УДК 004.056.5

КЛЮЧОВІ ПРОБЛЕМИ БЕЗПЕКИ У ТЕХНОЛОГІЯХ БЕЗДРОТОВОГО ЗВ'ЯЗКУ 5G

Чибізов І. О.
Науковий керівник- старший викладач В’юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: ihor.chybizov@nure.ua

5G is the fifth generation of mobile communications that offers significantly higher speed, bandwidth and reliability compared to 4G. The growing use of 5G in various industries, such as the Internet of Things (IoT), autonomous vehicles, and telemedicine, makes the issue of 5G communication security extremely important. Previous generations of mobile networks had the primary goal of providing fast and reliable data services to users. However, 5G extends this concept by offering a wide range of wireless services through different access platforms and multi-layer networks. It is through services that the main issues of technology security will be considered in this work.

5G – це п'яте покоління мобільного зв'язку, яке пропонує значно більшу швидкість, пропускну здатність та надійність, порівняно з 4G. Зростаюче використання 5G у різних галузях, таких як Інтернет речей (IoT), автономні транспортні засоби та телемедицина, робить питання безпеки зв'язку 5G надзвичайно важливим [1].

Попередні покоління мобільних мереж мали основну мету у наданні швидких і надійних послуг передачі даних для користувачів. Однак 5G розширює цю концепцію, пропонуючи широкий спектр бездротових послуг через різні платформи доступу та багаторівневі мережі [2].

Архітектура 5G створює динамічну, узгоджену та гнучку структуру для підтримки різноманітних програм. Вона використовує більш інтелектуальну систему з мережами радіодоступу (RAN), які вже не обмежені лише базовими станціями чи складною інфраструктурою. Замість цього, 5G впроваджує дезагреговану, гнучку та віртуальну RAN з новими інтерфейсами, що створюють додаткові точки доступу до даних.

Для 5G існують два варіанти розгортання:

1. Архітектура "Неавтономна" (NSA), де мережа радіодоступу 5G (AN) та інтерфейс New Radio (NR) використовуються разом з існуючою базовою мережею інфраструктури LTE та EPC (відповідно до 4G Radio та 4G Core), що дозволяє використовувати технологію NR без необхідності заміни мережі. У цій конфігурації підтримуються лише послуги 4G, але вони використовують можливості, що пропонує 5G New Radio (зокрема, менша затримка). NSA також відомий як "E-UTRA-NR Dual Connectivity (EN-DC)" або "Архітектурний варіант 3" (рисунок 1).

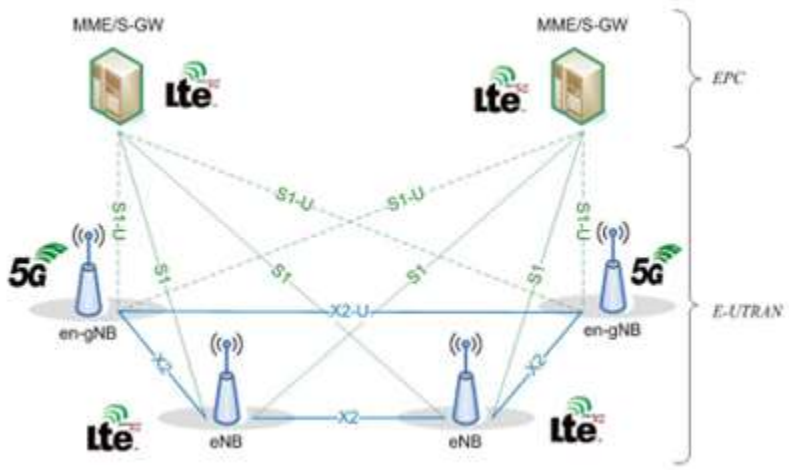

Рисунок 1 – Архітектура неавтономного доступу до мережі 5G

2. Архітектура "Автономна" (SA), де NR підключений до 5G CN. Тільки в цій конфігурації підтримується повний набір послуг 5G Phase 1 (рисунок 2).

