розвитку мобільних сервісів і контент-платформ.

Архітектура мереж 3G також зазнала суттєвих змін у порівнянні з 2G. Вона передбачає більш тісну інтеграцію радіодоступу з ядром мережі, підтримку пакетної комутації та механізмів управління якістю обслуговування. Завдяки цьому мережа може ефективніше розподіляти ресурси між голосовими та інформаційними сервісами, забезпечуючи прийнятну якість навіть за високого навантаження. Крім того, у 3G були покращені механізми безпеки, включно з аутентифікацією абонентів і шифруванням трафіку, що підвищило захист даних у порівнянні з 2G.

У загальному контексті розвитку мобільного зв'язку 3G стало ключовим перехідним етапом між класичними стільниковими мережами, орієнтованими переважно на голос, і сучасними широкосмуговими мобільними системами. Воно заклало технологічну основу для подальшого розвитку 4G і 5G, сформувало звичку користувачів до постійного мобільного доступу до Інтернету та суттєво вплинуло на цифровізацію суспільства, бізнесу й повсякденного життя.

Основні стандарти:

- **UMTS** (WCDMA) — Європа
- CDMA2000 1xEV-DO — США, Азія

UMTS (Universal Mobile Telecommunications System) — стандарт 3-го покоління (3G), визначений 3GPP.
WCDMA (Wideband CDMA) — радіоінтерфейс UMTS; у розмовній мові їх часто називають разом: UMTS/WCDMA. UMTS дав істотний приріст швидкостей даних і сервісів порівняно з 2G (GSM/CDMAOne) і ввів архітектуру з розділенням радіо- і комутаційної частин (UTRAN + Core Network).

UMTS стандартизовано в релізі 99 (Release 99) і широко розгорталося з початку 2000-х; пізніше він еволюціонував до HSPA (HSDPA/HSUPA) і потім до LTE.

Нововведення:

- Високошвидкісний доступ до інтернету
- Відеодзвінки
- Мобільне телебачення та потокове відео
- Підтримка програм і сервісів, що потребують швидких даних

Швидкості:

- UMTS — до 384 кбіт/с
- HSPA (3.5G) — до 14 Мбіт/с
- HSPA+ (3.75G) — до 42 Мбіт/с

Переваги:

- Різке зростання швидкості інтернету
- Підтримка VoIP
- Можливість одночасної передачі голосу й даних

Недоліки:

- Висока вартість обладнання
- Відносно велика затримка ~100–200 мс
- Не оптимізовано для IoT

4G, або четверте покоління мобільного зв’язку, є етапом розвитку стільникових мереж, який забезпечив якісно новий рівень мобільного доступу до інтернету та мультимедійних сервісів. Основною ідеєю 4G стало створення повністю пакетної мережі, орієнтованої на передачу даних, у якій інтернет-трафік є базовою складовою, а голосовий зв’язок розглядається як один із сервісів, що працює поверх IP-інфраструктури. Саме тому 4G стало фундаментом для сучасних цифрових сервісів і мобільних додатків, які потребують високої пропускної здатності та стабільного з’єднання.

Технологічною основою 4G є стандарт LTE (Long-Term Evolution), який був розроблений як еволюційний розвиток мереж 3G із радикально спрощеною та оптимізованою архітектурою. На відміну від попередніх поколінь, у LTE використовується повністю пакетна передача даних на базі IP, що дозволяє ефективніше керувати трафіком і зменшувати затримки. У мережах 4G відсутня класична комутація каналів для голосу, а телефонні дзвінки здійснюються через технології типу VoLTE, де голос передається у вигляді цифрових пакетів разом з іншими даними.

Однією з ключових переваг 4G є значно вища швидкість передачі даних у порівнянні з 3G. Завдяки використанню сучасних методів модуляції, широких смуг частот, а також технологій OFDMA та багатоантенних систем MIMO, мережі 4G здатні забезпечувати швидкості в десятки й сотні мегабіт за секунду. Це зробило можливим комфортний перегляд відео високої якості, включно з HD і Full HD, стабільні відеодзвінки, онлайн-ігри, хмарні сервіси та швидке завантаження великих обсягів даних на мобільних пристроях.

Важливою характеристикою 4G є зменшення затримки передачі даних. У порівнянні з 3G, затримка в мережах LTE значно нижча, що позитивно впливає на якість інтерактивних сервісів, таких як відеозв’язок у реальному часі, потокові сервіси та мобільні ігри. Це також стало передумовою для розвитку нових застосувань, які потребують швидкої реакції мережі, зокрема хмарних обчислень і віддаленого доступу до сервісів.

З архітектурної точки зору 4G характеризується спрощеним ядром мережі та більш тісною інтеграцією радіодоступу з транспортною інфраструктурою. Такий підхід дозволяє операторам гнучко масштабувати мережу, підвищувати її надійність і впроваджувати нові сервіси без суттєвих змін базової структури. Крім того, у 4G були покращені механізми безпеки, зокрема аутентифікація користувачів і шифрування трафіку, що підвищило рівень захисту персональних даних у мобільних мережах.

У загальному контексті розвитку мобільного зв’язку 4G стало поколінням, яке зробило мобільний інтернет повсякденним і масовим. Воно перетворило смартфон на універсальний пристрій для спілкування, розваг, роботи та доступу

до цифрових сервісів. Саме на базі 4G сформувалися сучасні екосистеми мобільних додатків, потокового контенту та хмарних платформ, а також було закладено технологічний фундамент для подальшого розвитку мереж п’ятого покоління.

4G (четверте покоління) – це стандарт мобільного зв'язку, що забезпечує високошвидкісний доступ до інтернету на мобільних пристроях. Він пропонує швидкість передачі даних, яка набагато перевищує 3G, дозволяючи комфортно переглядати відео високої якості, робити відеодзвінки та грати в онлайн-ігри. Часто використовується разом із терміном LTE (Long-Term Evolution), який є технологією, що реалізує стандарт 4G.

Основні цілі 4G:

- Забезпечити інтернет на рівні провідних мереж
- Підтримати масові відеосервіси
- Створити платформу для мобільних додатків

Технології:

- LTE (Long Term Evolution)
- LTE-Advanced
- OFDMA (для downlink)
- MIMO (багатоантенні системи)

LTE — це архітектура та набір радіо/мережевих стандартів 3GPP для еволюції мобільного зв’язку до високошвидкісного пакетного 4G-рівня; перша релізація з’явилася в 3GPP Release-8 (формально «E-UTRAN / EPC»). 3g4g.co.uk+1. Головні цілі й ідея. Замість складної змішаної CS/PS архітектури UMTS, LTE зроблено як чисто пакетну (all-IP) систему з простою архітектурою радіо-доступу (eNodeB — без окремого RNC) та ядром EPC (Evolved Packet Core). Це дає менші затримки, вищі швидкості і кращу масштабованість. 3g4g.co.uk. Радіо-технологія. Downlink застосовує OFDMA (Orthogonal Frequency Division Multiple Access); uplink — SC-FDMA (щоб знизити PAPR у UE). Каналова ширина LTE типово: 1.4 / 3 / 5 / 10 / 15 / 20 MHz. Фізична модуляція — QPSK, 16QAM, 64QAM залежно від CQI та умов каналу.

LTE-Advanced — еволюція LTE (помітно релізи 10+), мета — досягти вимог IMT-Advanced (іноді називають «істинним 4G»): пікові швидкості ближче до 1 Gbps в downlink та 500 Mbps в uplink у певних сценаріях. 3gpp.org+1

Ключові технології LTE-Advanced:

- Carrier Aggregation (CA): агрегація кількох компонент-каналів (component carriers) щоб досягти сумарної смуги до 100 MHz (наприклад 5×20 MHz). Це дозволяє підвищити пікову швидкість і використовувати розрізнені спектральні блоки. ETSI+1
- Advanced MIMO: більше антен (4×4, 8×8 у базі) і передові стратегії (spatial multiplexing + beamforming). remcom.com
- Coordinated Multipoint (CoMP): координація передачі/прийому між базовими станціями для підвищення швидкості на краях сот і зменшення інтерференції. ETSI
- Relay nodes, heterogeneous networks (HetNet): малі соти (pico/femto), ретранслятори і т.д. — щоб покращити покриття і ємність

OFDMA — мультидоступна версія OFDM: загальну смугу ділять на багато вузькополосних субносіїв (subcarriers); кожному користувачу/пакету динамічно призначаються підмножини субносіїв у частоті та часі. Це основна multiple-access технологія LTE для downlink.

MIMO — сукупність методів, що використовують кілька антен на передавачі та/або на приймачі, щоби підвищити пропускну здатність, надійність або обидва одночасно. У LTE/MIMO використовують три основні режими: diversity (винахідність), spatial multiplexing (множення потоків) і beamforming.

Як це реалізовано в LTE:

- LTE підтримує конфігурації типу 2×2, 4×2, 4×4 і навіть більше (на боці eNodeB — 8×8 в LTE-A/пізніших релізах).
- Коли канал дозволяє, вач-комбінація MIMO + OFDMA дає суттєвий приріст пікових та середніх швидкостей. При цьому потрібні складні алгоритми

Максимальні швидкості:

- LTE: до 150 Мбіт/с
- LTE-A: до 1 Гбіт/с
- Затримка: 30–50 мс

Переваги:

- Високі швидкості через широку смугу частот
- Підтримка HD-відео
- Якісний мобільний інтернет
- Краща енергоефективність
- Базова підтримка IoT (NB-IoT, LTE-M)

Недоліки:

- Обмежені можливості для масових пристроїв
- Мережа не оптимізована для мікросекундних затримок
- Потрібна щільніша інфраструктура

5G, або п’яте покоління мобільного зв’язку, є новим етапом розвитку стільникових мереж, який суттєво розширює можливості мобільного зв’язку порівняно з 4G. Його ключова ідея полягає не лише у збільшенні швидкості передачі даних, а й у створенні універсальної мережевої платформи, здатної одночасно підтримувати дуже різні за вимогами сервіси — від надшвидкого мобільного інтернету до масового підключення мільйонів пристроїв і критично важливих застосувань із мінімальною затримкою.

Однією з головних характеристик 5G є значно вища швидкість передавання даних. Теоретично вона може досягати рівня від кількох гігабіт за секунду до 10 Гбіт/с, що у багато разів перевищує можливості 4G. Такі швидкості стають можливими завдяки використанню ширших смуг частот, зокрема в міліметровому діапазоні, сучасних методів модуляції, технологій massive MIMO та спрямованого формування променя (beamforming). Для користувача це означає практично миттєве завантаження великих файлів, потокове відео в надвисокій якості, стабільну роботу хмарних сервісів і новий рівень мультимедійного контенту.

Не менш важливою перевагою 5G є суттєве зменшення затримки сигналу. Якщо в 4G затримка вимірюється десятками мілісекунд, то в 5G вона може знижуватися до одиниць мілісекунд. Це відкриває можливості для застосувань, які раніше були недоступними для мобільних мереж, зокрема дистанційного керування технікою, автономних транспортних засобів, телемедицини, промислової автоматизації та інтерактивних сервісів віртуальної й доповненої реальності. Низька затримка робить мобільну мережу придатною для критичних сценаріїв, де швидка реакція системи має вирішальне значення.

Архітектурно 5G суттєво відрізняється від попередніх поколінь. Вона побудована на принципах віртуалізації та програмно-керованих мереж, що дозволяє гнучко налаштовувати інфраструктуру під конкретні завдання. Однією з ключових інновацій є network slicing — можливість логічно розділяти одну фізичну мережу на кілька незалежних «зрізів», кожен з яких оптимізується під певний тип сервісу. Наприклад, один зріз може бути призначений для надшвидкісного мобільного інтернету, інший — для масового IoT, а третій — для критичних застосувань із мінімальною затримкою та підвищеними вимогами до надійності.

Особливе місце в концепції 5G займає масовий Інтернет речей. Мережа п’ятого покоління здатна одночасно підтримувати підключення величезної кількості пристроїв на одиницю площі — сенсорів, лічильників, розумних пристроїв, промислового обладнання. При цьому такі пристрої можуть споживати мінімум енергії та працювати роками без заміни батарей. Це створює основу для розвитку «розумних міст», цифрової інфраструктури, енергетичних систем, аграрного сектору та промислового IoT.

5G також тісно інтегрується з хмарними обчисленнями та edge-технологіями. Обробка даних може виконуватися ближче до користувача, на крайових вузлах мережі, що додатково зменшує затримку та підвищує ефективність роботи сервісів. Такий підхід є критично важливим для застосувань на кшталт автономного транспорту, систем відеоаналітики та сервісів доповненої реальності, де швидкість реакції мережі має вирішальне значення.

У стратегічному плані 5G розглядається як фундамент для майбутнього цифрового суспільства. Воно не лише покращує користувацький досвід мобільного інтернету, а й створює технологічну основу для нових галузей економіки, автоматизації виробництва та розвитку інноваційних сервісів. В Україні, відповідно до планів цифрового розвитку, передбачається поетапне впровадження 5G, зокрема пілотні запуски, що мають відбутися у найближчі роки. Це має стати важливим кроком до інтеграції країни в глобальний технологічний простір і підготовки інфраструктури до вимог майбутніх поколінь мобільного зв’язку.

Таким чином, 5G є не просто швидшим продовженням 4G, а принципово новою платформою, орієнтованою на надшвидкісні з’єднання, мінімальні затримки, масовий IoT та підтримку складних інноваційних застосувань, які визначатимуть розвиток цифрових технологій у найближчі десятиліття.

5G (п'яте покоління) — це новий стандарт мобільного зв'язку, який пропонує значно вищу швидкість передачі даних (до 1-10 Гбіт/с), меншу

затримку сигналу, більшу пропускну здатність та можливість підключення великої кількості пристроїв одночасно. Ця технологія є наступним етапом еволюції після 4G і розробляється для підтримки майбутніх технологій, таких як "інтернет речей" (IoT), автономні транспортні засоби та розширена/віртуальна реальність. В Україні планується пілотний запуск 5G, зокрема в 2025 році, повідомляє Мінцифри. масовий IoT

Технології 5G:

- mmWave (міліметрові хвилі)
- Massive MIMO
- Beamforming
- Network slicing
- Cloud RAN / virtual RAN

mmWave — це діапазони радіочастот приблизно від 24 GHz до ~100 GHz (іноді початок позначають від 20–24 GHz). Ці частоти мають дуже велику доступну смугу (широкі блоки спектра), тому їх використовують для надвисокошвидкісних з’єднань 5G (висока пропускна здатність на одиницю спектра).

Технічні властивості:

- Дуже коротка довжина хвилі → великі втрати на відстані (path loss) і сильне загасання внаслідок перешкод і навіть атмосфери/дощу.
- Погано проходять через стіни і предмети, тому покриття сильно залежить від прямої видимості (LOS) або від відбиттів.
- Дозволяють розміщувати багато малих елементів антен у компактних масивах (надають апаратні умови для beamforming і високо-швидкісного MIMO).

Massive MIMO — розширення ідей MIMO до дуже великої кількості антен на шаці базової станції (наприклад десятки — сотні елементів). Це ключовий інструмент для підвищення ємності та продуктивності 5G у щільних середовищах.

Як працює: велика антена-матриця дозволяє одночасно формувати багато незалежних потоків (spatial multiplexing) і застосовувати тонке управління променями (beamforming/null-forming) для зниження інтерференції і підвищення

SINR. Масиви дають array gain (покращення відношення сигнал/шум) і великі просторові ресурси для обслуговування багатьох UE одночасно.

Beamforming — метод керування фазою й амплітудою сигналів на елементах антенної решітки, щоб скерувати енергію у певні напрямки (промені) і/або створити «нуль» у напрямі перешкод. Це може бути реалізовано як аналогове, цифрове або гібридне керування.

Типи реалізації:

- Аналогове beamforming — фазові шифтери/аналогові суматори; ефективне за апаратними витратами, але менш гнучке.
- Цифрове beamforming — кожна антена має окремий RF-ланцюг → повна гнучкість, складніший і енергоємніший.
- Гібридне — поєднує обидва підходи і часто використовується в mmWave (щоби не мати по RF-ланцюгу на кожен елемент, але зберегти гнучкість).

Network slicing — логічна віртуалізація фізичної мережі на кілька незалежних «слайсів», кожен із яких має власні характеристики (пропускна здатність, затримка, надійність, функції мережі). Ідея — дати кожному сервісу чи клієнту віртуальний канал, налаштований під його SLA (наприклад: IoT-слайс з великою щільністю і низькою пропускною, URLLC-слайс з наднизькою затримкою, MBB-слайс для мобільного інтернету).

Як працює: оператор використовує віртуалізацію (NFV, SDN) та елементи управління (orchestration, slice manager), щоб створювати, масштабувати та видаляти слайси. Кожен слайс може складатися з компоненції RAN, ядра (Core) і сервісних функцій, виділених або логічно гарантованих для цієї задачі.

Cloud RAN / virtual RAN (C-RAN / vRAN): обидва підходи належать до концепції віртуалізації функцій радіомережі.

Cloud RAN (C-RAN): централізація (консолідація) базової обробки (BBU) у загальному пулі (Data Center або розподіленому PoP), а на точках присутні тільки радіо-блоки (RRU). Це дає економію, кращий розподіл ресурсів і простіше впровадження координаційних технологій (CoMP).

virtual RAN (vRAN): віртуалізація RAN-функцій як software-network-functions (NFV/container) на загальному x86-обладнанні; часто йдеться про поділ на CU/DU (Central Unit / Distributed Unit), які можуть запускатися в хмарі/edge. vRAN — більш гнучка, постачальнико-незалежна реалізація C-RAN.

Технічні вимоги і виклики: суворі вимоги на затримку між RRH і DU/CU (фронт-холл / midhaul), потреба в високошвидкісних/низько-латентних транспортних каналах (фронт-haul), складність оптимізації віртуалізованих реальних-часових функцій (потрібні спеціальні драйвера й прискорювачі), операційна інтеграція і безпека в хмарі.

Три ключові сценарії 5G:

- eMBB — надширокосмуговий мобільний інтернет (до 10 Гбіт/с)
- URLLC — наднадійний надмалозатримковий зв'язок (1–5 мс)
- mMTC — масові IoT-комунікації (до 1 млн пристроїв/км²)

Характеристики:

- Швидкість: до 10 Гбіт/с (теоретично), 1 Гбіт/с у реальному середовищі
- Затримка: 1–10 мс
- Ефективність спектру: +300% у порівнянні з LTE

Переваги:

- Ультрашвидкісний інтернет
- Супернизька затримка → нові сценарії (дрони, автопілоти, промисловий контроль)
- Масштабований IoT на рівні міст
- Гнучкість мережі через slicing

Недоліки:

- Потреба у щільній мережі малих сот
- Висока енергетична вартість масивних станцій
- Підвищені ризики кіберзагроз через віртуалізацію

6G, або шосте покоління мобільного зв'язку, розглядається як наступний етап еволюції стільникових мереж, який має з'явитися орієнтовно у період 2030–2035 років. На відміну від попередніх поколінь, 6G поки що не має остаточно затверджених стандартів, однак його концепція активно формується міжнародними організаціями зі стандартизації, науково-дослідними центрами та провідними компаніями телекомунікаційної галузі. В обговоренні майбутнього 6G беруть участь такі структури, як 3GPP та ITU-R, а також глобальні технологічні лідери, серед яких Samsung, Nokia, Huawei, Ericsson, NTT DoCoMo

та інші. Їхні дослідження спрямовані не просто на покращення існуючих характеристик мобільного зв'язку, а на створення принципово нової цифрової інфраструктури.

Головна ідея 6G полягає в тому, що він не буде лише швидшою або більш ефективною версією 5G. Очікується, що 6G стане універсальною платформою для повністю цифрового світу, у якому взаємодіють не тільки люди та традиційні мобільні пристрої, а й штучний інтелект, автономні машини, робототехнічні системи, цифрові аватари та кіберфізичні об'єкти. Мережа майбутнього має поєднувати фізичний і віртуальний простір у єдину систему, де обчислення, зв'язок і інтелект будуть тісно інтегровані між собою.

