УДК 004.052

БЕЗПЕКА МЕРЕЖ 5G

Михайловський Руслан Андрійович
Науковий керівник– к.т.н., Желанов О.О.
Харківський національний університет радіоелектроніки,
каф. МІРЕС, м. Харків, Україна
тел. +380997138451, e-mail: ruslan.mykhailovskyi@nure.ua

The report discusses the current threats to information security for 5G networks and the basics for ensuring their protection.

Новий стандарт мобільного зв'язку може стати універсальною інфраструктурою взаємодії людей, розумних пристроїв, організацій та цілих галузей економіки. Але загальна пов'язаність має зворотний бік – поява найбільш масштабних кіберзагроз.

На відміну від попередніх поколінь мобільних мереж, орієнтованих в основному на масового споживача (послуги голосового зв'язку, мобільного доступу в Інтернет), стандарт 5G розвивається переважно на користь корпоративного та державного сектора.

Для вивчення питань пов’язаних з проблемами безпеки, розглянемо основні особливості архітектури мереж 5G

1. Мережа радіодоступу (RAN) заснована на новому стандарті 5G NR (New Radio), що реалізує необхідні характеристики: пропускна здатність, мінімальні затримки або масові підключення. Згідно концепції архітектури, інші мережі радіодоступу (Wi-Fi, 4G-LTE) повинні підключатися до єдиного ядра мережі 5G. Основні ризики: велика кількість підключень та висока пропускна здатність збільшують поверхню атаки, IoT-пристрої менш стійкі до злому.

2. Архітектура опорної мережі (ядро мережі або 5G Core) заснована на хмарних технологіях та віртуалізації мережевих функцій (SDN, NFV), що дозволяє створити безліч незалежних сегментів і підтримувати таким чином сервіси з різним набором характеристик. Сегментування також дозволяє операторам надавати мережеву інфраструктуру у вигляді сервіса для організацій. Ризиками будуть серйозні наслідки збоїв або зловживань з огляду на масштаб використання.

3. 5G передбачає активне використання технології периферійних обчислень (MEC). Це можуть бути, зокрема, корпоративні програми, що працюють на мережі операторів: інтелектуальні сервіси, фінансові сервіси, мультимедіа. Слід додати, що у цьому випадку відбувається інтеграція операторських мереж 5G у корпоративну інфраструктуру.

Основними ризиками стають можливості проникнення в корпоративні мережі, розміщення обладнання MEC поза захищеним периметром організації.

4. Централізована інфраструктура управління мережею (O&M)

ускладнюється за рахунок необхідності одночасної підтримки великої кількості сервісних сегментів. Ризиками стають наслідки зловживання ресурсами та помилки конфігурації O&M.

Серед найбільш значущих загроз для кожного з головних компонентів мережі 5G можна виділити наступні (див. табл.).

Таблиця 1

Загрози для RAN	Загрози для опорної мережі та сервісів оператора	Загорози для MEC	Загрози для інфраструктури 5G із зовнішніх мереж
DDoS-атаки від термінальних пристроїв. Використання підроблених базових станцій. Атаки на бездротові інтерфейси - перехоплення, підміна даних користувача	Програмні та апаратні збої елементів ядра, помилки конфігурації Використання шкідливого коду або експлуатація вразливостей компонентів інфраструктури. Порушення ізоляції сегментів, НСД до сегменту	Фізичний доступ порушника до обладнання Підроблений або вразливий сторонній додаток в екосистемі. Проникнення в корпоративні або операторські мережі із вузлів MEC	DDoS-атаки з Інтернету НСД до API постачальників сервісів. НСД до інтерфейсу управління із зовнішніх мереж

Ґрунтуючись на основних принципах стандарту 5G, визначимо, які заходи будуть необхідні для протидії загрозам в мережах 5G:

1. Захист на рівні стандарту:

-поділ шарів протоколу передачі даних на три площини: User Plane, Control Plane, Management Plane;

- ізоляція, шифрування та контроль цілісності площин; шифрування абонентського та сигнального трафіку; збільшення довжини ключа шифрування трафіку з 128 біт до 256 біт;

- єдиний механізм автентифікації абонентів для різних типів бездротового зв'язку;

2. Захист на рівні рішень, обладнання та інфраструктури мережі:

- багаторівнева ізоляція та захист цілісності компонентів SDN та VNF – гіпервізора, віртуальних машин, ОС, контейнерів;

- забезпечення високої доступності віртуальних машин для швидкого відновлення після атак;

- додатковий фактор автентифікації при доступі до корпоративної мережі, білий список пристроїв та служб;

- захищені канали зв'язку між базовою станцією; виявлення атак у реальному часі на мережевих вузлах та елементах віртуальної інфраструктури з використанням алгоритмів ІІ.

3. Захист на рівні управління мережею:

- багатофакторна автентифікація та розмежування доступу до сегментів з боку O&M;

- засоби виявлення підроблених базових станцій на основі моніторингу подій обслуговування;

- безпечне управління життєвим циклом даних користувача а також аналітичних та службових даного оператора – шифрування, анонімізація, безпечне зберігання та видалення;

- централізоване управління вразливостями, політиками ІБ, аналіз більших даних для виявлення аномалій та раннього реагування на атаки (SOC).

Безпека мереж 5G не обмежується технічними заходами захисту та складається зі спільних зусиль сторін, які довіряють один одному– розробників стандарту, регуляторів, вендорів, операторів та постачальників послуг.

Список використаних джерел:

1. Пастушенко М. С. Кібербезпека в мережах 5G / М. С. Пастушенко, Б. О. Сазонов // Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023) : матеріали дев’ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 141-143.

2. Understanding 5G: A Guide to the Next-Generation Wireless Technology by Federal Communications Commission. URL: https://www.fcc.gov/5G. (дата звернення: 18.02.2024).

3. 5G Security - The Future of Networks by GSMA. URL: https://www.gsma.com/security/5g-security/. (дата звернення: 18.02.2024).

4. The 5G Cybersecurity Dilemma: A Guide to the Global Network Vulnerabilities of 5G by The Council on Foreign Relations. URL: https://www.cfr.org/report/5g-cybersecurity-dilemma. (дата звернення: 18.02.2024).

5. 5G Security Challenges and Opportunities" by Deloitte. URL: https://www2.deloitte.com/us/en/insights/focus/5g-wireless-security.html. (дата звернення: 18.02.2024).