що використовують соціальну інженерію для маніпуляцій користувачами, становлять серйозну загрозу, оскільки здатні обійти технічні засоби захисту, впливаючи безпосередньо на людський фактор. Ефективні методи протидії включають впровадження сучасних систем багатофакторної автентифікації (MFA), що значно ускладнюють доступ до мереж навіть у разі компрометації облікових даних [1]. Важливою складовою захисту є також підвищення обізнаності користувачів щодо технік соціальної інженерії та навчання співробітників основам кібергігієни. Проведення регулярних тренінгів з виявлення фішингових атак та небезпечних комунікацій дозволяє значно знизити ризики таких інцидентів [2]. Інші технічні рішення включають використання автоматизованих систем виявлення фішингових загроз, таких як інтелектуальні фільтри для електронної пошти та інтеграція з базами даних відомих зловмисних доменів. Ці заходи сприяють вчасному виявленню потенційних загроз і захисту кінцевих користувачів від небажаного впливу [3].

Метою доповіді є розгляд сучасних методів захисту від фішингових атак та соціальної інженерії в телекомунікаційних мережах, аналіз ключових викликів і шляхів їх вирішення.

Список літератури

1. Кузьменко М.В. Мультфакторна автентифікація як метод захисту від фішингу – Київ: Видавничий дім "Кібербезпека", 2010. – 210 с.

2. Савчук Г.Д. Підвищення обізнаності користувачів: навчання кібергігієни – Київ: Видавництво "Інформаційна безпека", 2013. – 340 с.

3. Левченко П.О. Автоматизовані системи виявлення фішингових загроз у телекомунікаційних мережах – Київ: Інститут телеком. технологій, 2019. – 307 с.

ЗАХИСТ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ: МЕТОДИ ШИФРУВАННЯ ТА АВТЕНТИФІКАЦІЇ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком телекомунікаційних систем та зростанням обсягів переданої інформації питання захисту даних стає дедалі актуальнішим. Для забезпечення конфіденційності, цілісності та автентичності інформації, що передається через мережі, ключову роль відіграють методи шифрування та автентифікації. Сучасні криптографічні алгоритми, такі як AES (Advanced Encryption Standard) та RSA, забезпечують високий рівень захисту, роблячи передані дані недоступними для несанкціонованого доступу або втручання. Використання цих методів є необхідним для захисту приватних та конфіденційних комунікацій, включаючи фінансові транзакції та особисті дані користувачів [1]. Автентифікація, яка гарантує ідентифікацію користувачів та пристроїв, є ще одним важливим компонентом захисту даних. У телекомунікаційних системах широко застосовуються двофакторна автентифікація (2FA) та протоколи, такі як OAuth і Kerberos, які забезпечують безпечний обмін даними між клієнтами

та серверами. Ці технології не тільки підтверджують особу користувача, але й захищають від атак типу «людина посередині» (MitM) та несанкціонованого доступу до ресурсів мережі [2]. **Метою доповіді є** огляд сучасних методів шифрування та автентифікації, які використовуються для захисту даних у телекомунікаційних системах, аналіз їхньої ефективності та надійності, а також перспективи розвитку новітніх технологій у цій сфері.

Список літератури

1. Осламенко Д.Д. AES та RSA: Основи шифрування даних у сучасних телекомунікаційних мережах – Київ: Видавничий дім "Безпека", 2009. – 282 с.

2. Кривонос В.М. Протоколи автентифікації в телекомунікаціях: Захист доступу за допомогою 2FA та OAuth – Київ: Видавництво "Телекомунікації", 2017. – 279 с.

КІБЕРБЕЗПЕКА В ЕПОХУ 5G: НОВІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАХИСТУ

Показій К.О., Тимошенко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком 5G технологій виникають нові виклики у сфері кібербезпеки, що пов'язані зі збільшенням кількості підключених пристроїв, масштабністю мереж та складністю їх інфраструктури. 5G надає можливість підключати значну кількість пристроїв, зокрема в межах Інтернету речей (IoT), що розширює поверхню для атак і збільшує потенційні вразливості [1]. Однією з ключових загроз в епоху 5G є складність управління безпекою в розподілених і віртуалізованих мережах, які використовують програмно-визначені мережі (SDN) та мережеві функції віртуалізації (NFV). Ці технології покладаються на програмне забезпечення, яке може стати об'єктом кібератак, якщо не будуть впроваджені належні заходи захисту. Особливо вразливими є інфраструктури критичних галузей, де збій або атака на мережу можуть мати серйозні наслідки для безпеки й економіки [2]. Для вирішення цих викликів важливим є розробка нових стратегій захисту, що включають використання штучного інтелекту та машинного навчання для автоматизованого виявлення і запобігання загрозам у реальному часі. Додатково, потрібно забезпечувати сегментацію мережі для ізоляції атак та зниження ризику їх поширення, а також впроваджувати нові стандарти шифрування та аутентифікації для забезпечення захисту даних під час їх передачі в 5G мережах [3].

Метою доповіді є розгляд нових викликів кібербезпеки, які постають з впровадженням 5G технологій, та аналіз ефективних стратегій захисту, що допоможуть знизити ризики кібератак і забезпечити надійне функціонування телекомунікаційних мереж.

Список літератури

1. Ткаченко О.В. Виклики кібербезпеки 5G: Інтернет речей та розширююча поверхня атак – Київ: Технічний університет, 2023. – 250 с.