З технічної точки зору 6G орієнтується на надзвичайно високі швидкості передачі даних, які потенційно можуть досягати сотень гігабіт або навіть терабіт за секунду. Це стане можливим завдяки використанню нових діапазонів частот, зокрема субтерагерцового та терагерцового спектра, а також подальшому розвитку технологій масивних антенних систем і надточного формування променя. Такі характеристики дозволять передавати величезні обсяги даних у реальному часі, що є необхідним для голографічного зв'язку, повністю занурювальної віртуальної та доповненої реальності, а також для цифрових двійників складних об'єктів і процесів.

Однією з ключових особливостей 6G стане ще більш радикальне зменшення затримки сигналу. Очікується, що затримка може бути знижена до рівня мікросекунд, що зробить мережу придатною для надкритичних застосувань. Це відкриває шлях до дистанційного керування роботами з тактильним зворотним зв'язком, синхронної взаємодії між автономними транспортними засобами, а також до нових форм людино-машинної взаємодії, де реакція системи має бути майже миттєвою.

Архітектура 6G мережі розглядається як повністю програмно визначена, інтелектуальна та самокерована система. Штучний інтелект відіграватиме центральну роль у керуванні мережею, оптимізації радіоресурсів, забезпеченні безпеки та адаптації до змінних умов. Мережа зможе самостійно навчатися, прогнозувати навантаження, виявляти аномалії та автоматично реагувати на загрози. Таким чином, 6G стане не лише середовищем передачі даних, а активним учасником цифрових процесів.

Важливою складовою концепції 6G є інтеграція з квантовими технологіями. У перспективі мережі шостого покоління можуть використовувати квантово-захищені канали зв'язку, системи квантового розподілу ключів і нові криптографічні підходи, стійкі до атак квантових комп'ютерів. Це пов'язано з необхідністю забезпечення довгострокової конфіденційності та захисту даних у

світі, де квантові обчислення можуть становити серйозну загрозу для традиційних методів шифрування.

6G також розширить можливості масового підключення пристроїв, перевершуючи навіть потенціал 5G у сфері Інтернету речей. Мова йде не лише про сенсори чи побутові пристрої, а й про масштабні кіберфізичні системи, розумні інфраструктури, екосистеми «розумних міст» і промислові комплекси, де мільярди об’єктів обмінюються даними в режимі реального часу. При цьому мережа має бути енергоефективною та екологічно стійкою, що є одним із важливих напрямів досліджень у рамках 6G.

У глобальному сенсі 6G розглядається як основа для формування нового цифрового суспільства, де межі між фізичним і цифровим світом поступово зникають. Він має стати технологічним фундаментом для економіки майбутнього, нових форм комунікації, освіти, медицини, промисловості та культури. Таким чином, 6G є не просто наступним поколінням мобільного зв’язку, а комплексною платформою, що поєднує зв’язок, обчислення, інтелект і безпеку в єдину глобальну цифрову екосистему.

Стандарт 6G (Sixth Generation Mobile Network) — це майбутня технологія мобільного зв’язку, яку очікується впровадити приблизно у 2030–2035 роках. Хоча 6G ще не стандартизований, його концепція активно формується міжнародними організаціями, дослідницькими інститутами та провідними телеком-гігантами (3GPP, ITU-R, Samsung, Nokia, Huawei, Ericsson, NTT DoCoMo тощо).

6G не просто продовжить розвиток 5G — він має стати інфраструктурою повністю цифрового світу, де з’єднані не лише люди та пристрої, а й штучний інтелект, робототехніка, цифрові аватари, квантові мережі та інтегрований фізичний і віртуальний простір.

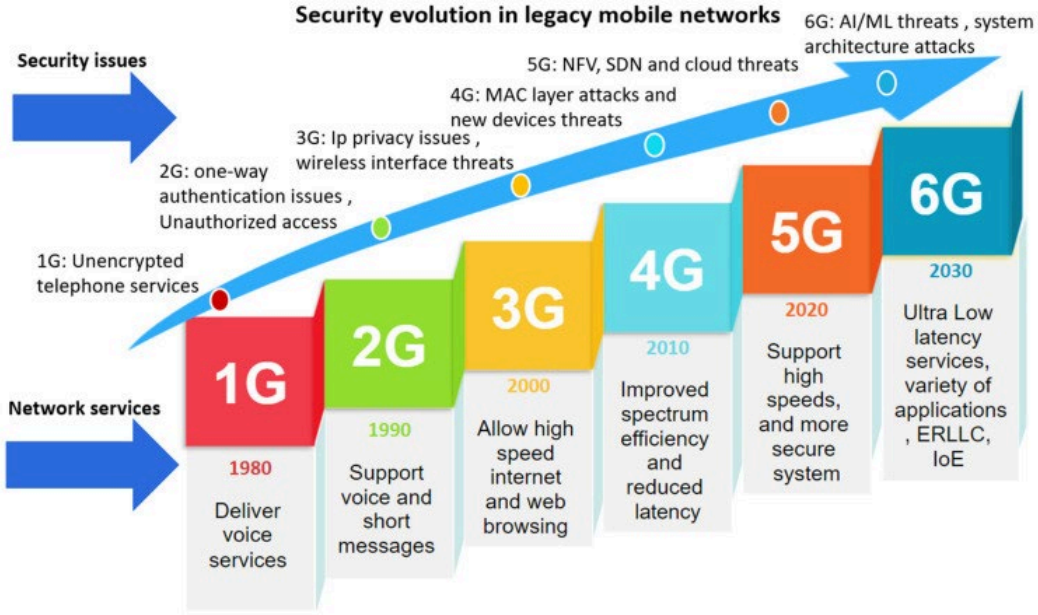
Архітектура 6G: глобальні зміни, 6G передбачає:

- Інтеграцію космічного та наземного зв’язку. Супутники LEO/MEO стануть частиною базової архітектури.
- Використання терагерцових частот. Це дає величезну швидкість, але потребує мікро-, піко- та фемто-стежин, масивного beamforming та високої щільності базових станцій

- Мережі на основі кубітів. Квантові комунікації почнуть вбудовуватись у інфраструктуру, такі як - квантовий розподіл ключів (QKD), квантово-стійкі протоколи, нові методи квантомережевого шифрування.

1.3 Кіберзагрози кожного з поколінь зв'язку

Розвиток мобільного зв'язку від 1G до 6G супроводжувався не лише зростанням швидкості, пропускної здатності та функціональних можливостей, а й поступовим ускладненням кіберзагроз. Кожне покоління мобільних мереж мало власні технічні обмеження й архітектурні особливості, які створювали нові вектори атак. Еволюція технологій одночасно відкривала нові можливості для користувачів і для зловмисників.



Нижче детально розкрито кіберризики від найперших аналогових систем до проєктованих 6G-мереж, що формуються у контексті квантових обчислень та масового застосування штучного інтелекту.

1.3.1 1G — аналоговий зв'язок: повна відсутність захисту

Покоління 1G (1980-ті роки) базувалося на аналоговій передачі сигналу, де дані передавалися у вигляді радіохвиль без жодного шифрування чи автентифікації. Це робило 1G найбільш незахищеною системою.

Основні загрози:

- Перехоплення голосових викликів — достатньо було сканера радіочастот.
- Підміна абонента (spoofing) — зловмисник міг клонувати мобільний телефон, використовуючи його ідентифікаційні параметри.
- Несанкціоновані дзвінки за рахунок іншого абонента — «клонування IMEI/ESN» стало масовою проблемою.
- Відсутність будь-якої захистної логіки — неможливість протидіяти перехопленню, глушінню чи фальсифікації сигналів.

1G фактично не передбачав інформаційної безпеки як явища — усе передане ефіром було доступним для прослуховування.

1.3.2 Кіберзагрози 2G — цифрових GSM/EDGE мереж

Перехід до цифрової передачі значно підвищив якість та безпеку зв’язку, але 2G мала свої суттєві проблеми. Основні загрози 2G:

- Слабке шифрування A5/1 та компрометований A5/2

A5/1 і A5/2 — це два різновиди потокових шифрів, створених для захисту радіоканалу в мережах GSM другого покоління. Обидва алгоритми працюють за принципом формування псевдовипадкового бітового потоку, який поєднується з даними XOR-операцією, утворюючи зашифрований сигнал. Вони побудовані на використанні лінійних регістрів зсуву зі зворотним зв’язком, але їхня внутрішня структура суттєво відрізняється, що і визначило їхню історію та рівень захищеності.

A5/1 був основним європейським варіантом і задумувався як відносно сильний шифр для свого часу. Він базується на трьох LFSR різної довжини, які працюють не повністю синхронно. Кожен регістр генерує послідовність бітів, а спеціальний механізм «міжчасової» синхронізації визначає, які регістри рухаються в кожен момент. Далі бітові значення з трьох регістрів комбінуються в один біт шифропотоку, який і використовується для шифрування голосу чи даних у реальному часі. Загалом A5/1 мав 64-бітний ключ і на момент розробки вважався достатньо стійким, оскільки його внутрішня конструкція була закритою, а типові атаки вимагали б значних обчислювальних витрат. Однак із часом стало зрозуміло, що криптографічні засади, закладені в 1980-х, уже не відповідають сучасним стандартам. З появою нових методів криптоаналізу,

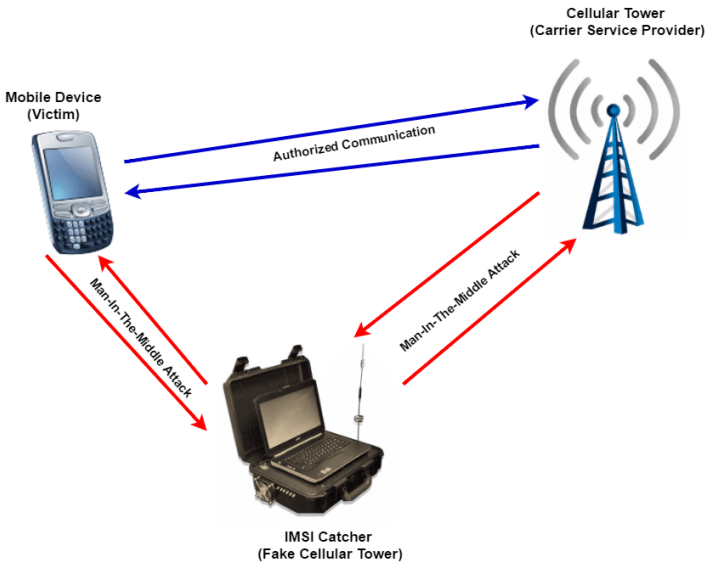
швидших процесорів і відкритих досліджень стало можливо відновлювати ключ за певних умов і з обмеженої кількості перехоплених даних. Це не робить алгоритм миттєво зламним у всіх сценаріях, але демонструє, що він суттєво застарів і більше не може вважатися сучасним захистом.

A5/2, навпаки, був створений не для підсилення безпеки, а для її навмисного послаблення. У 1990-х існували експортні обмеження на сильну криптографію, тому для певних країн був розроблений спеціально ослаблений варіант. Він так само ґрунтувався на LFSR, але його архітектура мала багато лінійних залежностей, передбачуваних зв'язків між регістрами і значно менш ентропійний внутрішній стан. Через це криптоаналітики досить швидко довели, що A5/2 є практично непридатним для безпеки. Його можна було зламати за секунди на звичайному комп'ютері, причому для цього достатньо було дуже невеликої кількості перехопленого трафіку. Після публікації вразливостей A5/2 офіційно визнали повністю компрометованим, і з початку 2000-х його перестали застосовувати, заборонивши в стандартах GSM.

Головною проблемою для обох алгоритмів є те, що сам GSM не передбачає взаємної автентифікації. Телефон автентифікує себе перед мережею, але не перевіряє автентичність базової станції. Це означає, що шахрайська станція може наказати телефону знизити рівень шифрування, використати A5/2 або навіть перейти на A5/0, тобто повністю відмовитися від шифрування. Саме тому загальна безпека GSM залежить не тільки від криптографії, а й від архітектури протоколу, яка сьогодні вважається застарілою, що й спричинило поступове вимкнення 2G у більшості країн і перехід на технології з повноцінною взаємною автентифікацією та сильнішими алгоритмами, як у 3G, 4G та 5G.

- Алгоритми шифрування GSM з часом були зламані, а їх ключі — зменшені. Атаки реального часу на GSM сьогодні можливі з недорогим радіообладнанням.

- Фальшиві базові станції (IMSI-catchers / Stingrays)

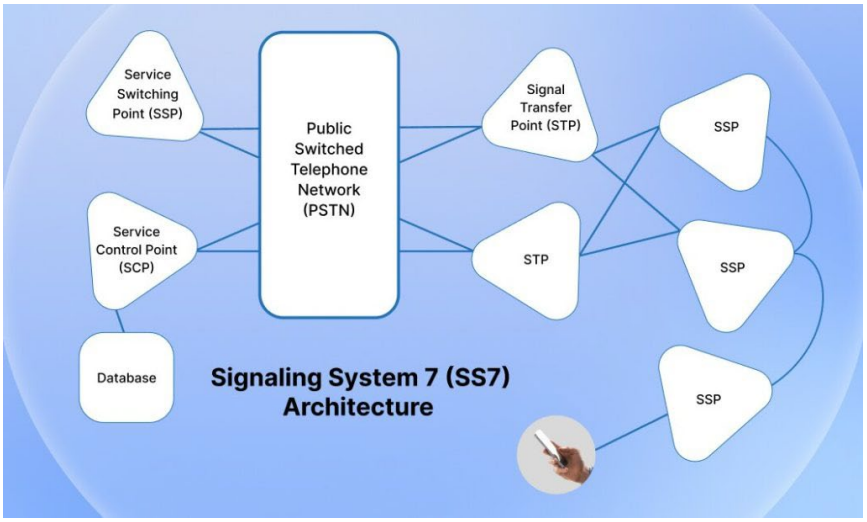


IMSI-catcher — це пристрій, який маскується під звичайну базову станцію мобільного оператора і змушує телефони поблизу під'єднатися саме до нього. Коли телефон бачить такий «фальшивий» передавач, він автоматично переходить на нього, бо 2G не вимагає автентифікації мережі, тобто смартфон не може перевірити, чи ця станція справжня. Після підключення пристрій отримує технічні ідентифікатори телефону — насамперед IMSI, який використовується для реєстрації абонента в мережі, а також може відстежувати, які пристрої знаходяться поруч, або примушувати їх переходити на слабке чи відкрите шифрування.

Такі системи не працюють як повноцінні операторські станції й зазвичай не можуть забезпечити реальний зв'язок, тому телефон або змішується між стільниковими мережами, або переключається між режимами шифрування. У більшості випадків призначення IMSI-catcher — не перехоплення контенту дзвінків, а ідентифікація пристроїв, спроба контролю трафіку сигналізації або зміна параметрів з'єднання. Сучасні мережі — особливо 4G і 5G — мають вбудовані механізми захисту, які роблять такі атаки значно складнішими, тоді як старі 2G залишаються вразливими через відсутність автентифікації базової станції та можливість нав'язати слабші алгоритми шифрування.

- Атаки на сигнальний протокол SS7

SS7 — це глобова система сигналізації, яка з’єднує між собою операторів мобільного зв’язку та дає змогу мережам обмінюватися службовою інформацією: маршрутизацією дзвінків, SMS, перевіркою балансу, аутентифікацією абонентів та даними про їхнє місцезнаходження. Проблема в тому, що SS7 проєктувався у 1970–1980-х роках, коли всі оператори вважалися «довіреними». У цій системі майже немає сучасних механізмів безпеки: якщо хтось отримує технічний доступ до мережі SS7 (через недобросовісного оператора, куплені шлюзи або вразливі вузли), він може надсилати запити так, ніби є легітимною мережею.



Через цю довіреність у SS7 можливі такі атаки: визначення місцезнаходження абонента через запити локації, перехоплення або перенаправлення SMS, включно з кодами 2FA, а також втручання у маршрутизацію дзвінків. Система дозволяє це, бо не перевіряє суворо, хто має право робити такі запити. Хоч сучасні оператори ставлять фільтри на периметрі, протоколи SS7 залишаються застарілими, і вразливості повністю усунути неможливо, доки мережі 2G/3G не будуть вимкнені або замінені на захищеніші 4G/5G-механізми сигналізації (Diameter, 5G SBA).

- Перехоплення SMS

Оскільки SMS — відкритий текст у низці сегментів з’єднання, їх можна зловити через IMSI-catcher або вразливості SS7.

1.3.3 Кіберзагрози 3G — мереж широкосмугового інтернету

3G вперше вирішила ключові проблеми GSM - вона ввела взаємну автентифікацію та посилила шифрування (KASUMI). Проте вона теж має свої уразливості:

- Уразливості протоколу KASUMI

KASUMI — це симетричний блочний алгоритм шифрування, створений спеціально для мобільних мереж 3G як основа для захисту даних і сигналізації. Він був адаптованою та спрощеною версією сильнішого алгоритму MISTY1, але під час адаптації деякі елементи були змінені для підвищення швидкодії на апаратному рівні. Саме ці спрощення пізніше стали причиною криптографічних слабкостей.

У мережах 3G KASUMI використовується для двох ключових функцій: шифрування трафіку між телефоном та базовою станцією й генерації кодів автентифікації, які забезпечують захист від підміни та несанкціонованих команд. На відміну від 2G-алгоритмів A5/1 та особливо слабкого A5/2, KASUMI значно сильніший і був спроєктований з урахуванням реальних атак: перехоплення в ефірі, примусової зміни алгоритмів і можливості атакувати систему в реальному часі.

Проблема полягає в тому, що хоча KASUMI вважався криптографічно надійним, згодом були відкриті теоретичні атаки, які знижують його стійкість у певних режимах. Ці атаки не надто практичні у реальних мережах і потребують значних обчислювальних ресурсів та доступу до великих обсягів даних, але вони показують, що алгоритм не є ідеальним. У практичних сценаріях зв’язок на KASUMI все одно набагато безпечніший, ніж 2G, бо алгоритм використовується в поєднанні з взаємною автентифікацією між телефоном і мережею, а не лише з одностороннім захистом, як у GSM.

- Вразливість до SS7-атак (спадщина 2G)

- Атаки через підроблені NodeB

NodeB — це базова станція мобільної мережі 3G (UMTS), тобто той елемент радіодоступу, який безпосередньо обслуговує мобільні телефони, приймає та передає радіосигнал, керує каналами та забезпечує доступ абонента до мережі оператора. У системі UMTS NodeB виконує роль, подібну до веж GSM чи eNodeB в LTE, але побудований навколо технології WCDMA, де багато пристроїв передають дані на тій самій частоті, розрізняючись за кодами.

NodeB приймає радіосигнали від телефонів, перетворює їх у транспортні дані та передає далі до контролера RNC, який координує роботу багатьох таких базових станцій. Саме NodeB відповідає за модуляцію сигналу, керування

потужністю, корекцію помилок у радіоканалі й підтримку стабільного зв’язку, навіть коли абонент рухається між секторами чи зонами покриття. Завдяки WCDMA NodeB може одночасно підтримувати більше користувачів, ніж старі GSM-вежі, і забезпечувати вищі швидкості передачі даних.

- Обрізання безпечного каналу

Телефон може бути змушений перейти в 2G → уразливе середовище. Це називається Downgrade attack.

Downgrade attack у контексті мобільних мереж — це навмисне примушення телефону перейти з більш захищеного стандарту зв’язку (наприклад, 4G/5G або 3G) на старіший і слабко захищений режим, такий як 2G або навіть конкретний слабкий алгоритм шифрування. Сенс атаки в тому, що старі технології мають або слабкі алгоритми (A5/1), або взагалі зламані (A5/2), або не мають взаємної автентифікації між телефоном і мережею, як у GSM. Через це зловмисник може змусити телефон працювати у режимі, де перехоплення чи підміна сигналу стають можливими.

