УДК 654.01

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В 5G МЕРЕЖАХ

Орест Полотай, Нагірний Ростислав

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів

кафедра безпеки інформаційних технологій Національного університету Львівська Політехніка, м. Львів

Описано особливості інформаційної безпеки сучасних технологій 5G-мереж.
Ключові слова: інформаційна безпека, 5G-мережі

Features of information security of modern 5G network technologies are described.
Keywords: information security, 5G networks

5G – це п’яте покоління мобільних мереж, новий етап розвитку технологій, який покликаний розширювати можливості доступу до Інтернету через мережі радіодоступу, пропонує надійніші з'єднання на смартфонах та інших пристроях, ніж будь-коли раніше.

Найбільша відмінність між мережами 5G і мережами попередніх поколінь – це вища швидкість мережі Інтернет. Теоретично можливі швидкості становлять 10-20 Гбіт/с, при цьому затримка передачі сигналу становить лише 1-2 мс. Наприклад, теоретична максимальна швидкість для 4G становить до 1 Гбіт/с із затримкою сигналу 10 мс, а для 3G - до 42 Мбіт/с із часом відгуку 100 мс.

Безпека в 5G – це захищеність інформації та допоміжної інфраструктури від випадкових або навмисних природних або антропогенних впливів, які можуть завдати шкоди власникам і користувачам інформації та допоміжної інфраструктури.

Поняття безпеки в 5G, як і захист інформації, є комплексним питанням, яке реалізується через впровадження систем безпеки. Питання захисту інформації є багатогранним і складним і включає в себе ряд ключових проблем.

Основними загрозами в 5G мережах є:

- Загрози пов'язані з навколишнім середовищем (стихійні лиха, техногенні катастрофи і т.д.);
- Технічні (відмови обладнання і програмного забезпечення, витік інформації по каналах зв'язку і т.д.);
- Людські (в результаті навмисних і ненавмисних дій).

Як і будь-яка масштабна технологія, 5G приверне увагу хакерів і кіберзлочинців.

Концепція безпеки мереж 5 п'ятого покоління включає в себе:

- Автентифікацію користувача з боку мережі.
- Автентифікацію мережі з боку користувача.
- Узгодження криптографічних ключів між мережею і призначеним для користувача обладнанням.
- Шифрування і контроль цілісності сигнального трафіку.
- Шифрування і контроль цілісності призначеного для користувача трафіку.
- Захист ідентифікатора користувача.

• Захист інтерфейсів між різними елементами мережі відповідно до концепції мережевого домену безпеки.

• Ізоляцію різних верств механізму network slicing і визначення для кожного шару власних рівнів безпеки.

• Автентифікацію користувача і захист трафіку на рівні кінцевих сервісів (IMS, IoT та інших).

Безпека телекомунікаційних мереж визначається наступними елементами

• Стандартизація: процес, за допомогою якого оператори, постачальники та інші зацікавлені сторони встановлюють стандарти для спільної роботи мереж у всьому світі. Сюди входить і те, як найкраще захистити мережу та її користувачів від зловмисників.

• Проектування мережі: проектування, розробка та впровадження постачальниками мережі узгоджених стандартів для функціональних мережевих елементів і систем, які відіграють ключову роль у забезпеченні функціональності та безпеки кінцевого мережевого продукту.

• Це відіграє ключову роль у встановленні параметрів безпеки та подальшому підвищенні безпеки та стійкості мережі.

• Розгортання та експлуатація мережі. Операційні процеси, які дозволяють мережі функціонувати і забезпечувати цільовий рівень безпеки, сильно залежать від розгортання і роботи самої мережі. Тому для ефективного захисту потоків даних в мережі необхідно використовувати новітні технології, в тому числі продукти Cisco Systems.

Мережі 5G пропонують вищі швидкості, ніж їхні попередники, що може допомогти зменшити затримку та забезпечити більш безпечну передачу даних. Ця покращена швидкість забезпечує міцну основу для розробки більш безпечних служб, таких як хмарні служби. Мережі 5G також забезпечують більш безпечний зв’язок між пристроями завдяки покращеним протоколам шифрування та покращеним механізмам автентифікації. Цей покращений захист допомагає зловмисникам ускладнити доступ до мереж і компрометувати дані.

5G також підтримує розвиток нових технологій, таких як Інтернет речей (IoT). Використання пристроїв IoT збільшує поверхню атаки мережі, роблячи її більш уразливою до кібератак. Мережі 5G можуть допомогти захистити ці пристрої, надаючи розширені протоколи шифрування та автентифікації. Мережі 5G також забезпечують більш розширені заходи безпеки, такі як технології розподіленої книги, які можна використовувати для захисту передачі даних.

Мережі 5G можуть допомогти компаніям захистити свої дані від кібератак, а також дозволити компаніям впроваджувати розширені засоби контролю безпеки, такі як штучний інтелект і машинне навчання, які можуть допомогти швидше виявляти кіберзагрози та реагувати на них. Ця підвищена швидкість і надійність може допомогти захистити компанії від витоку даних, що може коштувати дорого та завдати шкоди їхній репутації.

Підсумовуючи, можна стверджувати, що запровадження мереж 5G трансформує ландшафт цифрової безпеки. Мережі 5G пропонують покращену швидкість, надійність і заходи безпеки, які можуть допомогти захистити бізнес від кібератак. Цей покращений захист може допомогти компаніям захистити свої дані та забезпечити більшу безпеку своїх систем.

Література

1. Наслідки для безпеки 5G-мереж. URL: https://ts2.space/uk/наслыдки-для-безпеки-мереж-5g-2/#gsc.tab=0
2. Правило В.В., Кормульов О.С. Методи забезпечення заданих показників безпеки // Збірник матеріалів XIV Міжнародної науково-технічної конференції "Перспективи телекомунікацій 2020". Київ: 2020. С. 178-180.
3. Як захистити 5G від взлому: вивчаємо архітектуру безпеки Хабр URL: https://habr.com/ru/company/trendmicro/blog/453120/