УДК 004.056:621.396.946

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ 5G

Хелмі Муханнад, Марчук В.С.
e-mail: muhanad.ahmad.helmy@nure.ua , volodymyr.marchuk@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім В.В.Поповського
м. Харків, Україна

This work is devoted to the features of information protection in 5G telecommunication networks. In addition to standard applications, the 5G network has new ones based on virtualization and software-defined network technologies. Information protection in SDN networks lies in overcoming attacks on the path from network elements to the controller, and the presence of a virtualized NFVI infrastructure requires protection against DoS attacks and from the injection of malicious virtual network functions VNF.

Технології 5G суттєво відрізняються від попередніх поколінь, які виконували два головні завдання: комунікації (телефонний зв'язок та текстові повідомлення) і мобільний доступ до Інтернету. Мережа 5G – це мережа, орієнтована на різні застосування, а не лише на голос, текстові повідомлення та широкосмуговий доступ до Інтернету. Важлива відмінність у тому, що мережі 5G засновані на технологіях віртуалізації та програмно-конфігурованих мереж. Це породжує нові проблеми безпеки та нові вразливості [1,2].

Ще одна відмінність нової технології полягає в тому, що в мережах попередніх поколінь для кожного нового завдання потрібно було створювати нову мережу або виділяти окремий сервер додатків. У 5G, внаслідок віртуалізації та програмного конфігурування, можна створювати логічно незалежні мережеві шари (Network Slicing) на базі єдиної мережної інфраструктури [3]. У попередніх поколіннях таке було неможливе. Проте коло ризиків безпеки розширюється.

Розглянемо особливості захисту в мережах 5G. Технологія 5G заснована на програмно-конфігурованій мережі SDN (Software-Defined Networking) та віртуалізації мережевих функцій NFV (Network Function Virtualization). Як SDN, так і NFV широко використовують протоколи HTTP і REST API. Ці протоколи добре вивчені та широко використовуються в Інтернеті. Засоби знаходження та експлуатації вразливостей цих протоколів добре відомі зловмисникам.

Друга група ризиків пов'язана з архітектурою додатків. Найчастіше веб-додатки містять небезпечні вразливості. Бурхливе зростання кількості веб-додатків суттєво збільшує небезпеку злому мережі.

Третя група ризиків – використання технології Network Slicing. Створення кількох логічних мереж за наявності єдиної мережної

інфраструктури може призводити до ризиків компрометації окремих мережевих шарів та доступу зловмисників до ресурсів та пристроїв користувачів.

На етапі керування доступом до мережі SDN або NFV можуть виникати ризики, які відносяться, в основному до порталів самообслуговування, де здійснюється процес керування доступом (Admission Control). При цьому суттєвим є протидія атакам типу «відмова від обслуговування» DoS (Denial of Service).

Додаткові ризики виникають у авторизованих користувачів, які здійснюють в мережі ризиковані дії, так званий відгук доступу (Maverick Endpoints).

SDN – централізовано керована структура передачі, у якій процес адаптивної маршрутизації має місце у центральному контролері, а не в апаратних мережевих вузлах. Вразливість у мережі SDN криється на шляху від мережевого елемента до контролера SDN, тобто. у каналі управління площиною передачі. На цьому шляху також може бути атака «відмова в обслуговуванні» (DoS).

У NFV програмні (віртуальні) мережеві функції VNF, які входять до складу віртуальних «пристроїв», розподілені у складі фізичної інфраструктури. При цьому існують два види ризиків:

– можливий ризик атак DoS із боку площини даних у горизонтальних з'єднаннях;

– можливі значні ризики у вертикальних зв'язках між віртуальними функціями VNF та ресурсами, виділеними для кожної VNF.

Ще один ризик може виникнути при ін’єкції зловмисником в інфраструктуру NFV функцій VNF, які згубно впливають на програми та дані користувачів.

Слід звернути увагу на вразливості в API серверів. Якщо не буде захисту на контролері, зловмисник може отримати повний контроль мережі.

Список використаних джерел:

1. A 5G Americas White Papers. Security for 5G. URL: https://www.5gamericas.org/wp-content/uploads/2021/12/Security-in-5G.pdf (дата звернення 25.02.2025)

2. I.Ahmad, S.Shahabuddin, T.Kumar. Security for 5G and Beyond. URL: https://www.researchgate.net/publication/332970813_Security_for_5G_and_Beyond#fullTextFileContent (дата звернення 25.02.2025)

3. V.Singh, M. Singh, S. Hegde. Security in 5G Network Slices: Concerns and Opportunities. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10494839 (дата звернення 25.02.2025)