Механіка атаки в загальному випадку виглядає так: телефон завжди прагне під'єднатися до найкращої доступної технології, але також повинен підтримувати старі покоління для зворотної сумісності. Зловмисник використовує фальшиву базову станцію або вразливості сигналізаційних систем, щоб створити умови, коли сучасний стандарт виглядає недоступним або забороненим. Наприклад, IMSI-catcher може «заглушити» LTE/3G або оголосити, що ці режими недоступні, і тоді телефон автоматично переходить на GSM. У GSM пристрій не перевіряє автентичність базової станції, і нападник може нав’язати слабке шифрування чи повну його відсутність. Тоді трафік легко перехоплюється в ефірі, а операторський контроль стає мінімальним.

Подібна ситуація можлива і у контексті слабких алгоритмів: навіть коли телефон і мережа підтримують A5/1 або кращі системи шифрування, фальшива станція може повідомити, що доступний лише A5/2 або навіть «null cipher» (без шифрування). У UMTS та LTE цей сценарій значно складніший через взаємну автентифікацію та сильніші алгоритми (KASUMI, AES, ZUC), але якщо телефон спочатку змусити вийти з 3G або LTE, захист зникає.

Уся логіка downgrade attack побудована на фундаментальній проблемі мобільних мереж: старі й слабкі стандарти довго залишаються активними поруч із новими, а телефони за замовчуванням сумісні з усіма поколіннями. Звідси і можливість атак — примус перебудуватися на вразливу технологію, де захист низького рівня, а підробка базових станцій чи перехоплення зв’язку стають цілком реальними.

1.3.4 Кіберзагрози 4G / LTE — мереж високошвидкісного інтернету

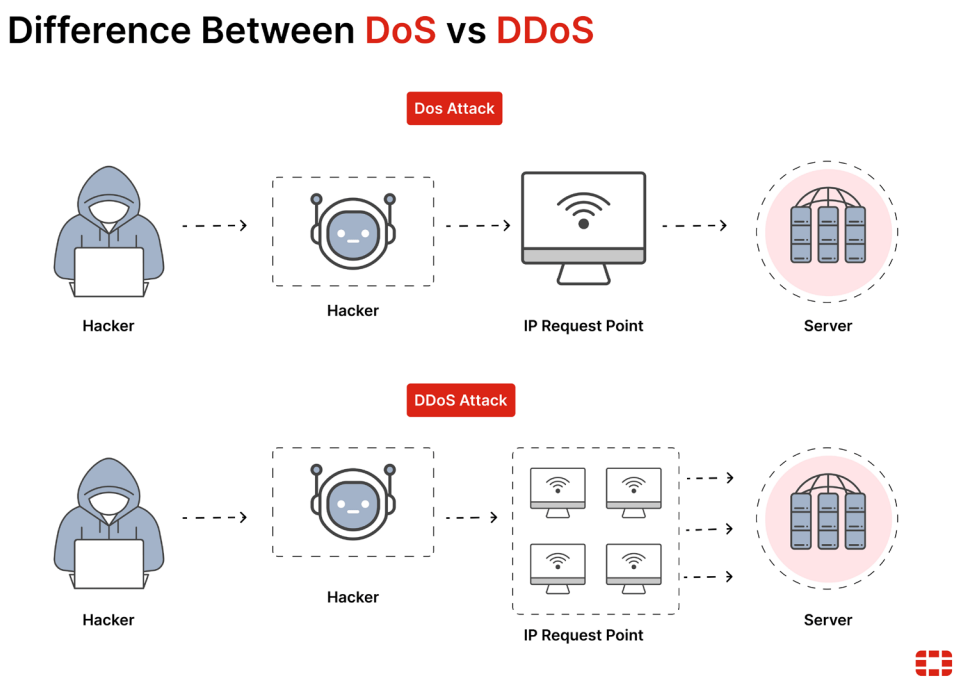
4G — перше покоління, повністю орієнтоване на IP-трафік. Воно суттєво покращує безпеку, але через складну архітектуру має нові загрози:

- Вразливості сигнального протоколу Diameter

Diameter — це сучасний протокол сигналізації, який прийшов на зміну застарілому SS7 у 4G та частково в 5G. Його головна задача — аутентифікація абонентів, управління доступом, білінг, роумінг і обмін технічною службовою інформацією між мережами операторів. На відміну від SS7, Diameter спочатку створювався як захищений протокол: він підтримує шифрування, автентифікацію вузлів і контроль доступу, тому сторонні мережі не можуть легко видавати себе за операторів.

У контексті downgrade-атак та IMSI-catcherів Diameter важливий тим, що підсилює захист у LTE й унеможливлює багато сценаріїв шпигунства, характерних для SS7. Він не дає просто так запитати локацію абонента чи перехопити SMS, адже вузли мають підтверджувати свою справжність і працюють через захищені канали. Проте він не повністю ідеальний: деякі помилки конфігурації, старі вузли або шлюзи сумісності можуть створювати вразливості, особливо коли оператори з’єднуються з зовнішніми партнерами. Але загалом Diameter значно безпечніший за SS7 і став основою більш захищеної сигналізації у сучасних мобільних мережах.

- Атаки на IP-орієнтовану архітектуру (DoS, DDoS)



Оскільки LTE використовує IP-трафік, мережу можна атакувати звичайними методами інтернет-атак:

DoS і DDoS в контексті мобільних мереж — це атаки, що спрямовані не на перехоплення даних, а на виведення мережевих елементів із ладу або створення перевантаження, через яке послуги для абонентів стають недоступними. У класичних IT-системах це зазвичай flood-трафік, але в мобільних мережах додаються ще й специфічні механізми сигналізації.

У старіших системах, як SS7, зловмисник може надсилати масу некоректних або надмірних запитів на рівні сигналізації — наприклад, запити локації, аутентифікації чи оновлення стану абонента. Це перевантажує вузли оператора (HLR, VLR, MSC), які не розраховані на таку кількість запитів, і викликає затримки або повний збій обслуговування. У Diameter ситуація краща, бо є автентифікація й контроль доступу, але неправильні конфігурації або відкриті інтерфейси можуть дати змогу створювати аналогічні перевантаження.

На рівні радіомереж також можливі DoS: фальшива базова станція може зайняти всі канали або надсилати команди, що змушують телефони постійно перепідключатися, фактично «вибиваючи» їх із мережі. Такі атаки зазвичай не дають зловмиснику доступу до даних, але ефективно руйнують доступність — що інколи навіть шкідливіше, ніж перехоплення.

- Підміна та модифікація IMSI через LTE IMSI-catcher

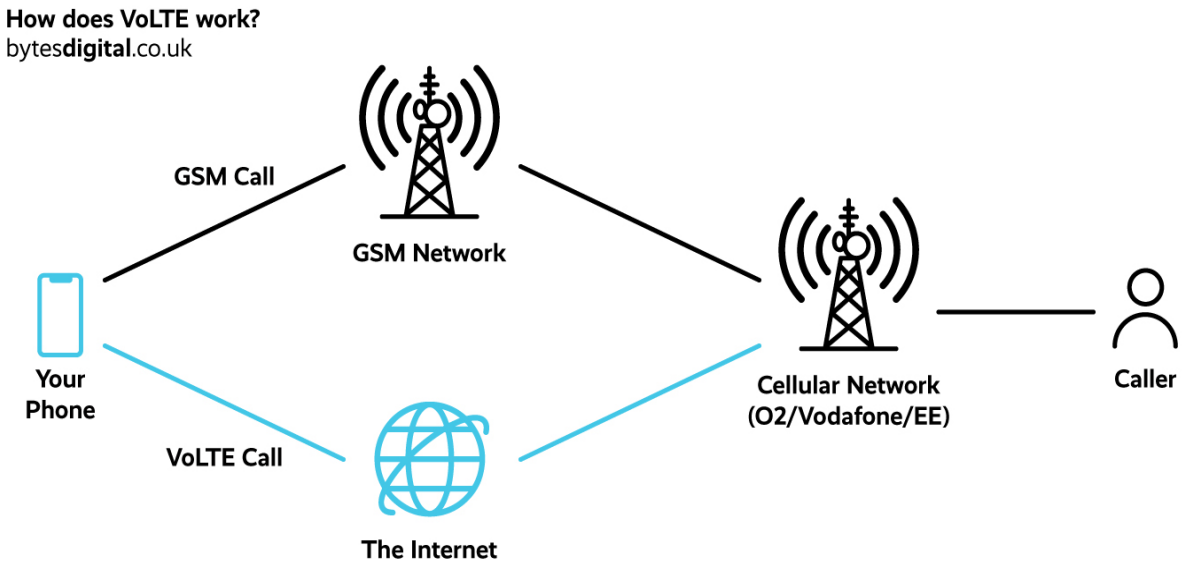


Підміна та модифікація IMSI через LTE IMSI-catcher — це атака, у якій фальшива базова станція змушує телефон розкрити свій справжній IMSI або прийняти підроблений ідентифікатор. У LTE телефон зазвичай використовує тимчасові TMSI й майже ніколи не передає IMSI відкрито, але IMSI-catcher створює умови, за яких пристрій «думає», що мережа легітимно запитує його справжній ідентифікатор. Це може відбуватися через нав’язаний повторний attach, примусовий «помилковий» reject, або через примушення телефону перейти в режим 2G/3G, де захист слабший.

Модифікація IMSI означає, що підроблена станція може видати телефону фальшиві параметри мережі, змінити TMSI або змусити його працювати з некоректними ідентифікаторами, чим фактично порушує нормальну логіку аутентифікації. У результаті смартфон можна відстежувати, вибивати з мережі (DoS) або переводити в режим, де подальші атаки — перехоплення, downgrade чи маніпуляції сигналізацією — стають можливими.

- Атаки на VoLTE

Атаки на VoLTE стосуються способу, у який голос у LTE передається як звичайний IP-трафік поверх спеціального сигнального протоколу IMS. Попри загальний сильний захист LTE, VoLTE має свою власну площину атак, яка пов’язана з тим, що голосовий сервіс залежить від коректної роботи IP-сесій, SIP-сигналізації та правильних ідентифікаторів абонента.



У контексті IMSI-catcherів, підміни ідентифікаторів та DoS, VoLTE стає вразливим тоді, коли зловмисник може впливати на початкову сигналізацію attach або змусити телефон перейти в некоректний режим. Підроблена базова станція (навіть якщо не може повністю відтворити IMS-ядро) може порушити логіку реєстрації SIP, викликати постійні повторні дзвінки, перенаправлення чи блокування викликів. У деяких випадках можлива зміна SIP-параметрів або маніпуляція QoS, що призводить до відмови VoLTE, затримок чи спотворення голосу. Також VoLTE може бути мішенню DoS, бо для роботи необхідно підтримувати стабільний IP-канал; достатньо збити інфраструктурні сигналізаційні повідомлення, і сервіс перестане працювати, навіть якщо LTE-дані залишаються доступними.

Загалом атаки на VoLTE рідко дають можливість прослуховування, але вони ефективні для підриву доступності голосу, вибивання абонента з сервісу або створення умов, у яких він змушений перейти на менш захищені режими дзвінків (наприклад, у 2G/3G), що відкриває шлях до подальших атак.

- Downgrade до 2G/3G

1.3.5 Кіберзагрози 5G — мереж надвисокої щільності та низької затримки

5G значно підвищує рівень безпеки: впроваджує SUCI, SBA-архітектуру, розділення контрольної та користувацької площин, Network Slicing. Однак складність мережі створює нові ризики.

- Атаки на Network Slicing

Network slicing у 5G — це механізм, який дозволяє оператору розділити одну фізичну мережу на кілька ізольованих «віртуальних мереж» (слайсів), кожна з яких має свої правила безпеки, пріоритети, пропускну здатність і навіть окремі служби (наприклад, окремий слайс для VoLTE/VoNR, окремий — для IoT, окремий — для критичних сервісів).

У контексті IMSI-catcherів, підміни ідентифікаторів, DoS та атак на VoLTE network slicing важливий тим, що він дозволяє логічно відокремити голосовий трафік або критичні служби від звичайного мобільного інтернету. Це ускладнює спроби порушити роботу всього сервісу через одну точку: атака на загальний LTE/5G трафік не повинна відразу «покласти» VoLTE чи інші ключові функції. Однак якщо зловмиснику вдається вплинути на сигналізацію доступу (наприклад, через downgrade чи фальшиву станцію), телефон може бути зареєстрований у неправильному слайсі або залишитися без потрібного слайсу зовсім — і тоді голосовий сервіс не запуститься, або буде працювати з перебоями.

Тобто network slicing підвищує захищеність завдяки ізоляції, але водночас створює нову площину атак: неправильно виданий слайс, відмова в доступі до потрібного слайсу або перенаправлення в слабший слайс можуть стати інструментами DoS проти VoLTE/VoNR чи інших критичних сервісів.

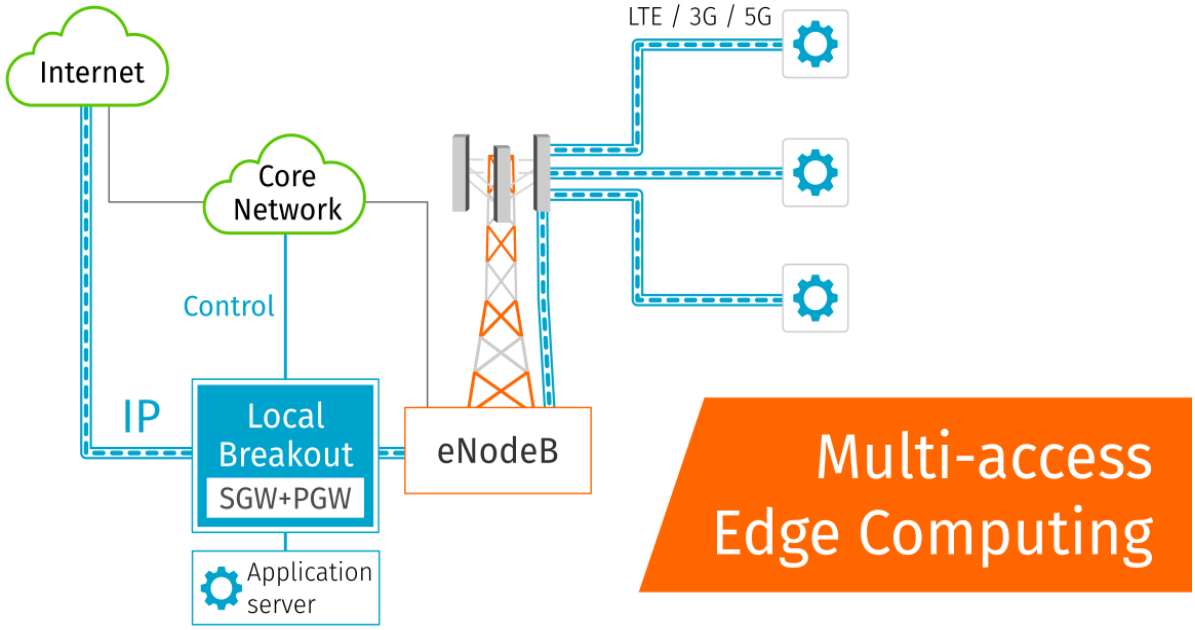
- Атаки на мережеві функції SBA (Service-Based Architecture)

SBA (Service-Based Architecture) у 5G — це нова архітектура ядра мережі, де всі ключові функції (аутентифікація, управління сесіями, політики, маршрутизація тощо) працюють як окремі мережеві сервіси, які взаємодіють між собою через стандартизовані API, подібно до мікросервісів у хмарі. Це робить мережу гнучкішою, масштабованішою та значно легше керованою.

У контексті network slicing, VoLTE/VoNR, DoS і атак на доступ SBA важлива тим, що кожен слайс і кожен сервіс (у тому числі голосові) залежить від правильного функціонування цих мережевих компонентів. Якщо зловмисник впливає на сигналізацію доступу (наприклад, через downgrade або фальшиву станцію), він може спричинити збій у виклику потрібних SBA-сервісів — наприклад, AMF чи SMF — і тоді телефон не отримає правильний слайс або не зможе зареєструвати VoLTE/VoNR.

SBA покращує безпеку за рахунок автентифікації вузлів, шифрування й гнучкої ізоляції сервісів, але водночас додає ризики: якщо DoS чи неправильні параметри доступу блокують виклик одного критичного сервісу, вся сесія абонента може зірватися, навіть якщо радіозв’язок залишився стабільним.

- Вразливості в MEC (Multi-access Edge Computing)



MEC (Multi-access Edge Computing) — це технологія, яка виносить обробку даних і частину 5G-функцій дуже близько до користувача, «на край мережі». Це зменшує затримки і дозволяє запускати сервіси (VoNR, AR/VR, відеоаналітика, IoT) практично локально. Але саме через це MEC стає новою критичною точкою атаки.

У контексті SBA, network slicing, VoLTE/VoNR та DoS головні вразливості MEC пов'язані з тим, що він працює як маленький локальний дата-центр, який повинен правильно взаємодіяти з сервісами ядра 5G. Якщо зловмисник порушує сигналізацію доступу (через downgrade, IMSI-manipulation, фальшиві стани attach), телефон може бути спрямований на некоректний MEC-вузол або не отримати потрібні edge-послуги. Через це критичні сервіси можуть працювати з перебоями або взагалі не запускатися.

Також MEC чутливий до локальних DoS: перевантаження edge-серверів або підміна їхніх параметрів може вивести з ладу конкретний слайс або сервіс (наприклад, голос, відео чи IoT), навіть якщо решта 5G-мережі працює нормально. Іншими словами, MEC значно підсилює можливості мережі, але додає окремий шар ризиків, де локальний збій або цілеспрямована атака може вибити з ладу певний сегмент користувачів чи цілий слайс.

- Атаки на масові IoT-пристрої

Атаки на масові IoT-пристрої у контексті MEC, SBA та network slicing стають критично важливими, тому що в 5G величезна кількість дрібних пристроїв

працює у спеціальних слайсах і часто покладається саме на edge-інфраструктуру. IoT-девайси зазвичай слабко захищені, погано оновлюються і мають мінімальну обчислювальну потужність, тому навіть прості атаки можуть легко «зламати» цілу групу пристроїв.

Якщо порушити роботу MEC або вплинути на доступ до потрібного слайса (через DoS, неправильну сигналізацію, підміну параметрів, маніпуляцію ідентифікаторами), IoT-пристрої починають масово відключатися, зависати чи втрачати доступ до своєї edge-логіки. Через це виникає «ланцюгова реакція»: тисячі пристроїв одночасно починають повторно під'єднуватись, що додатково перевантажує MEC та SBA-сервіси й може спричинити ширший збій.

Також зламані IoT-пристрої часто використовуються для DDoS на сам MEC або окремі 5G-сервіси, бо кожен з них хоч і слабкий, але разом вони формують величезну атакувальну силу. У результаті один вразливий клас IoT-девайсів може «покласти» окремий слайс або місцевий edge-кластер, навіть якщо основне ядро мережі працює нормально.

- Глушіння та втручання в mmWave

Глушіння та втручання в mmWave — це атаки, спрямовані проти високочастотних 5G-смуг, які надзвичайно чутливі до перешкод. mmWave працює на дуже високих частотах, де сигнал слабшає швидко, погано проходить крізь перешкоди й залежить від точного спрямування променя (beamforming, massive MIMO). Через це навіть відносно слабкі джерела шуму можуть повністю зірвати зв'язок.

У контексті MEC, IoT, SBA та network slicing такі атаки особливо небезпечні, бо mmWave часто використовується для навантажених або критичних сервісів — наприклад, локальної аналітики на MEC або швидкісного підключення IoT у промисловості. Якщо зловмисник створює шум у потрібній частоті чи «збиває» формування променя, пристрої перестають отримувати стійкий сигнал: вони масово перепід'єднуються, падають з mmWave у слабші смуги або взагалі втрачають зв'язок.

Це викликає локальний DoS на рівні радіоінтерфейсу, але наслідки стають системними: MEC перевантажується повторними запитами, IoT-масиви виходять з ладу, SBA-сервіси не встигають обробляти відновлення сесій, а необхідні network slices тимчасово «відвалюються». Тобто навіть проста перешкода в mmWave може спричинити збій цілого сегмента 5G-мережі, якщо він покладається на локальні edge-сервіси та масові IoT.

