СУЧАСНІ ЗАСОБИ ЗАХИСТУ МЕРЕЖ WI-FI

Блінна В.С., В'юхін Д.О., Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Бездротові мережі стали не тільки частиною життя, але й мішенню для кібератак. Використання комплексного захисту значно зменшує ризики злому.

Метою доповіді є розгляд та порівняння сучасних засобів захисту Wi-Fi. Розглядаються основні типи захисту.

1) Використання надійного пароля. Пароль повинен мати щонайменше 10-12 символів з використанням цифр, розділових знаків і службових символів ($, @ і %), без простих послідовностей, щоб уникнути атаки грубою силою.

2) Приховання SSID (ідентифікатор набору послуг) [1] зменшує ризик несанкціонованого доступу та атак, таких як War Driving і Evil Twin. Після ручних налаштувань Wi-Fi більше не буде видимим при скануванні сусідніх мереж, ці точки можливо знайти лише при використанні додаткових засобів.

3) Увімкнення бездротового шифрування також є важливим для захисту даних. Сьогодні найбільш захищеним є протокол WPA3 [2]. WPA3 пропонує більш гнучке шифрування за допомогою AES-CCMP/AES-GCMP, дозволяє використовувати 128- і 256-бітові сеансові ключі [3].

4) Вимкнення віддаленого доступу до Wi-Fi, оскільки зловмисники, особливо у публічних мережах, можуть отримати контроль над маршрутизатором через атаки Brute Force, Man-in-the-Middle та DNS Spoofing.

5) VPN також має важливе значення для захисту інформації, він відправляє трафік користувача через зашифрований «тунель», що ускладнює його розшифрування та перехоплення, і маскує IP-адресу [4].

Таким чином, складні паролі, VPN, протокол WPA3 та приховування мережі забезпечують надійний рівень захисту для Wi-Fi. Нажаль, іноді неможливо застосувати всі засоби, тому приховування SSID може бути менш важливим, особливо коли ввімкнено WPA3, яке забезпечує більш надійне шифрування та захист від грубої сили. У такому випадку навіть якщо хтось побачить SSID, зламати мережу без знання пароля буде вкрай складно.

Список літератури

1. Hack proofing your wireless network / ed. by B. Christian, O. Neal. Rockland, Mass: Syngress Pub., 2002. 483 c.

2. Золотарьов В., Фодченко А. ШИФРУВАННЯ WI-FI 6-МЕРЕЖ. *Радіоелектроніка та молодь у XXI столітті. Т. 4: Конференція "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій"*. Харків, Україна, 2024. DOI: https://doi.org/10.30837/iyf.pdicimt.2024.168.

3. Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained. eSecurity Planet. URL: https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks.

4. Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN. 2023.