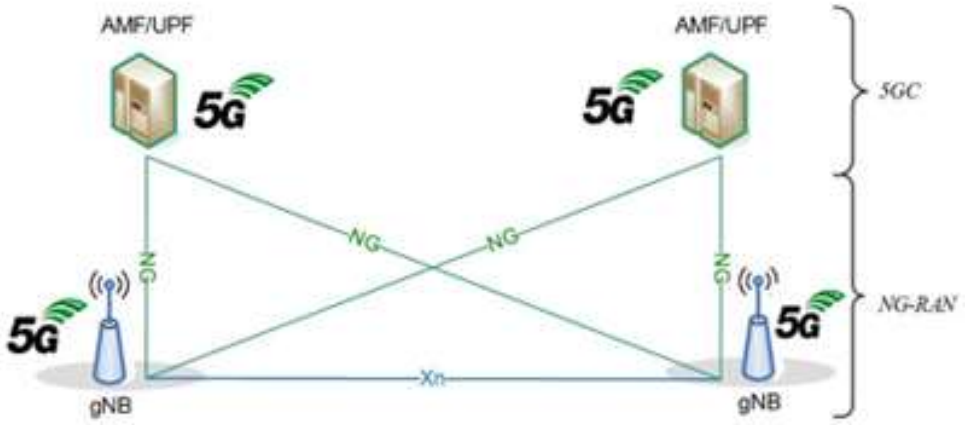

Рисунок 2 – Архітектура автономного доступу до мережі 5G

Впровадження технології 5G пов'язане з рядом викликів в галузі безпеки, які потребують уваги та вирішення. Одним із головних аспектів є безпека критичної інфраструктури, яка стає більш вразливою через збільшення кількості підключених пристроїв та IoT. Порушення безпеки в таких системах може мати катастрофічні наслідки для суспільства. Крім того, забезпечення безпеки радіоінтерфейсів важливе для запобігання доступу до конфіденційної інформації через незахищені канали [3].

Розробка ефективних стратегій та рішень для вирішення цих викликів є критичною для забезпечення безпеки та надійності мереж 5G. Співробітництво між виробниками обладнання, операторами мереж та регуляторними органами може допомогти розробити стандарти та протоколи, які забезпечать безпеку мереж 5G на високому рівні [3].

Деякі з ключових викликів, визначених Mobile Networks Next Generation (NGMN) включають такі:

1. Флеш-мережевий трафік: Збільшена кількість підключених пристроїв та IoT може призвести до перевантаження мережі, що може вплинути на безпеку та стабільність системи.
2. Безпека радіоінтерфейсів: Використання незахищених каналів для передачі ключів шифрування може зробити мережу вразливою перед атаками.
3. Цілісність площини користувача: Відсутність криптографічного захисту цілісності даних користувача може призвести до ризику несанкціонованого доступу до чутливої інформації.
4. Безпека роумінгу: Недостатня оновлення параметрів безпеки під час роумінгу між мережами операторів може призвести до ризику компрометації безпеки.
5. Атаки типу "відмова в обслуговуванні" (DoS): Напади на інфраструктуру мережі, такі як DoS, можуть призвести до переривання послуг та зниження якості обслуговування.
6. Сигнальні шторми: Неспроможність розподілених систем керування координувати свою діяльність може призвести до ситуацій, коли рівень сигналізації перевищує потреби мережі, що може вплинути на її ефективність.
7. DoS-атаки на пристрої кінцевих користувачів: Відсутність адекватних заходів безпеки на пристроях кінцевих користувачів може зробити їх вразливими перед атаками та незаконним доступом до особистих даних.

Як можна побачити з виявлених вище проблем то основна їх частина походить від збільшення кількості підключень до базових станцій на які можуть бути здійснені DoS-атаки через ці пристрої за допомогою слабозахищених каналів передачі даних. Ще існує ймовірність неуважного користувача мобільного зв'язку і якщо всі фактори складуться, то втрата особистих даних, грошових коштів тощо стає постійною загрозою безпеці.

Вирішенням виявлених загроз можна зробити обмеженням пристроїв на одну базову станцію, автоматичним оновленням протоколів безпеки і якщо це корпоративна мережа вести облік користувачів мережі та активних пристроїв.

Список використаних джерел

1. 5G NR: технологія бездротового доступу нового покоління. Ерік Дальман, Стефан Парквалл, Йохан Скольд. Академ. вид.: 2020 р.. 548 с.
2. Тимошенко, Д. В. Публікація: Вплив розвитку 5G технологій на майбутнє телекомунікаційного сектору 2023р.
https://openarchive.nure.ua/handle/document/25365
3. Базові мережі 5G: посилення цифровізації. Стефан Роммер, Пітер Хедман, Магнус Олссон, Ларс Фрід, Шабнам Султана. Академічна преса: 2019 р., 476 с.