1.3.6 Кіберзагрози 6G

Уразливості, зумовлені залежністю від штучного інтелекту (AI-native networks). 6G стане першою мережею, де ШІ — не додаткова функція, а основа всієї архітектури. Це створює низку принципово нових загроз:

- Атаки на моделі ШІ (Model Poisoning, Data Poisoning)

Атаки на моделі ШІ в 6G (Model Poisoning, Data Poisoning) стають ще небезпечнішими, ніж у 5G, тому що в 6G ШІ інтегрований не просто в MEC, а в усю архітектуру мережі: від радіочастотного управління до маршрутизації, beamforming, IoT-аналітики й навіть самооптимізації мережі. 6G фактично покладається на автономні AI-моделі, які працюють локально на edge-вузлах, у гіперлокальних MEC-кластерах і навіть на самих IoT-пристроях. У цьому контексті атаки стають такими:

Data Poisoning у 6G означає підміну або спотворення даних, які надходять у локальні AI-моделі (відео, сенсори, трафік IoT, RF-сигнали). Оскільки 6G масово використовує федеративне навчання на edge-рівні, зловмисник може маніпулювати даними, які окремі вузли відправляють для оновлення моделі. У результаті мережа приймає неправильні рішення: beamforming починає працювати некоректно, IoT-потоки класифікуються неправильно, а критичні сервіси можуть зупинятись.

Model Poisoning у 6G означає цілеспрямовану зміну ваг або логіки самої AI-моделі, що працює на edge-вузлі або в MEC. Через те, що 6G дозволяє автоматично оновлювати моделі та обмінюватися параметрами між вузлами, одна отруєна модель може поширити хибні параметри на весь регіональний кластер. Це здатне порушити роботу цілого network slice, вплинути на тисячі IoT-пристроїв або навіть послабити захист на рівні радіоінтерфейсу.

У зв’язку з попереднім контекстом (mmWave-глушіння, IoT-масиви, MEC-перевантаження) такі атаки стають ще ефективнішими: достатньо викликати збій у датчиках чи навмисно спотворити edge-трафік, щоб моделі отримали некоректні дані й почали масово приймати хибні рішення. У 6G це може спричинити каскадні збої, де IoT-кластер, MEC-вузол і цілий AI-керований network slice втрачають функціональність.

- Adversarial Attacks та AI-as-a-Target атаки

Adversarial Attacks та AI-as-a-Target у 6G — це атаки, спрямовані безпосередньо на ШІ-моделі, що керують роботою мережі. У 6G вони особливо

небезпечні, бо штучний інтелект відповідає за beamforming, маршрутизацію, розподіл ресурсів, захист IoT-кластерів, аналіз радіосигналів і роботу MEC.

Adversarial Attacks — це створення спеціальних «ворожих» сигналів, даних або пакетів, які виглядають нормальними, але змушують модель помилятися. У 6G це може бути мікрозміна RF-параметрів, IoT-телеметрії чи мережевих метаданих, щоб AI-алгоритми неправильно налаштовували промені mmWave, пропускали шкідливий трафік або відключали частину базових станцій.

AI-as-a-Target означає, що самі AI-моделі стають основною ціллю. Зловмисник може атакувати їх через MEC, через OTA-оновлення моделі, або через вразливості у federated learning. Мета — отримати контроль над алгоритмами, які керують slice-ами, QoS, IoT та радіоресурсами.

- Квантові загрози для криптографії

Квантові комп’ютери в 6G-мережах становлять пряму загрозу для традиційних криптосистем, таких як RSA, ECC і Diffie-Hellman, бо алгоритм Шора дозволяє швидко розкладати великі числа та знаходити дискретні логарифми — тобто зламувати те, що сьогодні вважається криптостійким.

У контексті попереднього (AI-атаки, MEC, AI-as-a-Target, data poisoning) це означає, що з появою потужних квантових машин з’явиться можливість розшифровувати трафік між ключовими елементами 6G: між базовими станціями, MEC-вузлами, edge-кластерами, вузлами federated learning і навіть між AI-модулями, що координують network slicing та beamforming. Якщо RSA/ECC/DH будуть зламані, зловмисник зможе перехопити ключі, розшифрувати оновлення моделей, підробити дані для AI або втрутитися в процес управління мережею.

У результаті квантова загроза посилює всі попередні атаки: adversarial вплив, poisoning, AI-as-a-Target — бо з’являється можливість не тільки маніпулювати даними, а й повністю читати та імітувати закриті канали між вузлами 6G. Саме тому в 6G вже закладається перехід до постквантової криптографії та квантово-безпечних протоколів.

2. Квантові технології в мережах мобільного зв’язку та їх кіберзагрози

2.1 Квантові технології

Під квантовими технологіями зазвичай розуміють набір підходів і пристроїв, що опираються на властивості квантової механіки: суперпозицію, переплутаність (entanglement), квантові вимірювання тощо. Найпоширеніші підгрупи — квантові обчислення (quantum computing), квантова криптографія/квантове розподілення ключів (QKD), квантова телекомунікація та квантові сенсори. У мобільному зв’язку ці технології розглядають як інструменти як для підвищення безпеки та продуктивності, так і як джерело нових загроз.



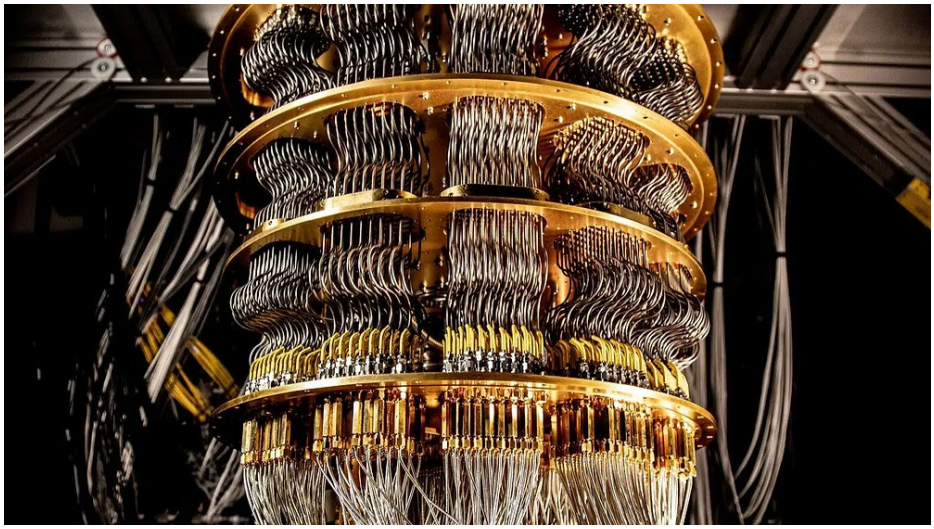
Квантові технології одночасно дають можливості (наприклад, захищене розподілення ключів або прискорення певних алгоритмів оптимізації) і створюють загрози (в першу чергу — загроза зламування традиційних криптосхем квантовими комп’ютерами). Для мобільних мереж — де важливі конфіденційність, аутентифікація, цілісність і доступність — це породжує як технічні, так і організаційні виклики.

Квантові технології спираються на властивості квантової механіки — суперпозицію, заплутаність, квантове тунелювання та дискретність енергії. На

основі цих принципів формуються кілька ключових систем, кожна з яких виконує різні завдання: обчислення, зв’язок, вимірювання, шифрування та сенсори.

2.2 Як працюють квантові технології, їх різновиди

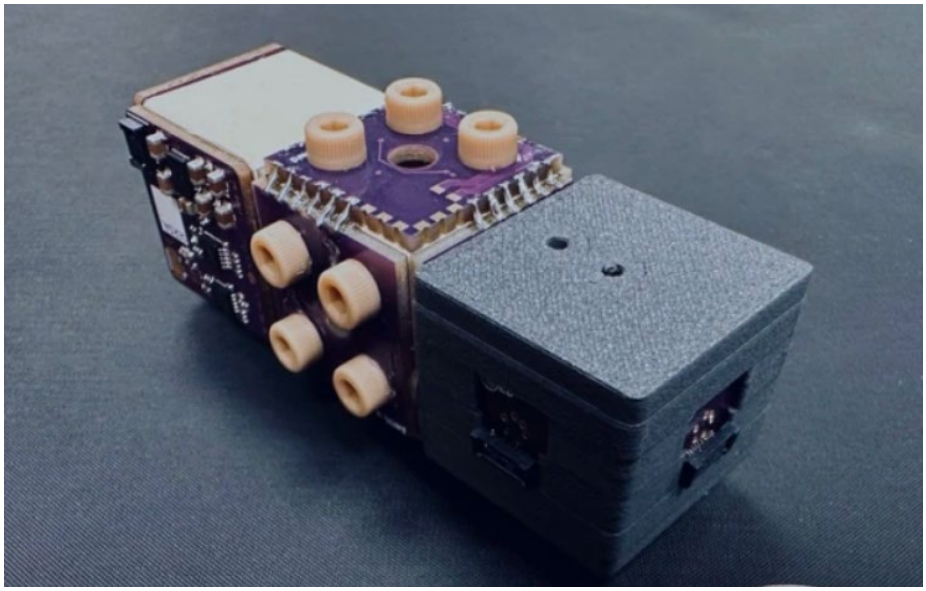
Основою квантових технологій, є квантові обчислення системи квантових комп’ютерів, де інформація зберігається у квантових бітах — кубітах. На відміну від класичних бітів, кубіт може перебувати в суперпозиції, тобто одночасно у станах 0 і 1, що дає змогу здійснювати паралельну обробку великої кількості можливих значень. Друга ключова властивість — заплутаність, коли стан одного кубіта миттєво пов’язаний зі станом іншого, незалежно від відстані. Це дає змогу створювати квантові алгоритми, які значно перевершують класичні: алгоритм Шора для факторизації, алгоритм Гровера для пошуку, квантові симуляції фізичних систем та оптимізаційні процедури. Реалізації кубітів можуть бути різними: надпровідникові контури, іонні пастки, фотонні кубіти, спіни NV-центрів у алмазі, топологічні кубіти. Однак квантові комп’ютери вразливі до декогеренції, шуму і помилок, тому практична реалізація вимагає складних механізмів квантової корекції помилок і так званих логічних кубітів, які складаються з сотень фізичних.



Окремим напрямом є квантові комунікації, що використовують квантові стани світла для передавання інформації. Найважливішим інструментом у них є квантовий розподіл ключів, який дозволяє двом сторонам створювати спільні криптографічні ключі таким чином, що будь-яке перехоплення автоматично змінює квантовий стан і стає помітним. Це робить протокол фізично захищеним,

на відміну від традиційних методів, які покладаються на математичну складність. Реалізація квантових мереж передбачає використання фотонних каналів, оптоволокна, супутникових ліній і квантових повторювачів, які дозволяють долати обмеження відстані. У перспективі формується концепція квантового інтернету — глобальної мережі, де квантові стани передаються між вузлами так само звично, як сьогодні передаються цифрові дані.

Третя основна категорія — це квантові сенсори. Вони використовують надзвичайну чутливість квантових систем до змін у магнітних, електричних чи гравітаційних полях. Наприклад, атомні інтерферометри здатні з надвисокою точністю вимірювати прискорення та обертання, оптичні решітчасті годинники забезпечують найточніший час у світі, а магнітометри на основі NV-центрів в алмазі можуть реєструвати магнітні поля окремих молекул чи нейронів. Завдяки цьому квантові сенсори відкривають можливість для точнішого GPS, медичної діагностики на нанорівні, геологічного аналізу та виявлення підземних структур.

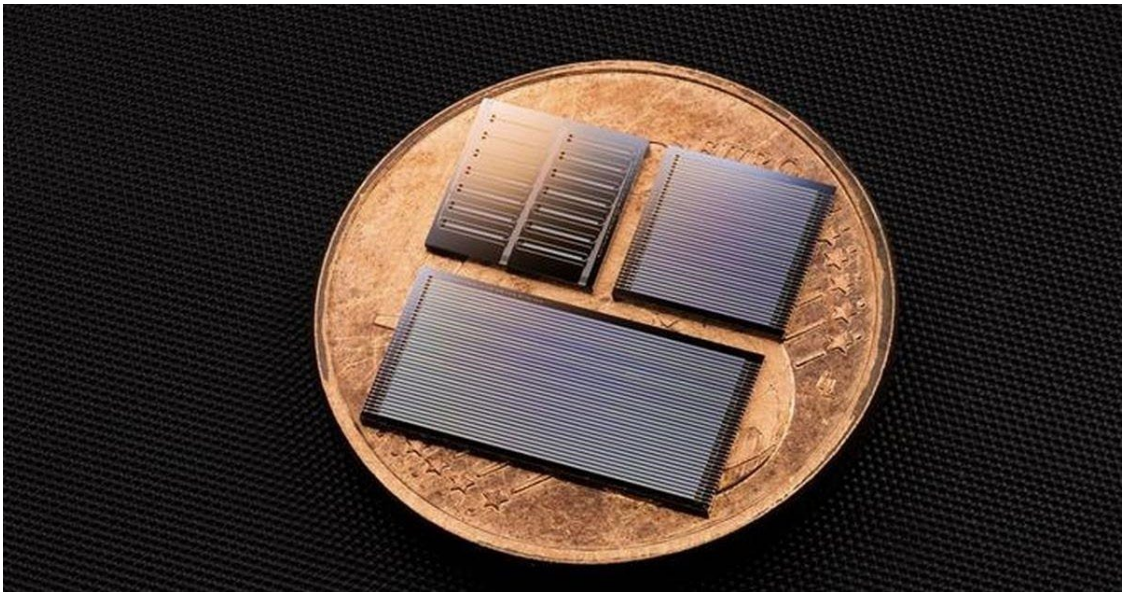


Ще один важливий напрям — квантові симулятори. Вони створені для відтворення поведінки складних квантових систем, таких як надпровідники, молекули, хімічні реакції або матеріали з нетривіальними фазами. На відміну від універсальних квантових комп’ютерів, симулятори спеціалізовані, але значно стійкіші та продуктивніші в конкретних задачах. Їх використовують у фармакології, матеріалознавстві, моделюванні плазми й у вивченні фундаментальної фізики.

Свою роль відіграють і постквантові криптосистеми — це вже не квантові пристрої, але математичні алгоритми, створені для протистояння атакам

квантових комп’ютерів. Вони використовують задачі, які складні не лише для класичних, але й для квантових алгоритмів: решіткові криптографічні схеми, хеш-орієнтовані підписи, кодові та мультимеморандумні системи. Їх інтеграція в мережі майбутнього є критично важливою, оскільки квантові комп’ютери зможуть розламувати сучасні RSA, ECC і DH.

Окремо варто згадати квантову фотоніку — апаратну основу для багатьох квантових технологій. Це мініатюрні фотонні чипи, які маніпулюють одиничними фотонами, створюють заплутані стани, проводять обчислення та передають інформацію. В майбутніх мережах саме фотонні квантові модулі стануть ядром комунікаційних систем, оскільки вони поєднують високу швидкість, низькі втрати та сумісність з оптоволоконними технологіями.



Усі ці системи формують екосистему квантових технологій, де обчислення, зв’язок, шифрування, вимірювання й моделювання взаємодіють у єдиній інфраструктурі. Квантові комп’ютери працюють над задачами, які недосяжні для класичних машин; квантові мережі забезпечують фізичну захищеність зв’язку; квантові сенсори створюють новий рівень точності; симулятори прискорюють наукові відкриття; а постквантова криптографія захищає цифрову інфраструктуру до моменту повної зрілості квантових систем. У сукупності це створює фундамент для технологічної бази наступних поколінь зв’язку, безпеки та обчислень.

2.3 Де й як квантові технології інтегруються у мобільні мережі

- Клієнтський рівень (UE / абонентські пристрої): QKD-сумісні модулі

QKD-сумісні модулі — це апаратні компоненти, які дозволяють мережевому обладнанню працювати з технологією квантового розподілу ключів (QKD, Quantum Key Distribution). Вони інтегруються у телеком-інфраструктуру так само, як оптичні або криптографічні модулі, але мають здатність генерувати, передавати та приймати квантові стани світла, що використовуються для формування абсолютно захищених криптографічних ключів.



По суті, кожен QKD-модуль виконує кілька критичних функцій. Перша — створення одиничних фотонів або слабких оптичних імпульсів, що несуть квантові стани (поляризацію, фазу або часові бінарні інтервали). Друга — вимірювання цих квантових станів на приймальному боці з використанням високочутливих фотодетекторів. Третя — виявлення будь-якого втручання: оскільки перехоплення змінює квантовий стан, модуль одразу фіксує спробу прослуховування. Четверта — узгодження й корекція помилок, після яких обидві сторони (наприклад, два вузли мережі) отримують однаковий випадковий секретний ключ.

Такі модулі проєктуються таким чином, щоб підключатися до існуючих мережевих пристроїв — комутаторів, маршрутизаторів, базових станцій, оптичних транспортних систем. Вони використовують стандартне оптоволокно або спеціальні канали, сумісні з DWDM, що дозволяє розміщувати квантовий канал паралельно зі звичайними даними. Зазвичай вони працюють парами: один модуль у передавальному вузлі, другий — у приймальному, синхронізовані за часом і протоколами.

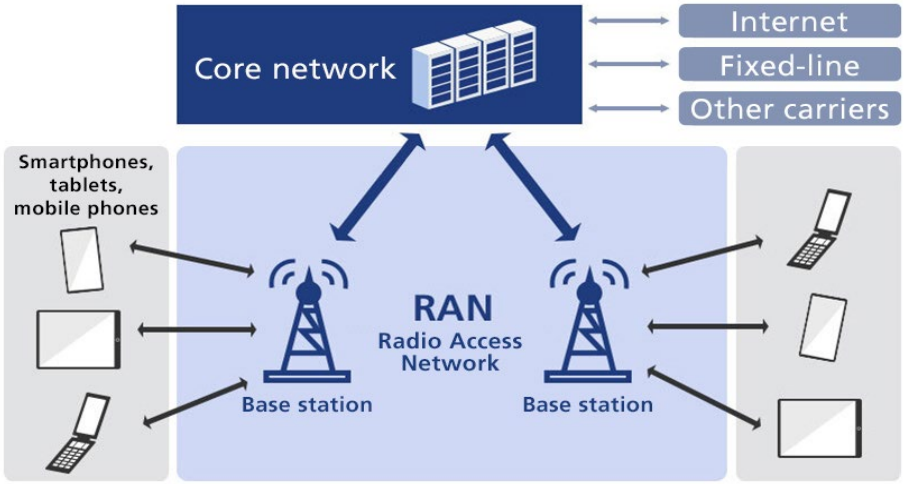
Основна їхня цінність полягає в тому, що вони дають змогу створювати ключі, стійкі до квантового злому. Навіть якщо з’явиться квантовий комп’ютер, здатний розкласти RSA чи зламати ECC, ключі, отримані через QKD, залишаться недоступними для дешифрування, бо їх безпека базується не на математиці, а на фізиці квантових вимірювань.

Таким чином, QKD-сумісні модулі — це апаратна основа для побудови квантово-безпечних мереж, де криптографічні ключі формуються в реальному часі та гарантовано захищені від перехоплення. Вони вже розглядаються як обов’язковий компонент майбутніх 6G-мереж, критичної інфраструктури, банківських та урядових комунікацій.

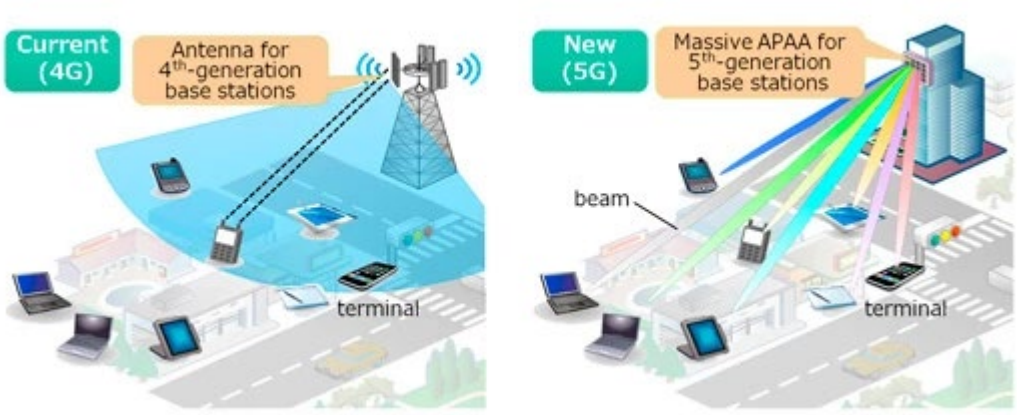
- RAN (радіодоступ), beamforming.

Квантова обробка для оптимізації ресурсів, квантові сенсори для покращення локалізації/управління променем.

RAN (Radio Access Network) — це частина мобільної мережі, яка забезпечує радіодоступ між користувачами та ядром мережі. Саме RAN відповідає за передачу сигналу між смартфоном, IoT-пристроями чи будь-яким радіотерміналом і базовими станціями. У традиційних мережах це були переважно звичайні макровежі, але в сучасних 5G–6G RAN став набагато складнішим: він складається з тисяч малих осередків, масивів антен, розподілених радіоелементів і часто працює разом із Cloud RAN або Open RAN. Основне завдання RAN — управляти радіочастотами, забезпечувати доступ, контроль потужності, хендовери, обробку радіосигналів і взаємодію з ядром мережі. RAN постійно оцінює якість каналу, інтерференцію, навантаження та динамічно розподіляє радіоресурси, щоб забезпечити стабільний зв’язок у реальних умовах.



Beamforming — це технологія керованого спрямування радіосигналу, яка дозволяє RAN «фокусувати» енергію не навсібіч, а точно в напрямку конкретного користувача чи пристрою. Якщо порівняти класичні антени з ліхтариком, що світить рівномірно, то beamforming — це лазерний промінь, який підлаштовується під рух абонента. Замість однієї антени використовується масив антен (MIMO або massive MIMO), які передають сигнали з точно розрахованими фазами. Завдяки цьому хвилі підсилюють одна одну в потрібному напрямку і гасяться в інших. Це робить зв'язок сильнішим, швидшим і захищенішим, особливо на високих частотах (наприклад, mmWave), де затухання дуже велике.

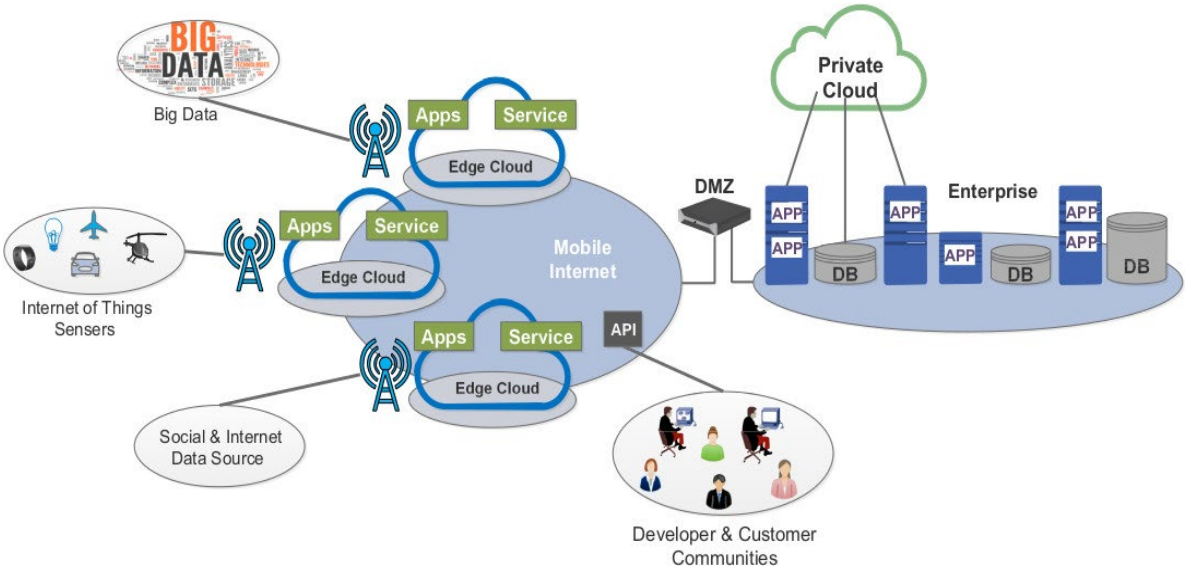


У комплексі RAN та beamforming забезпечують високу спектральну ефективність і точну доставку радіосигналу. RAN відповідає за всі процеси радіодоступу, а beamforming — за інтелектуальне спрямування хвиль, щоб покращити покриття, пропускну здатність та енергетичну ефективність у сучасних мобільних мережах.

- Edge / MEC: вузли, де можна розмістити квантово-захищені сервіси, ключові менеджери з QKD-терміналами або гібридні криптосервіси

Edge / MEC (Multi-access Edge Computing) — це розподілена архітектура, у якій частина обчислень, зберігання даних і сервісів переноситься з центрального дата-центру ближче до користувачів — на «край» мережі. Це можуть бути невеликі серверні вузли біля базових станцій, в локальних дата-центрах операторів, у транспортних вузлах або навіть всередині великих підприємств.

У контексті квантово-безпечних систем Edge/MEC набуває особливо важливого значення. Саме ці вузли стають майданчиком, де можна розміщувати квантово-захищені сервіси, оскільки вони ближче до реальних користувачів, мають низькі затримки й можуть швидко управляти ключами, трафіком і безпековими політиками.



MEC-вузли можуть містити QKD-термінали — пристрої, які генерують квантові ключі за допомогою одиничних фотонів. У MEC вони розташовуються достатньо близько одне до одного, тому оптоволокно між ними не має великих втрат, а QKD працює стабільно. Кожен такий вузол отримує квантові ключі від іншого вузла або від центрального квантового «кореня», і далі може роздавати ці ключі локальним сервісам — шифруванню трафіку, AI-процесам, управлінню IoT, захищеним каналам до базових станцій.

Edge/MEC виступає місцем розміщення ключових менеджерів. Це системи, що беруть ключі з QKD-терміналів і перетворюють їх у придатний для мережевих сервісів формат: IPsec, TLS, MACsec, квантово-безпечні VPN або гібридні криптографічні протоколи (постквантові алгоритми + QKD). Саме менеджери вирішують, у який момент оновлювати ключ, як його поширювати до найближчих RAN-вузлів, як інтегрувати його в slice або MEC-додаток.

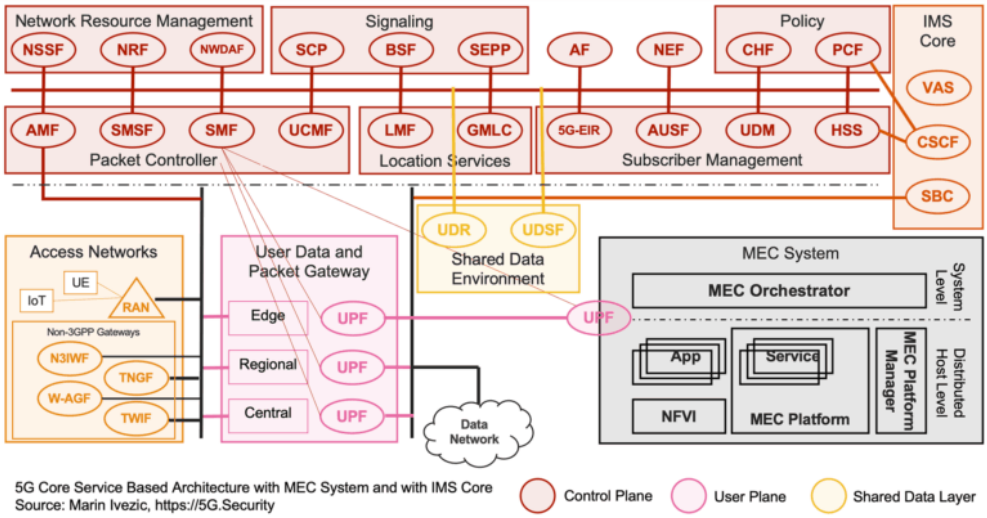
На Edge/MEC можна розміщувати гібридні криптосервіси. Це сервіси, які одночасно використовують QKD-ключі та постквантові математичні алгоритми. Гібридна модель потрібна, тому що QKD працює тільки через оптичний канал між вузлами, а постквантові алгоритми можна застосувати поверх будь-якої мережі. MEC ідеально підходить, бо може забезпечити обчислення й ключову логіку поруч із місцем, де опрацьовується трафік користувачів.

Фактично MEC стає першою лінією квантового захисту. Ключі генеруються на краю мережі, там же інтегруються в шифрування, трафік не потрібно вести в центральний дата-центр для обробки, а квантово-безпечні канали створюються між сусідніми вузлами або між вузлом MEC і RAN. Це дає високу швидкість, низьку затримку та стійкість до квантових атак, оскільки основний криптографічний захист здійснюється локально, а не десь далеко в центрі мережі. У результаті Edge/MEC стає не просто обчислювальним

майданчиком, а квантово-орієнтованим безпековим вузлом, який забезпечує швидку генерацію ключів, локальний розподіл квантового захисту та інтеграцію гібридної криптографії в 5G–6G мережах.

- Core (SBA, 5GC): захищені канали управління, використання PQC для аутентифікації, можливе підключення до квантових шлюзів і менеджерів ключів.

Core мережі в 5G/6G — це центральна частина мобільної інфраструктури, де зосереджені всі функції управління, маршрутизації, аутентифікації, політик безпеки та інтелектуальної логіки. У 5G ця частина працює за моделлю SBA (Service-Based Architecture) — архітектурою, у якій кожна функція ядра є окремим сервісом, що взаємодіє з іншими через захищені API. Така структура гнучка, масштабована та сумісна з хмарними технологіями, але водночас висуває високі вимоги до шифрування та автентифікації, оскільки десятки сервісів постійно обмінюються чутливими даними.



У контексті квантової стійкості ядро мережі (5GC) має виконувати три ключові функції: забезпечувати захищені канали управління, використовувати постквантову криптографію (PQC) для автентифікації вузлів і взаємодії сервісів, а також підтримувати інтеграцію з квантовими шлюзами та системами управління ключами, які працюють на основі QKD або гібридного підходу.

Перший елемент — захищені канали управління. У SBA сервіси ядра постійно передають один одному інформацію: статус абонентів, політики безпеки, параметри сесій, телеметрію, маршрутизацію трафіку та дані аутентифікації. Усе це має бути зашифровано та захищено від підробки, оскільки

компрометація хоча б одного каналу дозволяє зловмиснику втрутитися в роботу цілої мережі. Сьогодні для цього використовують TLS й IPsec, але з появою квантових комп'ютерів такі канали можуть бути вразливими, тому необхідно переходити на PQC або гібридне шифрування, де частина ключів створена постквантовим алгоритмом, а частина може бути забезпечена QKD.

Другий елемент — використання постквантової криптографії для аутентифікації. Оскільки 5G/6G-ядро є повністю програмним і складається з багатьох мікросервісів, кожен сервіс має регулярно підтверджувати свою справжність. Для цього застосовують цифрові підписи, сертифікати, криптографічні протоколи та механізми взаємної автентифікації. Проблема в тому, що класичні схеми на RSA або ECC у майбутньому можуть бути зламані квантовими комп'ютерами. PQC-алгоритми — решіткові, кодові, хешеві схеми — дозволяють створювати підписи та ключі, які стійкі до атак квантових алгоритмів, а отже гарантують, що ядро можна буде захистити навіть тоді, коли квантові комп'ютери стануть доступними.

Третій елемент — це інтеграція з квантовими шлюзами та менеджерами ключів. Квантовий шлюз — це спеціалізований модуль (фізичний або віртуальний), який приймає ключі з QKD-мережі або з гібридних систем, а потім розподіляє їх між сервісами ядра. Менеджер ключів функціонує як центр управління криптографією у 5GC: він визначає, які сервіси отримають який ключ, коли ключ потрібно оновити, коли використовувати QKD, а коли PQC, і яким чином ключ включається в канали SBA. У 6G такі менеджери будуть працювати в автоматичному режимі та інтегруватися з MEC-вузлами, RAN і зовнішніми квантовими мережами.

У результаті ядро 5G/6G перетворюється на квантово-безпечний центр, де канали управління шифруються з урахуванням майбутніх квантових загроз, кожен сервіс аутентифікується за допомогою постквантових алгоритмів, а ключі можуть надходити як із класичних криптосистем, так і зі справжніх квантових ліній. Це робить ядро стійким до атак квантових комп'ютерів і забезпечує повну безпеку взаємодії між усіма компонентами мобільної мережі.

- Backhaul / transport: оптичні лінії можуть підтримувати QKD (через тунелі або виділені волокна); це особливо релевантно для операторів, що мають власні транспортні мережі.

Backhaul і transport у мобільних мережах — це опорна магістральна інфраструктура, що забезпечує зв'язок між радіодоступом (RAN) та ядром мережі (Core). Фактично це вся фізична та логічна мережа, яка переносить мобільний трафік від базових станцій до центральних обчислювальних вузлів оператора. У 5G і особливо у 6G ця частина мережі стає набагато складнішою, бо

повинна забезпечувати дуже високі швидкості, мінімальні затримки, підтримку масового IoT, розподілених систем ШІ та нових моделей безпеки, включаючи постквантову криптографію і квантовий розподіл ключів.

Backhaul у широкому сенсі — це вся інфраструктура, що з'єднує gNB, RAN-вузли, агрегаційні точки та маршрутизатори з ядром мережі. Найчастіше він побудований на оптоволоконних каналах (DWDM-лінії), мікрохвильових радіорелейних лінках або L2/L3 Ethernet/MPLS транспорті. Через ці канали рухається як користувацький трафік (тобто дані абонентів), так і сигнальний трафік, який відповідає за керування з'єднаннями, мобільністю, безпекою, аутентифікацією і розподілом ресурсів. Transport — це ширше поняття, яке охоплює всі рівні передачі: фронтхоул (RU–DU), мідхоул (DU–CU) і бекхоул (CU/gNB–Core), а також магістральну IP/MPLS або Segment Routing інфраструктуру. Transport-мережа керує маршрутизацією, пріоритезацією трафіку, наданням гарантованої якості обслуговування, синхронізацією часу (PTP, SyncE), а у 6G також підтримує мережеву автономність, динамічне виділення ресурсів і інтелектуальні механізми самооптимізації.

У контексті безпеки backhaul/transport є одним із найбільш критичних сегментів, оскільки тут проходять найбільш важливі й найчутливіші дані мережі: ключі шифрування, службові канали, інформація про місцерозташування абонентів, параметри керування мережею, міжвузловий трафік, а також телеметрія від RAN і Core. Будь-яке порушення безпеки на транспортному рівні може дати зловмиснику можливість перехоплювати трафік, маніпулювати сигнальними протоколами (наприклад, PFCP, NGAP), атакувати маршрутизатори, здійснювати перенаправлення трафіку або втручатися у критичні сервіси URLLC. У 6G, через зростання ролі edge-комп'ютингу, туди додатково потрапляють дані ШІ-моделей, управлінська інформація для beamforming, хмарні ресурси BO-RAN і велика кількість даних від IoT.

Основний виклик для backhaul/transport у майбутніх мережах пов'язаний із переходом на постквантові криптосистеми, оскільки традиційні механізми шифрування (RSA, ECC, DH) у майбутньому стануть уразливими для квантових обчислень. Тому транспортна інфраструктура має підтримувати нові типи захисту: PQC-алгоритми в IPsec і MACsec, гібридні схеми шифрування, а також інтеграцію з квантовими ключовими менеджерами. Якщо оператор впроваджує QKD-лінії, саме по оптоволоконних транспортних каналах проходить квантовий розподіл ключів, а маршрутизатори та комутатори обладнують QKD-сумісними модулями. Транспорт таким чином стає основою для побудови квантово-захищеного простору обміну ключами між RAN, edge та core.

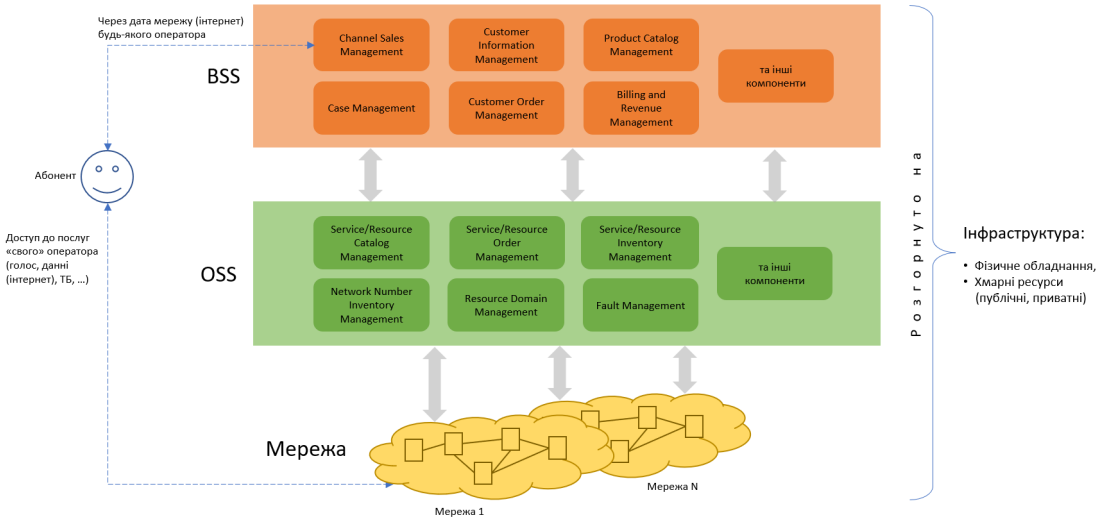
У 6G транспорт також виконує функцію інтелектуальної магістралі. Він переносить не просто IP-трафік, а великий масив даних для алгоритмів ШІ, що

керують мережею, включаючи прогнозування навантаження, оптимізацію beamforming, динамічну перебудову маршрутизації та аналіз безпекових подій у реальному часі. Це означає, що transport повинен бути надзвичайно стабільним, підтримувати мікросекундну синхронізацію, мати механізми самовідновлення й працювати під контролем розподілених AI-агентів. З огляду на це transport розглядається як один з головних компонентів, де оператори першими впроваджуватимуть квантові засоби безпеки, PQC-протоколи, сегментовані маршрути SRv6, а також захищені канали для критичних сервісів.

Таким чином, backhaul/transport — це ключовий рівень мобільної інфраструктури, який з'єднує радіодоступ і ядро, забезпечує пересилання даних, сигналізації та управління, а в епоху 6G стає магістраллю для квантово-захищеного трафіку, транспортом для ШІ-алгоритмів та критично важливим сегментом з точки зору кібербезпеки.

- OSS/BSS та хмарні сервіси: збереження і обробка даних з урахуванням квантових ризиків (довгострокова конфіденційність) — перехід на PQC в усіх сервісах.

OSS/BSS та хмарні сервіси в мобільних мережах — це управлінська та бізнес-інфраструктура оператора, яка відповідає за роботу всієї мережі, її планування, обслуговування, взаємодію з абонентами, тарифікацію, аналітику та збереження великих обсягів даних. У 5G і особливо в майбутніх 6G-системах ці сервіси стають ще важливішими, оскільки працюють у хмарному форматі, інтегровані з інтелектуальними системами ШІ, зберігають критичні дані про мережу та абонентів, і забезпечують автоматизацію на рівні всього оператора. Саме тому вони особливо вразливі до квантових атак і потребують переходу на постквантову криптографію.



OSS (Operations Support Systems) — це операційна частина, що керує технічною стороною мережі. Тут відбувається моніторинг стану обладнання, аналіз роботи RAN, transport і core, планування розгортання нових базових станцій, обробка телеметрії, оптимізація ресурсів, управління fault-алертами, автоматизація оновлень мережі та інтеграція з системами AI/ML для прогнозування навантаження або виявлення аномалій. OSS працює з великими масивами технічних даних, історією конфігурацій, логами, інженерними параметрами й елементами управління мережею. Багато з цих даних повинні зберігатися десятиліттями, а довгострокова конфіденційність — дуже важлива, бо конфігурація мережі, маршрути, коди помилок і налаштування безпеки є стратегічною та чутливою інформацією. У контексті квантової загрози OSS повинен переходити на постквантові алгоритми шифрування, щоб дані, зашифровані сьогодні, не могли бути розшифровані майбутнім квантовим комп'ютером.

BSS (Business Support Systems) — це бізнес-рівень оператора. Він керує білінгом, абонентськими профілями, тарифами, транзакціями, CRM-системами, історією платежів, деталізацією дзвінків та даних, а також аналітикою поведінки абонентів. Ця інформація не просто конфіденційна — вона юридично регулюється та зберігається протягом багатьох років. Якщо квантовий комп'ютер у майбутньому зламає RSA або ECC, великі архіви BSS можуть бути розшифровані заднім числом, що означає витік персональних даних мільйонів абонентів. Тому перехід на PQC у BSS є критичним не лише з технічної, а й з правової точки зору.

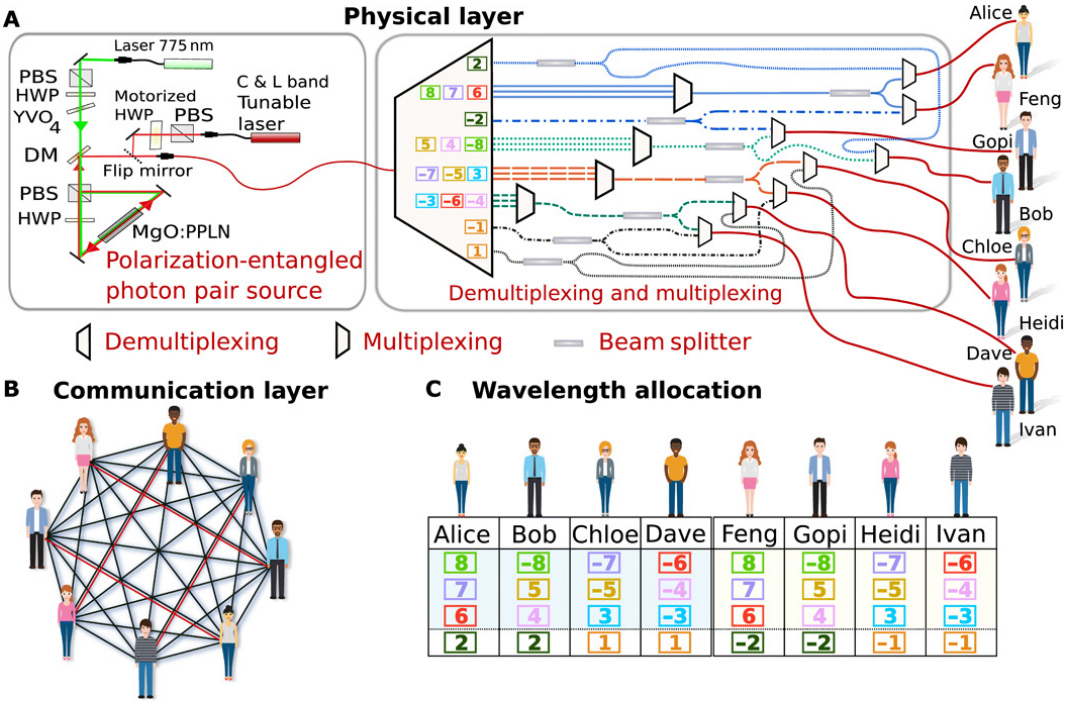
Хмарні сервіси, які використовує оператор (приватні, публічні або гібридні), також зберігають величезні обсяги чутливої інформації: журнали RAN/Core, дані про переміщення абонентів, метадані трафіку, моделі ШІ, аналітичні дані, телеметрію транспортних мереж, інформацію про slice-и та політики доступу. У 5G/6G усе це розміщується в контейнеризованих середовищах, мікросервісах та SBA-архітектурі. З точки зору квантових ризиків це означає, що збережений у хмарі трафік або дані, які сьогодні шифруються класичними алгоритмами, необхідно захищати методами, стійкими до квантових атак, бо в майбутньому їх можуть розшифрувати заднім числом.

Перехід на PQC в OSS/BSS та хмарних сервісах — це не просто оновлення алгоритмів, а комплексне завдання: заміна сертифікатів, нові криптографічні бібліотеки, перехід на гібридні схеми шифрування, перевірка сумісності з legacy-сервісами, підтримка довгострокового збереження конфіденційності, захищені канали між сервісами і захист API, через які обмінюються даними різні компоненти SBA/Cloud-інфраструктури. Оскільки ці сервіси управляють усією мережею та зберігають її найцінніші дані, вони стають одними з перших, які мають бути переведені на постквантову криптографію, щоб майбутні квантові

атаки не могли отримати доступ до трафіку, налаштувань та історичних записів, навіть якщо ці дані будуть перехоплені або збережені зловмисником сьогодні.

2.4 Позитивні ефекти від застосування квантових технологій у мережах мобільного зв'язку

Впровадження квантових технологій у мобільні мережі створює якісно новий рівень безпеки, продуктивності та довгострокової надійності інфраструктури зв'язку. Один із ключових ефектів полягає в тому, що квантова криптографія забезпечує математично недосяжний для класичних методів рівень захисту. Зокрема, QKD (Quantum Key Distribution) дає можливість генерувати та розповсюджувати криптографічні ключі способом, який неможливо перехопити непомітно, оскільки будь-яке втручання змінює квантовий стан фотонів і одразу виявляється. Це дозволяє створювати канали зв'язку, які забезпечують довготривалу конфіденційність навіть у перспективі появи потужних квантових комп'ютерів. На відміну від класичної криптографії, яка з часом стає вразливою до зростання обчислювальних ресурсів, квантові методи залишаються безпечними навіть теоретично, оскільки базуються на законах фізики, а не на складності математичних задач.



Ще одна важлива перевага — стійкість до загроз майбутнього, включно з можливістю «записати зараз — розшифрувати потім», яку можуть застосовувати ворожі структури. Квантово-захищені канали дозволяють мережам мобільного

зв’язку гарантувати, що дані, передані сьогодні, не зможуть бути розкриті навіть через десятиліття. Це критично для державних установ, оборонної сфери, медицини, фінансового сектору та всіх сервісів, де інформація має довгий строк зберігання або високу стратегічну цінність.

Квантизація захисту також підвищує загальну стійкість мережевої інфраструктури. Включення квантових ключових менеджерів у ядро мережі або використання QKD у Backhaul і транспортних сегментах суттєво ускладнює проведення кібератак на канали управління, сигнальні інтерфейси та критично важливі внутрішні протоколи. Це робить неможливим перехоплення трафіку між опорними вузлами, підміну конфігурацій, атаки типу Man-in-the-Middle чи компрометацію механізмів аутентифікації, які в класичних системах можуть стати слабким місцем.

Ще одним суттєвим ефектом є підвищення довіри до хмарних сервісів і OSS/BSS-платформ. Оскільки в таких системах зберігаються великі обсяги персональних даних, білінгова інформація, логи, конфігурації та аналітика мережі, забезпечення квантового рівня захисту дозволяє операторам гарантувати безпеку даних протягом усього терміну їх зберігання. Перехід на постквантові алгоритми у поєднанні з квантовим розподілом ключів створює багаторівневий гібридний захист, який знижує ризики внутрішнього шахрайства, витоків або компрометації при атаках на хмарну інфраструктуру.

Квантові технології також позитивно впливають на архітектуру мобільних мереж нового покоління. Інтеграція квантово-захищених сервісів у MEC/Edge дозволяє забезпечувати безпечну обробку трафіку максимально близько до користувача, зменшуючи затримки й усуваючи ризики, що виникають при перенаправленні даних у центральні дата-центри. Це особливо важливо для критичних застосувань — автономного транспорту, телемедицини, промислової автоматизації, військових комунікацій — де навіть невелика вразливість у каналі може призвести до серйозних наслідків. Квантовий захист на рівні Edge-сервісів робить такі системи більш надійними та передбачуваними.

У великих інфраструктурах додатковою перевагою стає можливість побудови «квантових зон довіри» між вузлами мобільної мережі різних операторів або регіонів. Це відкриває шлях до створення захищених транскордонних мереж, у яких взаємодія 5G/6G-сегментів відбувається з гарантованим рівнем безпеки, незалежно від політики чи потенційної вразливості будь-якої окремої мережевої складової.

Ще один важливий ефект — підвищення надійності інтелектуальних функцій мережі. Оскільки 6G значною мірою буде використовувати ШІ для управління трафіком, частотним ресурсом, енергоспоживанням і безпекою, захист моделей та даних, що тренують ці моделі, стає критичним. Квантово-

захищені канали та постквантова криптографія забезпечують цілісність інтелектуальних систем, не допускаючи їх підміни або маніпуляції під час передачі між елементами мережі.

Зрештою, застосування квантових технологій створює стратегічну перевагу оператора. Впровадження квантових рішень підвищує конкурентоспроможність, дає можливість надавати послуги з підвищеним рівнем безпеки (secure slicing, quantum-safe private networks), підвищує довіру бізнес-клієнтів і державних структур, а також забезпечує довгостроковий технологічний запас із врахуванням появи квантових комп'ютерів та нових типів кібератак.

2.5 Основні категорії кіберзагроз, пов'язані з квантовими технологіями

Поява квантових технологій формує новий клас кіберзагроз, які мають потенціал суттєво змінити підходи до захисту мобільних мереж та зруйнувати традиційні моделі криптографічної безпеки. На відміну від класичних атак, що ґрунтуються на обмежених обчислювальних ресурсах і передбачуваних моделях зловмисників, квантові загрози характеризуються здатністю використовувати специфічні фізичні властивості квантових систем — суперпозицію, заплутаність та квантове тунелювання — що відкриває можливості для здійснення атак, недоступних у класичних середовищах. Найбільша небезпека полягає у тому, що квантові технології порушують фундаментальні принципи сучасної криптографії, на яких побудована безпека всіх мобільних поколінь від 2G до 5G і закладаються основи для 6G.

Першою і найбільш критичною категорією загроз є руйнування криптографічних алгоритмів, що базуються на складності математичних задач. Квантові алгоритми, такі як алгоритм Шора, здатні за реалістичних умов зламувати протоколи з відкритим ключем, включаючи RSA, DSA, ECDSA та більшість варіантів еліптичних кривих. Оскільки усі мобільні стандарти від 3G до 5G використовують ці схеми для автентифікації, узгодження ключів, шифрування і захисту сигнального трафіку, компрометація криптографії призведе до повного зняття захисту в мережах. Ця загроза носить відкладений характер: дані, які перехоплюються вже сьогодні («збирай зараз — розшифруєш пізніше»), можуть бути розкриті у момент, коли квантові комп'ютери досягнуть достатньої продуктивності.

Друга категорія загроз пов'язана з компрометацією каналів зв'язку через атаки, що використовують квантові ефекти. Класичні протоколи передавання,

включно з IP, LTE EPC, 5G SBA та міжоператорськими інтерфейсами, не передбачають захисту від квантових атак на математичні властивості генераторів випадкових чисел або ключових угод. Квантові технології дозволяють створювати прилади для надточного вимірювання слабких сигналів, що дає змогу зловмисникам здійснювати більш ефективне пасивне прослуховування, навіть якщо канал зашифрований. Наявність високочутливих квантових сенсорів може підвищити ризик перехоплення сигнального трафіку, маніпуляції радіочастотами, підміни базових станцій чи порушення стійкості синхронізації мережі.

Третьою категорією загроз є небезпеки, пов'язані з помилками квантових систем та їх вразливістю до фізичних впливів. Квантові обчислювальні системи є нестабільними, чутливими до шумів та температурних змін, що створює ризик маніпуляцій через фізичні впливи або атаки на побічні канали. Це особливо важливо для майбутніх мереж 6G, де передбачається використання квантових сенсорів, квантових прискорювачів ШІ та елементів квантової криптографії. Атаки на ці компоненти можуть призвести не лише до витоку даних, а й до повної дестабілізації мережевої інфраструктури, збоїв у системах локалізації, синхронізації часу або порушення роботи нейромереж, що керують ресурсами радіодоступу.

Четверта категорія загроз стосується можливості використання квантових технологій для проведення розширених атак на штучний інтелект та автономні механізми, інтегровані у 5G та особливо 6G. У майбутніх мережах ШІ керуватиме маршрутизацією, розподілом спектра, оптимізацією трафіку, прогнозуванням навантаження, виявленням аномалій та безпекою. Квантові моделі машинного навчання здатні обходити класичні алгоритми виявлення вторгнень, створювати високоточні фальсифіковані дані навчання або впливати на сам процес оптимізації систем зв'язку, що може призвести до порушення стабільності мобільних мереж чи маніпуляцій у роботі базових станцій.

П'ята категорія загроз пов'язана з тим, що квантова криптографія, попри високий рівень теоретичної безпеки, має реальні технічні вразливості. Квантові канали можуть бути атаковані через маніпуляції фотонними імпульсами, «темні» імпульси, переповнення детекторів, зниження енергії сигналів або введення шуму. Оскільки у 6G передбачається широке впровадження QKD для захисту міжоператорських інтерфейсів та хмар інфраструктури, наявність слабких місць у квантових системах може створити ілюзію безпеки, водночас залишаючи мережу відкритою для цілеспрямованих атак.

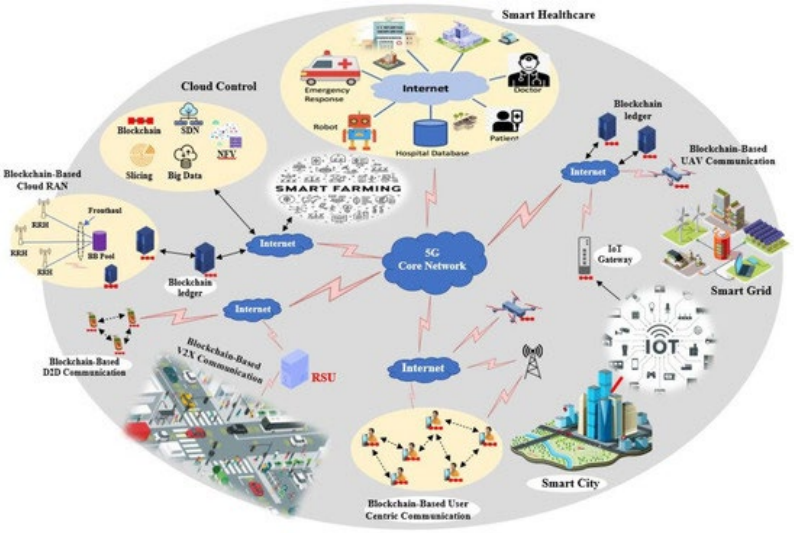
Остання фундаментальна категорія загроз полягає у глобальних геополітичних та технологічних ризиках, пов'язаних із контролем над квантовими обчислювальними ресурсами. Держава або організація, яка отримає

перші функціональні універсальні квантові комп’ютери, матиме можливість отримувати доступ до зашифрованих мобільних систем у світовому масштабі. Це створює ризик асиметричного контролю, коли мобільні мережі різних країн можуть бути приховано скомпрометовані без можливості виявлення факту атаки.

У сукупності ці категорії формують комплексний набір квантових кіберзагроз, які є значно ширшими за звичайні атаки на криптографію. Вони впливають на всі аспекти мобільних мереж — від радіодоступу до хмарної архітектури, від криптопротоколів до ШІ-керування, від сигнальних систем до глобальної міжоператорської взаємодії. Саме тому забезпечення стійкості мобільних мереж до квантових загроз стає ключовою передумовою розвитку 5G-Advanced і критично необхідною умовою для безпечного впровадження 6G.

3. Аналіз сучасних кіберзагроз мобільного зв’язку в умовах розвитку квантових технологій

Аналіз сучасних кіберзагроз мобільного зв’язку в умовах розвитку квантових технологій показує, що характер атак змінюється не стільки за формою, скільки за масштабом наслідків і довгостроковими ризиками. Якщо раніше більшість загроз були обмежені конкретними уразливостями протоколів або обладнання, то з урахуванням квантових технологій з’являється системний ризик для всієї архітектури мобільних мереж — від радіодоступу до OSS/BSS і хмарних сервісів



Кіберзагрози мереж мобільного зв’язку третього покоління (3G)

Мережі третього покоління мобільного зв’язку стали важливим етапом еволюції телекомунікацій, оскільки саме з їх впровадженням мобільний зв’язок трансформувався з голосоорієнтованої технології у повноцінну платформу для передавання даних і доступу до Інтернету. Стандарти UMTS та HSPA забезпечили підвищену швидкість передавання інформації та впровадили низку механізмів безпеки, зокрема взаємну автентифікацію між абонентом і мережею та покращені алгоритми шифрування. Проте, незважаючи на ці досягнення, 3G-мережі мають низку вразливостей, які формують характерний для цього покоління спектр кіберзагроз.

Однією з основних загроз для мереж 3G є атаки на сигнальні протоколи та міжоператорську взаємодію. Недостатній рівень захисту сигнального обміну між операторами створює можливості для несанкціонованого доступу до інформації про абонентів, зокрема даних про місцеперебування, маршрути викликів і параметри сесій. Такі атаки можуть використовуватися для прихованого стеження, порушення конфіденційності або підготовки більш складних цільових атак.

Істотною проблемою безпеки 3G залишається можливість використання фальшивих базових станцій. У певних сценаріях абонентські пристрої можуть бути змушені підключатися до зловмисної інфраструктури, що дозволяє реалізовувати атаки типу «людина посередині», перехоплювати трафік або примусово знижувати рівень шифрування. Додатковим фактором ризику є велика кількість застарілих 3G-пристроїв, які не отримують оновлень безпеки та містять відомі вразливості програмного забезпечення. Механізми зворотної сумісності з попередніми поколіннями ще більше посилюють ці загрози, знижуючи загальний рівень захищеності мобільного зв’язку.

Кіберзагрози мереж мобільного зв’язку четвертого покоління (4G)

Четверте покоління мобільного зв’язку, представлене стандартом LTE, ознаменувало перехід до повністю пакетної IP-архітектури. Це забезпечило значний приріст пропускної здатності, гнучкості та масштабованості мереж, але водночас призвело до перенесення в мобільний зв’язок широкого спектра загроз, характерних для класичних комп’ютерних мереж. Таким чином, кіберзагрози 4G мають змішаний характер, поєднуючи телекомунікаційні та IT-вразливості.

Однією з ключових загроз для 4G-мереж є атаки на сигнальний протокол Diameter, який використовується для автентифікації, авторизації, тарифікації та управління мобільністю. Недостатній рівень захисту міжоператорських з’єднань дозволяє зловмисникам здійснювати атаки на конфіденційність і доступність

сервісів, включаючи перехоплення сигнальної інформації та маніпуляцію параметрами сесій.

Суттєвим викликом безпеки в 4G є атаки на ідентифікацію абонентів, зокрема атаки типу SIM-swap. Такі атаки активно використовуються для компрометації облікових записів користувачів у фінансових і цифрових сервісах, оскільки мобільна мережа часто є основним каналом двофакторної автентифікації. Крім того, у 4G залишаються актуальними загрози, пов’язані з тимчасовим розкриттям ідентифікаторів абонентів і можливістю пасивного радіоперехоплення.

Віртуалізація мережевих функцій, що активно впроваджувалася в 4G, відкрила нові вектори атак на серверну інфраструктуру, операційні системи, платформи віртуалізації та системи оркестрації. Компрометація цих компонентів може мати масштабні наслідки, включаючи порушення стабільності роботи мережі на регіональному або навіть національному рівні.

Кіберзагрози мереж мобільного зв’язку п’ятого покоління (5G)

П’яте покоління мобільного зв’язку характеризується подальшим ускладненням архітектури та розширенням функціональних можливостей мережі. Концепції сегментації мережі, крайових обчислень і масового підключення пристроїв Інтернету речей дозволяють створювати гнучкі та високопродуктивні сервіси, але водночас формують принципово нові кіберзагрози. Незважаючи на найвищий на сьогодні рівень вбудованої безпеки, 5G залишається вразливою до складних багаторівневих атак.

Однією з ключових загроз для 5G є порушення ізоляції між логічними сегментами мережі. У разі помилок конфігурації або вразливостей програмного забезпечення атака на один сегмент може поширюватися на інші, включаючи критично важливі сервіси з підвищеними вимогами до надійності та безпеки. Крайові обчислення, що забезпечують мінімальну затримку та високу продуктивність, водночас збільшують кількість точок доступу до інфраструктури та підвищують ризик фізичних і комбінованих атак.

Масове впровадження IoT-пристроїв у мережах 5G створює одну з найбільш серйозних сучасних проблем кібербезпеки. Значна частина таких пристроїв має обмежені обчислювальні ресурси та спрощені механізми захисту, що робить їх привабливою ціллю для зловмисників. Компрометовані IoT-пристрої можуть використовуватися для організації розподілених атак на доступність мережі або як початкові точки проникнення в інші сегменти інфраструктури.

Окремим виміром загроз для 5G є довгострокові ризики, пов’язані з розвитком квантових обчислень. Дані, передані в мережах п’ятого покоління,

можуть бути перехоплені та збережені з метою подальшого розшифрування в майбутньому, що створює виклики для забезпечення довготривалої конфіденційності інформації. Таким чином, аналіз кіберзагроз 5G свідчить про необхідність переходу до квантово-стійких підходів до безпеки в мережах наступних поколінь.

Однією з найчастіших і найнебезпечніших ситуацій є перехоплення та накопичення зашифрованого трафіку з розрахунком на майбутній квантовий злам. У сучасних мережах 4G/5G більшість захищених з'єднань у RAN, backhaul, core та хмарних платформах використовують RSA, ECC або Diffie-Hellman для обміну ключами. Навіть якщо сьогодні ці алгоритми вважаються безпечними, зловмисники можуть масово записувати сигнальний і користувацький трафік, щоб у майбутньому, після появи потужних квантових комп'ютерів, розшифрувати його заднім числом. Це особливо критично для OSS/BSS, білінгових систем, історії місцезнаходження абонентів, державних комунікацій і промислових IoT-систем, де дані мають цінність протягом багатьох років.

Дуже поширеною залишається загроза компрометації сигнальних протоколів і каналів управління, але в квантовому контексті вона стає значно небезпечнішою. Протоколи на кшталт SS7, Diameter, HTTP/2 API в SBA-ядрі або PFCP між core і UPF вже сьогодні є привабливою ціллю для атак. Якщо квантові обчислення дозволять зламувати ключі автентифікації, зловмисник отримає можливість не просто підслуховувати, а повністю контролювати сигнальні процеси: перенаправляти трафік, змінювати політики безпеки, втручатися в механізми network slicing або відключати критичні сервіси. У 6G, де більшість управління буде автоматизована через AI, така атака може мати каскадний ефект на всю мережу.

Ще одна типова ситуація — атаки на радіодоступ у поєднанні з криптографічною деградацією. Downgrade-атаки, IMSI-catchers і фальшиві базові станції вже зараз використовуються для примусового переходу абонента на слабші алгоритми захисту або старі стандарти. У квантовому майбутньому навіть короткочасний перехід на класичні схеми шифрування означає, що зафіксований трафік можна буде розкрити пізніше. Це робить атаки на RAN не просто інструментом стеження в реальному часі, а способом збирання даних для довготривалого аналізу.

Критичною загрозою стають атаки на backhaul і транспортні мережі. Саме тут концентрується трафік від тисяч базових станцій, MEC-вузлів і core-функцій. Перехоплення оптичних ліній, компрометація маршрутизаторів або маніпуляції з MPLS/Segment Routing дозволяють зловмиснику отримати доступ до зашифрованих потоків управління та даних. У квантовому контексті навіть пасивне прослуховування транспортних каналів стає небезпечним, оскільки

накопичені дані можуть бути розшифровані в майбутньому. Це одна з причин, чому backhaul розглядається як пріоритетна зона для впровадження PQC і QKD.

Окрему групу сучасних загроз становлять атаки на MEC і edge-інфраструктуру. Оскільки edge-вузли розміщуються ближче до користувачів і часто мають менший фізичний та логічний захист, вони стають зручними точками для проникнення. Компрометація MEC може дозволити атакувати локальні AI-сервіси, підміняти дані для машинного навчання, втручатися в управління beamforming або порушувати роботу критичних додатків з низькою затримкою. Якщо такі вузли використовують класичну криптографію, їхній трафік і ключі також потрапляють під квантову загрозу.

Особливо актуальною стає проблема атак на системи штучного інтелекту, які дедалі глибше інтегруються в 5G і 6G. Model poisoning, data poisoning, adversarial attacks і AI-as-a-Target у поєднанні з криптографічною слабкістю можуть призвести до того, що зловмисник не лише отримає доступ до моделей, а й зможе змінювати логіку управління мережею. У квантовому сценарії перехоплення й розшифрування оновлень моделей або навчальних даних дозволить атакувати мережу системно, впливаючи на її поведінку протягом тривалого часу.

Не менш поширеною є загроза для OSS/BSS та хмарних платформ. Саме тут зберігаються історичні дані, журнали, фінансова інформація, персональні профілі абонентів і телеметрія мережі. Якщо ці дані зашифровані класичними алгоритмами, квантові комп’ютери в майбутньому можуть відкрити доступ до архівів за десятки років. Це створює серйозні ризики не лише для безпеки, а й для дотримання законодавства, конфіденційності та довіри до операторів.

У підсумку, найчастіші кіберзагрози мобільного зв’язку в умовах розвитку квантових технологій пов’язані не з появою абсолютно нових типів атак, а з радикальним посиленням уже відомих сценаріїв. Перехоплення трафіку, компрометація сигнальних протоколів, атаки на RAN, backhaul, MEC, AI-системи та OSS/BSS у квантовому контексті перетворюються на довгострокову загрозу для всієї екосистеми мобільного зв’язку. Саме тому перехід до постквантової криптографії, гібридних схем захисту та квантових технологій безпеки стає не опцією, а необхідністю для майбутніх 5G і 6G мереж.

3.3 Порівняльний аналіз постквантової криптографії (PQC) та квантового розподілу ключів (QKD) в системах мобільного зв’язку

Стрімкий розвиток квантових технологій створює принципово нові виклики для систем інформаційної безпеки, зокрема для мереж мобільного зв’язку, які є основою сучасного цифрового суспільства. Очікуване зростання обчислювальних можливостей квантових комп’ютерів ставить під загрозу більшість традиційних криптографічних алгоритмів, що використовуються для захисту даних у мережах від другого до п’ятого покоління. У цьому контексті особливої уваги набувають два ключові підходи до забезпечення безпеки в квантову епоху: постквантова криптографія (Post-Quantum Cryptography, PQC) та квантовий розподіл ключів (Quantum Key Distribution, QKD).

Постквантова криптографія являє собою сукупність криптографічних алгоритмів, які розробляються з урахуванням можливостей як класичних, так і квантових комп’ютерів. Основна ідея PQC полягає у створенні таких математичних задач, які залишаються обчислювально складними навіть для квантових алгоритмів, зокрема алгоритму Шора та алгоритму Гровера. На відміну від класичної криптографії з відкритим ключем, що базується на факторизації великих чисел або обчисленні дискретного логарифма, постквантові алгоритми використовують інші математичні конструкції, такі як ґратки, коди з виправленням помилок, багатовимірні поліноміальні системи та хеш-функції.

Однією з головних переваг PQC є її сумісність з існуючою інфраструктурою мобільних мереж. Постквантові алгоритми можуть бути реалізовані програмно та інтегровані в існуючі протоколи зв’язку без необхідності кардинальних змін фізичного рівня мережі. Це робить PQC особливо привабливою для практичного впровадження в мережах 4G, 5G та перспективних 6G, де масштабованість і зворотна сумісність мають критичне значення. Крім того, PQC дозволяє забезпечити захист як нових, так і архівних даних, що є важливим у контексті загрози типу «збирай зараз – розшифровуй пізніше».

Водночас постквантова криптографія має низку обмежень. Основним із них є те, що її стійкість базується на припущеннях щодо складності математичних задач, які ще не мають абсолютного доведення. Існує ймовірність того, що в майбутньому будуть знайдені нові квантові алгоритми, здатні знизити рівень стійкості навіть постквантових схем. Крім того, багато PQC-алгоритмів характеризуються значно більшими розмірами ключів і підписів, що створює додаткове навантаження на канали зв’язку та обчислювальні ресурси мобільних пристроїв, особливо в умовах масових IoT-мереж і M2M-комунікацій.

На відміну від постквантової криптографії, квантовий розподіл ключів базується не на математичних припущеннях, а на фундаментальних законах квантової фізики. Основний принцип QKD полягає в тому, що будь-яка спроба перехоплення квантового стану неминуче змінює його параметри, що дозволяє легітимним сторонам виявити факт втручання. Таким чином, QKD забезпечує інформаційно-теоретичну безпеку, яка вважається абсолютною і не залежить від обчислювальних можливостей зловмисника.

Квантовий розподіл ключів відкриває нові перспективи для захисту критично важливих сегментів мобільних мереж, таких як магістральні канали зв'язку між базовими станціями, ядром мережі та дата-центрами операторів. У таких сценаріях QKD може використовуватися для безпечного обміну криптографічними ключами, які надалі застосовуються в симетричних алгоритмах шифрування. Особливо актуальним це стає в умовах майбутніх мереж 6G, де очікується інтеграція супутникових, наземних і повітряних сегментів зв'язку.

Проте практичне впровадження QKD супроводжується значними технічними та економічними труднощами. По-перше, квантовий розподіл ключів вимагає спеціалізованого фізичного обладнання, включаючи джерела одиничних фотонів, детектори та квантові канали зв'язку, які є чутливими до втрат і шумів. По-друге, дальність дії QKD обмежена фізичними властивостями оптоволоконних або атмосферних каналів, що ускладнює його застосування в масштабних мобільних мережах з мільйонами абонентів. По-третє, QKD не вирішує проблему аутентифікації сам по собі, а отже потребує поєднання з класичними або постквантовими методами захисту.

Порівнюючи PQC і QKD з точки зору застосування в мобільних мережах, слід зазначити, що ці підходи не є взаємовиключними, а радше взаємодоповнюючими. Постквантова криптографія забезпечує гнучке та масштабоване рішення для масових користувачів, мобільних пристроїв і IoT-систем, тоді як квантовий розподіл ключів доцільно використовувати для захисту критичних каналів з високими вимогами до безпеки. Такий гібридний підхід дозволяє поєднати переваги обох технологій і мінімізувати їхні недоліки.

У контексті кіберзагроз особливу увагу слід приділити тому, що впровадження квантових технологій саме по собі створює нові вектори атак. Для PQC це можуть бути вразливості реалізації, побічні канали, помилки в параметризації алгоритмів та проблеми сумісності з існуючими протоколами. Для QKD основними загрозами є атаки на апаратне забезпечення, маніпуляції з детекторами фотонів, а також компрометація класичного каналу управління. Таким чином, навіть технології, які позиціонуються як «квантово-стійкі», потребують комплексного підходу до безпеки.

Загалом, аналіз показує, що в умовах переходу до мереж шостого покоління та подальшої цифровізації суспільства жоден із підходів не може вважатися універсальним рішенням. Постквантова криптографія є найбільш реалістичним і економічно доцільним варіантом для масового впровадження в мобільних мережах у найближчі десятиліття. Водночас квантовий розподіл ключів має значний потенціал у сфері захисту критичної інфраструктури та стратегічних комунікацій.

Отже, стратегія забезпечення безпеки мобільного зв'язку в квантову епоху повинна ґрунтуватися на поєднанні постквантових криптографічних алгоритмів, квантових методів розподілу ключів та класичних механізмів захисту, доповнених сучасними засобами моніторингу, штучного інтелекту та управління ризиками. Такий підхід дозволить забезпечити довгострокову конфіденційність, цілісність і доступність інформації в умовах постійно зростаючих кіберзагроз.

3.4 АНАЛІЗ МОДЕЛЕЙ ЗАГРОЗ ДЛЯ МАЙБУТНІХ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ 6G

Шосте покоління мобільного зв'язку (6G), яке наразі перебуває на етапі активних наукових досліджень і концептуального проєктування, розглядається як фундаментальна технологічна платформа для цифрового суспільства майбутнього. На відміну від попередніх поколінь, 6G орієнтований не лише на підвищення швидкості передавання даних, а й на глибоку інтеграцію комунікаційних, обчислювальних та інтелектуальних можливостей мережі. Очікується, що 6G забезпечить терабітні швидкості, наднизьку затримку на рівні мікросекунд, повну підтримку масових кіберфізичних систем, тактильного інтернету, автономних транспортних систем, розширеної та доповненої реальності, а також критично важливих сервісів державного й промислового рівня. Водночас така глибока цифровізація та ускладнення архітектури мережі призводять до якісно нового рівня кіберзагроз, що потребує ґрунтовного аналізу моделей загроз саме для 6G.

Модель загроз для мереж 6G формується під впливом кількох взаємопов'язаних чинників: радикального зростання кількості підключених пристроїв, переходу до програмно визначених і віртуалізованих мереж, широкого використання штучного інтелекту, інтеграції наземних, повітряних і космічних сегментів зв'язку, а також появи квантових обчислювальних технологій. У сукупності ці фактори створюють надзвичайно складне та динамічне середовище, у якому традиційні підходи до аналізу загроз і побудови систем захисту стають недостатніми. Мережа 6G перестає бути лише телекомунікаційною інфраструктурою і трансформується в універсальну цифрову екосистему, що обслуговує фізичний світ у реальному часі.

Однією з ключових особливостей моделей загроз для 6G є суттєве розширення поверхні атаки. Якщо у попередніх поколіннях мобільного зв'язку основними об'єктами атак були базові станції, ядро мережі та абонентські пристрої, то у 6G до них додаються віртуалізовані функції мережі, хмарні та крайові обчислювальні платформи, алгоритми штучного інтелекту, цифрові двійники, сенсорні мережі та елементи інфраструктури Інтернету речей. Кожен із цих компонентів може стати окремою точкою входу для зловмисника, а взаємозв'язки між ними значно ускладнюють виявлення та локалізацію атак.

Особливу роль у моделях загроз 6G відіграє програмно визначена природа мережі. У 6G більшість функцій реалізується у вигляді програмних модулів, які динамічно розгортаються у хмарному або крайовому середовищі. Це підвищує гнучкість і масштабованість мережі, але водночас створює ризики, пов'язані з компрометацією програмного забезпечення, ланцюгів постачання, механізмів оркестрації та автоматичного керування. Атаки на системи управління можуть призвести до повного контролю над мережевими ресурсами, порушення роботи критичних сервісів або прихованої модифікації логіки функціонування мережі.

Інтеграція штучного інтелекту в усі рівні архітектури 6G формує новий клас загроз, пов'язаних із впливом на алгоритми машинного навчання. У 6G штучний інтелект використовується для оптимізації радіоресурсів, маршрутизації трафіку, керування мобільністю, забезпечення якості обслуговування та виявлення аномалій безпеки. У цьому контексті зловмисник може цілеспрямовано атакувати навчальні дані, моделі або процес прийняття рішень, що призводить до помилкових або шкідливих дій мережі. Такі атаки є особливо небезпечними, оскільки вони можуть залишатися непоміченими тривалий час і мати кумулятивний ефект.

Ще одним критично важливим аспектом моделей загроз для 6G є злиття цифрового та фізичного світів. Мережі 6G забезпечуватимуть зв'язок для автономних транспортних засобів, промислових роботів, медичних систем, енергетичної інфраструктури та інших кіберфізичних об'єктів. У таких умовах кібератаки можуть мати безпосередні фізичні наслідки, включаючи пошкодження обладнання, загрозу життю людей або масштабні техногенні аварії. Модель загроз 6G повинна враховувати не лише інформаційну безпеку, а й функціональну безпеку та стійкість систем до навмисних впливів.

Важливе місце в аналізі загроз 6G посідає фактор квантових технологій. Очікується, що в період розгортання 6G квантові комп'ютери досягнуть рівня, достатнього для практичного зламу класичних криптографічних алгоритмів, які використовуються для захисту мобільних мереж. Це означає, що моделі загроз для 6G повинні враховувати сценарії компрометації шифрування, автентифікації та цілісності даних за допомогою квантових атак. Особливо небезпечними є так

звані атаки типу «зберегти зараз — розшифрувати пізніше», коли зашифрований трафік накопичується з метою його розкриття в майбутньому.

У контексті 6G загрози конфіденційності набувають нового виміру. Надвисока точність позиціонування, масовий збір сенсорних даних і використання цифрових двійників призводять до формування детальних профілів користувачів, об'єктів і процесів. Компрометація таких даних може використовуватися не лише для фінансових або шпигунських цілей, а й для маніпуляції поведінкою, соціального інжинірингу та дестабілізації суспільних процесів. Модель загроз 6G повинна враховувати ризики системного порушення приватності на глобальному рівні.

Додаткову складність становить гетерогенність архітектури 6G, яка поєднуватиме наземні мережі, безпілотні платформи, супутникові системи та підводні канали зв'язку. Така багаторівнева структура створює нові вектори атак, пов'язані з перехопленням сигналів, підміною вузлів, атаками на синхронізацію та порушенням узгодженої роботи різних сегментів мережі. У моделі загроз необхідно враховувати можливість комбінованих атак, що одночасно впливають на кілька рівнів інфраструктури.

Суттєвим елементом моделей загроз для 6G є також людський фактор. Зі зростанням складності мереж і автоматизації процесів управління зростає ризик помилок конфігурації, зловживання привілеями та соціальної інженерії. Навіть за наявності передових технічних засобів захисту, компрометація облікових даних або неправомірні дії персоналу можуть призвести до серйозних інцидентів безпеки.

Узагальнюючи, можна стверджувати, що моделі загроз для мереж 6G мають системний, міждисциплінарний характер і виходять далеко за межі класичної телекомунікаційної безпеки. Вони повинні охоплювати технічні, організаційні, криптографічні, квантові та соціальні аспекти, а також враховувати взаємодію цифрових і фізичних процесів. Саме комплексний підхід до аналізу загроз є ключовою умовою створення стійких, безпечних і надійних мереж шостого покоління, здатних забезпечити функціонування критично важливих сервісів у майбутньому інформаційному суспільстві.

3.5 Оптимізаційні підходи кібербезпеки мобільних мереж в умовах розвитку кіберзагроз і квантових технологій

Стрімкий розвиток мобільних мереж зв'язку, що еволюціонували від простих аналогових систем до інтелектуальних кіберфізичних платформ, супроводжується суттєвим зростанням складності їхньої архітектури та

розширенням поверхні атак. Умови сучасного цифрового середовища, зокрема масова цифровізація, інтеграція хмарних сервісів, програмно-визначених мереж (SDN), віртуалізація мережевих функцій (NFV), а також поява квантових технологій, вимагають перегляду традиційних підходів до забезпечення кібербезпеки мобільного зв'язку. Оптимізація кібербезпеки в цьому контексті має комплексний характер і передбачає одночасне підвищення рівня захищеності, продуктивності, надійності та адаптивності мереж.

Одним із ключових напрямів оптимізації кібербезпеки мобільних мереж є перехід від статичних моделей захисту до динамічних, контекстно-орієнтованих підходів. У мережах попередніх поколінь безпека базувалася переважно на фіксованих криптографічних алгоритмах і периметровому захисті. Проте в умовах 5G і перспективних 6G-мереж така модель стає неефективною через децентралізовану архітектуру, високу мобільність користувачів та велику кількість гетерогенних пристроїв. Оптимізація безпеки вимагає впровадження принципів Zero Trust, за яких жоден елемент мережі не вважається апріорі довіреним, а кожна взаємодія підлягає постійній перевірці та автентифікації.

Важливим оптимізаційним підходом є використання інтелектуальних систем виявлення та реагування на загрози. Зростання обсягів мережевого трафіку та складність атак унеможливлюють ефективне використання виключно традиційних засобів моніторингу. Застосування методів машинного навчання та штучного інтелекту дозволяє аналізувати поведінкові характеристики мережі в реальному часі, виявляти аномалії та прогнозувати потенційні атаки. Оптимізація полягає в адаптації алгоритмів аналізу до специфіки мобільних мереж, зокрема з урахуванням змінних умов радіосередовища, мобільності користувачів та динамічного масштабування ресурсів.

З огляду на розвиток квантових технологій, окремого значення набуває оптимізація криптографічного захисту. Класичні алгоритми асиметричного шифрування, які широко застосовуються в сучасних мобільних мережах, є потенційно вразливими до атак із використанням квантових комп'ютерів. У цьому контексті оптимізаційний підхід полягає у поетапному впровадженні постквантової криптографії (PQC), яка базується на математичних задачах, стійких до квантових обчислень. Важливою складовою оптимізації є забезпечення зворотної сумісності PQC-алгоритмів із чинною інфраструктурою мобільного зв'язку без істотного зниження продуктивності мережі.

Паралельно з PQC перспективним напрямом оптимізації кібербезпеки є інтеграція квантового розподілу ключів (QKD) у критично важливі сегменти мобільних мереж. Хоча QKD не є універсальним рішенням через обмеження дальності та складність реалізації, його використання у магістральних каналах зв'язку та міжцентрових з'єднаннях дозволяє досягти принципово нового рівня

захисту даних. Оптимізація полягає у комбінованому використанні QKD та класичних або постквантових криптографічних методів, що забезпечує баланс між безпекою, вартістю та масштабованістю.

Ще одним важливим напрямом оптимізації кібербезпеки є сегментація та ізоляція мережевих ресурсів. У мережах 5G і 6G активно застосовується технологія network slicing, яка дозволяє створювати віртуальні логічні мережі з різними вимогами до якості обслуговування та безпеки. Оптимізація кіберзахисту полягає у впровадженні індивідуальних політик безпеки для кожного сегмента мережі, що знижує ризик поширення атак та мінімізує наслідки компрометації окремих елементів.

Особливу увагу слід приділити оптимізації захисту периферійних обчислень (edge computing), які є невід'ємною складовою сучасних і майбутніх мобільних мереж. Перенесення обробки даних ближче до користувача зменшує затримки, але водночас створює нові вектори атак. Оптимізаційний підхід полягає у впровадженні локальних механізмів безпеки, апаратних коренів довіри та постійного контролю цілісності програмного забезпечення на edge-вузлах.

Не менш важливою складовою оптимізації є управління ризиками та кіберстійкістю мереж. Замість фокусування виключно на запобіганні атакам сучасні підходи передбачають здатність мережі швидко відновлюватися після інцидентів без суттєвих втрат функціональності. Це досягається шляхом резервування ресурсів, автоматизованого відновлення мережевих функцій та використання розподілених архітектур.

У контексті 6G оптимізація кібербезпеки набуває міждисциплінарного характеру, поєднуючи телекомунікації, кібербезпеку, штучний інтелект та квантову фізику. Висока щільність підключень, автономні системи, інтеграція сенсорних мереж і використання штучного інтелекту для управління мережею потребують принципово нових підходів до захисту. Оптимізація в цьому випадку полягає у створенні самонавчальних, самозахисних мереж, здатних адаптуватися до нових загроз у реальному часі.

Таким чином, оптимізаційні підходи кібербезпеки мобільних мереж в умовах розвитку кіберзагроз і квантових технологій мають комплексний і багаторівневий характер. Вони охоплюють архітектурні рішення, криптографічні механізми, інтелектуальні системи аналізу загроз та принципи кіберстійкості. Реалізація таких підходів є ключовою умовою забезпечення надійного та безпечного функціонування мобільного зв'язку в сучасному та майбутньому цифровому середовищі.

3.6 Аналіз Моделей Загроз Для Мереж 6g

Архітектура безпечної мережі мобільного зв’язку шостого покоління розглядається як комплексна, багаторівнева та інтелектуально керована система, яка поєднує комунікаційні, обчислювальні та захисні механізми в єдину інтегровану інфраструктуру. На відміну від попередніх поколінь, де безпека здебільшого реалізовувалася як додатковий функціональний шар, у 6G безпека закладається безпосередньо в основу архітектури, стаючи її невід’ємною властивістю. Такий підхід зумовлений критичною роллю 6G у підтримці кіберфізичних систем, автономних рішень, тактильного інтернету та сервісів, від яких безпосередньо залежать життя людей, стабільність економіки та національна безпека.

Базовою особливістю архітектури безпечної 6G-мережі є її повна віртуалізація та програмна визначеність. Усі ключові функції мережі, включно з радіодоступом, маршрутизацією, управлінням сесіями, автентифікацією та контролем доступу, реалізуються у вигляді програмних модулів, що розгортаються в хмарному або крайовому середовищі. Це дозволяє динамічно адаптувати конфігурацію мережі до поточних умов, рівня загроз і вимог сервісів. Водночас така гнучкість потребує розвинених механізмів захисту програмного середовища, включаючи перевірку цілісності коду, контроль ланцюгів постачання та ізоляцію виконання функцій.

Радіодоступ у безпечній 6G-мережі базується на використанні надвисокочастотних діапазонів, включаючи терагерцові хвилі, що забезпечують надзвичайно високу пропускну здатність і точність позиціонування. З точки зору безпеки це створює як нові можливості, так і нові загрози. З одного боку, вузькоспрямовані промені ускладнюють пасивне перехоплення сигналів, з іншого — висока складність радіосередовища потребує інтелектуальних механізмів захисту від активних атак, таких як підміна базових станцій, глушіння сигналу або маніпуляція параметрами каналу. У безпечній архітектурі 6G ці задачі вирішуються за рахунок тісної інтеграції радіорівня з системами штучного інтелекту.

Центральним елементом архітектури безпечної 6G-мережі є інтелектуальний рівень управління, який використовує алгоритми машинного навчання для моніторингу стану мережі, аналізу трафіку та виявлення аномалій. На відміну від традиційних систем безпеки, що працюють за заздалегідь визначеними правилами, 6G-архітектура здатна навчатися на основі реальних даних і адаптувати свої захисні стратегії в режимі реального часу. Це дозволяє виявляти складні багатовекторні атаки, які неможливо ідентифікувати класичними методами.

Крайові обчислення відіграють ключову роль у забезпеченні безпеки 6G-мережі. Перенесення обчислювальних ресурсів ближче до користувача зменшує затримку та підвищує стійкість системи до відмов, але водночас розширює поверхню атаки. У безпечній архітектурі 6G крайові вузли оснащуються апаратними модулями довіри, засобами захищеного завантаження та механізмами ізоляції виконання. Це дозволяє гарантувати, що навіть у разі часткової компрометації інфраструктури критичні функції залишатимуться захищеними.

Особлива увага в архітектурі безпечної 6G-мережі приділяється управлінню ідентичністю та доступом. Умови масового підключення мільярдів пристроїв вимагають нових підходів до автентифікації, які виходять за межі традиційних SIM-карт або статичних облікових даних. У 6G використовуються багатофакторні та контекстно-орієнтовані механізми автентифікації, що враховують поведінкові характеристики, фізичні параметри пристроїв і умови середовища. Це значно ускладнює несанкціонований доступ навіть у разі компрометації окремих компонентів.

Криптографічна підсистема є одним із фундаментальних елементів безпечної архітектури 6G. З урахуванням розвитку квантових обчислень у 6G передбачається широке використання постквантової криптографії для захисту каналів зв’язку, обміну ключами та цифрових підписів. Архітектура мережі повинна бути криптографічно гнучкою, щоб забезпечити можливість швидкого переходу на нові алгоритми без необхідності повної заміни інфраструктури. Паралельно з цим у критично важливих сегментах можуть застосовуватися елементи квантового розподілу ключів для досягнення максимального рівня конфіденційності.

Безпечна архітектура 6G також враховує необхідність інтеграції наземних, повітряних і космічних сегментів зв’язку. Така гібридна структура підвищує надійність і глобальне покриття мережі, але потребує уніфікованих механізмів безпеки, здатних працювати в різних середовищах і умовах. Синхронізація, автентифікація та захист даних між різними сегментами реалізуються на основі єдиної політики безпеки, що мінімізує ризик появи слабких місць на стиках систем.

Значну роль у безпечній архітектурі 6G відіграє концепція сегментації мережі. Мережа динамічно поділяється на логічні сегменти, кожен з яких оптимізується під конкретні вимоги сервісів і рівень ризику. Це дозволяє ізолювати критично важливі додатки від менш захищених компонентів і обмежувати поширення атак у разі компрометації окремих сегментів. Такий підхід підвищує загальну стійкість мережі та спрощує управління безпекою.

Важливим аспектом архітектури безпечної 6G-мережі є забезпечення конфіденційності та захисту персональних даних. Надточне позиціонування, аналіз поведінки користувачів і масовий збір сенсорної інформації вимагають впровадження принципів мінімізації даних і приватності за замовчуванням. У 6G ці принципи реалізуються шляхом локальної обробки даних, анонімізації та використання криптографічних методів, що дозволяють виконувати аналіз без розкриття змісту інформації.

Завершальним елементом архітектури безпечної 6G-мережі є система безперервного моніторингу та реагування на інциденти. У 6G безпека розглядається як безперервний процес, що включає прогнозування загроз, автоматичне реагування та самовідновлення мережі. У разі виявлення атаки мережа здатна динамічно змінювати конфігурацію, перенаправляти трафік і ізолювати скомпрометовані елементи без переривання надання сервісів.

Таким чином, архітектура безпечної 6G-мережі є складною, адаптивною та інтелектуально керованою системою, у якій безпека інтегрована на всіх рівнях — від фізичного середовища передачі сигналу до логіки управління та обробки даних. Саме такий підхід дозволяє забезпечити стійкість мереж шостого покоління до сучасних і майбутніх кіберзагроз та створити надійну основу для розвитку цифрового суспільства майбутнього.

3.7 Перспективи Впровадження Pqc І Qkd У Мережах 6g

Перспективи впровадження постквантової криптографії (Post-Quantum Cryptography, PQC) та квантового розподілу ключів (Quantum Key Distribution, QKD) у мережах мобільного зв’язку шостого покоління є одним із ключових напрямів розвитку безпечних телекомунікацій майбутнього. Формування 6G відбувається в умовах одночасного зростання кіберзагроз, ускладнення архітектури мереж та поступового наближення епохи практичних квантових обчислень. Саме цей збіг технологічних факторів робить питання квантово-стійкого захисту інформації не теоретичною гіпотезою, а стратегічною необхідністю, яка має бути закладена в концепцію 6G ще на етапі проєктування.

Очікується, що часовий горизонт впровадження 6G збігатиметься з періодом, коли квантові комп’ютери досягнуть достатньої потужності для ефективного виконання алгоритмів, здатних зламувати класичні криптографічні схеми з відкритим ключем. Алгоритми RSA, DSA та криптосистеми на еліптичних кривих, які широко застосовуються в сучасних мобільних мережах, є вразливими до алгоритму Шора, а симетричні алгоритми зазнають послаблення через алгоритм Гровера. У цьому контексті 6G не може спиратися на

криптографічні механізми попередніх поколінь без ризику втрати конфіденційності, цілісності та автентичності даних у довгостроковій перспективі.

Постквантова криптографія розглядається як еволюційний шлях переходу до квантово-стійкого захисту в мережах 6G. Її основна перевага полягає в тому, що PQC-алгоритми можуть бути реалізовані на класичному апаратному та програмному забезпеченні без необхідності впровадження спеціалізованих квантових каналів. Це робить PQC найбільш реалістичним і масштабованим рішенням для глобальних мобільних мереж. У контексті 6G постквантова криптографія може застосовуватися для автентифікації абонентів і мережевих елементів, захисту сигнального трафіку, обміну ключами між вузлами мережі, а також для забезпечення цілісності програмних компонентів у віртуалізованому середовищі.

Архітектура 6G, заснована на програмно визначених мережах і хмарно-крайових обчисленнях, створює сприятливі умови для поступового впровадження PQC. Криптографічна гнучкість, яка є однією з базових вимог до 6G, дозволяє динамічно оновлювати алгоритми шифрування та механізми управління ключами без повного перезапуску інфраструктури. Це особливо важливо з огляду на те, що стандарти постквантової криптографії все ще перебувають у стадії розвитку та вдосконалення. Мережі 6G повинні бути здатними адаптуватися до нових рекомендацій і стандартів у міру їхнього затвердження.

Водночас впровадження PQC у 6G супроводжується низкою технічних і організаційних викликів. Багато постквантових алгоритмів характеризуються значно більшими розмірами ключів і цифрових підписів порівняно з класичними схемами. Це створює додаткове навантаження на радіоінтерфейс, обчислювальні ресурси та енергоспоживання пристроїв, особливо в умовах масового Інтернету речей і крайових обчислень. Тому перспективи PQC у 6G тісно пов’язані з оптимізацією алгоритмів, апаратною підтримкою криптографічних операцій і використанням інтелектуальних механізмів управління ресурсами.

На відміну від постквантової криптографії, квантовий розподіл ключів є революційним підходом до забезпечення конфіденційності, що базується на фундаментальних законах квантової фізики. QKD забезпечує інформаційно-теоретичну стійкість обміну ключами, оскільки будь-яка спроба перехоплення квантового каналу неминуче призводить до його виявлення. У контексті 6G QKD розглядається як технологія для захисту найбільш критичних сегментів мережі, де вимоги до безпеки є максимальними, а компрометація даних неприпустима.

Перспективи використання QKD у 6G пов’язані насамперед із захистом магістральних каналів між центрами обробки даних, ядрами мережі, а також із

забезпеченням безпеки міжсегментної взаємодії в гібридних наземно-супутникових архітектурах. Інтеграція QKD із супутниковими платформами відкриває можливість глобального розподілу квантових ключів, що особливо актуально для мереж 6G з їхнім прагненням до повного планетарного покриття. У цьому контексті 6G може стати першим поколінням мобільного зв'язку, у якому квантові технології безпеки матимуть практичне, а не експериментальне застосування.

Разом із тим широке впровадження QKD у радіодоступі 6G стикається з істотними обмеженнями. Квантові канали є чутливими до втрат, завад і фізичних впливів, що ускладнює їх використання в мобільному середовищі з високою динамікою. Крім того, вартість квантового обладнання та складність його інтеграції залишаються значними стримувальними факторами. Тому в перспективі QKD у 6G розглядатиметься не як універсальна заміна класичних і постквантових методів, а як доповнення до них у гібридних архітектурах безпеки.

Однією з ключових перспектив розвитку безпеки 6G є поєднання PQC і QKD у єдиній криптографічній екосистемі. Такий гібридний підхід дозволяє компенсувати недоліки кожної з технологій і досягти балансу між масштабованістю, ефективністю та максимальним рівнем захисту. PQC може забезпечувати базовий рівень квантово-стійкої безпеки для масових сервісів і пристроїв, тоді як QKD застосовуватиметься для захисту ключових елементів інфраструктури та критичних потоків даних.

Важливою перспективою є інтеграція PQC і QKD з інтелектуальними механізмами управління безпекою в 6G. Алгоритми штучного інтелекту можуть використовуватися для динамічного вибору криптографічних механізмів залежно від контексту, рівня загроз і вимог сервісів. Такий адаптивний підхід дозволяє оптимізувати використання ресурсів і підвищити загальну стійкість мережі до як класичних, так і квантових атак.

З погляду довгострокової конфіденційності даних, впровадження PQC і QKD у 6G має вирішальне значення. Мережі шостого покоління обслуговуватимуть дані, цінність яких зберігатиметься десятиліттями, включаючи медичну інформацію, біометричні дані, промислові секрети та державні інформаційні ресурси. Захист таких даних повинен враховувати не лише поточні, а й майбутні загрози, що робить квантово-стійкі технології безпеки стратегічним елементом архітектури 6G.

Отже, перспективи впровадження постквантової криптографії та квантового розподілу ключів у мережах 6G є надзвичайно широкими й багатовимірними. PQC забезпечує практичний і масштабований шлях до квантово-стійкої безпеки для масових мобільних сервісів, тоді як QKD відкриває можливість досягнення безпрецедентного рівня захисту для критично важливих сегментів

інфраструктури. Їхнє поєднання в рамках гнучкої, інтелектуальної та адаптивної архітектури безпеки є одним із ключових чинників успішного розвитку мереж мобільного зв'язку шостого покоління та формування довіри до цифрового суспільства майбутнього.

ВИСНОВОК

У даній дипломній роботі було здійснено комплексний аналіз розвитку мобільного зв'язку та еволюції кіберзагроз у мережах різних поколінь — від ранніх цифрових систем до сучасних і перспективних мобільних технологій. Проведене дослідження дозволило сформувати цілісне уявлення про те, як ускладнення архітектури мобільних мереж, зростання їх ролі в цифровій економіці та інтеграція з інформаційними технологіями призвели до якісної трансформації ландшафту кіберзагроз.

У роботі показано, що кожне покоління мобільного зв'язку характеризується власним набором вразливостей, які безпосередньо випливають з його архітектурних рішень. Для мереж 3G основними проблемами залишаються вразливості сигнальних протоколів, можливість використання фальшивих базових станцій та наявність значної кількості застарілих пристроїв. У мережах 4G ці загрози доповнюються ризиками, пов'язаними з повною IP-орієнтацією, віртуалізацією мережевих функцій та масовим використанням мобільного зв'язку як інфраструктури для цифрових сервісів і фінансових операцій. Мережі 5G, незважаючи на найвищий рівень вбудованої безпеки, формують нові вектори атак через сегментацію мережі, крайові обчислення та масове підключення IoT-пристроїв.

Окрему увагу в роботі приділено перспективам розвитку мереж шостого покоління, які розглядаються не лише як еволюція швидкостей і затримок, а як глобальна кіберфізична платформа, що поєднує телекомунікації, штучний інтелект, хмарні та квантові технології. Аналіз моделей загроз для 6G показав, що саме зростання складності, програмної визначеності та глибокої інтеграції з критично важливими сервісами робить ці мережі потенційно найбільш вразливими. Особливо небезпечними є довгострокові загрози, пов'язані з розвитком квантових комп'ютерів, які ставлять під сумнів криптографічну стійкість традиційних алгоритмів захисту.

У результаті дослідження обґрунтовано, що оптимізація мобільного зв'язку в умовах сучасних і майбутніх кіберзагроз неможлива в межах класичної парадигми безпеки, заснованої на статичних мережах і традиційних

криптографічних механізмах. Перехід до нової моделі захисту повинен включати впровадження пост-квантової криптографії як базового елемента довгострокової конфіденційності даних, а також використання квантового розподілу ключів у критичних сегментах ядра мережі для забезпечення принципово нового рівня захисту.

Доведено, що ключовими напрямами підвищення кіберстійкості мобільних мереж нового покоління є глибока сегментація мережі та реалізація концепції Zero-Trust, яка передбачає постійну перевірку кожного елемента інфраструктури незалежно від його розташування. Важливу роль відіграє застосування систем штучного інтелекту для безперервного моніторингу аномалій, раннього виявлення атак і адаптивного реагування на інциденти безпеки. Додатково підкреслено значення апаратних коренів довіри та відкритих архітектур, зокрема Open RAN, які дозволяють зменшити залежність від закритих рішень і підвищити прозорість та контрольованість мережевих компонентів.

Узагальнюючи результати роботи, можна зробити висновок, що оператори мобільного зв’язку, які першими здійснять перехід до пост-квантових механізмів захисту, інтегрують квантові технології розподілу ключів, впровадять принципи Zero-Trust та AI-орієнтовану кібербезпеку, отримають не лише підвищену стійкість до майбутніх атак, а й стратегічну технологічну перевагу. Таким чином, питання безпеки мобільного зв’язку в умовах кіберзагроз і розвитку квантових комп’ютерів набуває не лише технічного, а й стратегічного значення, визначаючи напрями розвитку телекомунікаційної галузі в найближчі десятиліття.