

ЗАХИСТ МЕРЕЖ ДОСТУПУ НА БАЗІ ТЕХНОЛОГІЇ WI-FI

Сливар У. М.

e-mail: uliana.slyvar@nure.ua

Науковий керівник – старший викладач Ликова Г.О.

Харківський національний університет радіоелектроніки, каф. КРiСТЗІ
м. Харків, Україна

This work enhances Wi-Fi security by adding two-factor authentication with Google Authenticator. A one-time password (OTP) changes every minute, preventing brute-force and WPS attacks. Testing confirms improved protection against unauthorized access.

У сучасному світі бездротові мережі Wi-Fi є основним засобом доступу до Інтернету, що використовується у домівках, офісах, громадських місцях і підприємствах. Однак збільшення кількості підключених пристроїв і загальнодоступність мереж роблять їх привабливою ціллю для атак. Незважаючи на постійне вдосконалення стандартів безпеки (WPA, WPA2, WPA3), зловмисники знаходять нові методи компрометації мережевих паролів. Це вимагає розробки нових механізмів захисту, які можуть ускладнити несанкціонований доступ до Wi-Fi.

Однією з основних загроз є атаки брутфорсом та WPS Pixie Dust Attack, що дозволяють зловмисникам отримати пароль до бездротової мережі. Використання статичних паролів робить ці атаки ще більш ефективними. Тому актуальним є розробка методу додаткової автентифікації, який дозволив би мінімізувати ризики зламу мереж [1, 3].

Незважаючи на розвиток стандартів безпеки Wi-Fi, таких як WPA3, проблеми захисту залишаються актуальними. Серед основних недоліків існуючих методів:

- використання статичних паролів, які можуть бути підібрані шляхом брутфорс-атаки;
- уразливості WPS, які дозволяють здійснити атаку Pixie Dust;
- відсутність двофакторної автентифікації для доступу до Wi-Fi.

Рішенням цієї проблеми може стати інтеграція механізмів двофакторної автентифікації на основі одноразових паролів (OTP), які змінюються щохвилини та генеруються за допомогою Google Authenticator [2].

Запропонований метод базується на використанні додаткового рівня автентифікації через Google Authenticator. Для перевірки одноразового пароля використовується бібліотека Python pyotp, яка дозволяє обчислювати очікуване значення OTP на основі секретного ключа. Це забезпечує коректну синхронізацію між пристроєм користувача та сервером автентифікації. Динамічне генерування пароля, який змінюється кожну хвилину, суттєво ускладнює злам мережі, оскільки навіть у разі його перехоплення зловмисник не зможе використати його після закінчення короткого терміну дії.

Метод реалізується наступним чином:

- при підключенні пристрою до Wi-Fi мережі через пароль WPA/WPA2/WPA3 роутер блокує доступ до Інтернету;
- користувач вводить додатковий одноразовий пароль (ОТР), згенерований Google Authenticator;
- сервер автентифікації, використовуючи ruotp, перевіряє правильність введеного пароля;
- після успішної перевірки роутер додає IP-адресу пристрою до білого списку в фаєрволі, відкриваючи доступ до Інтернету;
- кожні 24 години білий список очищається, і користувачеві потрібно знову пройти автентифікацію.

Цей механізм можна реалізувати через перепрошивку роутера.

Результати дослідження:

- перехоплення трафіку зломисником не дозволяє отримати точний пароль, оскільки він змінюється щохвилини;
- атаки брутфорсом значно ускладнюються, адже підбирати кожен новий пароль зломисник не встигає.

Розглянутий метод двофакторної автентифікації для WPA/WPA2/WPA3 на базі Google Authenticator значно підвищує рівень безпеки Wi-Fi мереж.

Основними перевагами є:

- динамічна зміна паролів, що унеможлиблює їх компрометацію;
- висока стійкість до атак типу Brute Force та WPS Pixie Dust.

Таким чином, запропонований метод значно покращує захист бездротових мереж і ускладнює несанкціонований доступ до них.

Список використаних джерел:

1. Fortinet. What is a Brute Force Attack? Definition, Types & How It Works. URL: <https://www.fortinet.com/resources/cyberglossary/brute-force-attack> (дата звернення: 15.02.2025).

2. Google Authenticator. URL: <https://support.google.com/accounts/answer/1066447?hl=uk> (дата звернення: 09.02.2025).

3. Hack Wi-Fi Using WPS Pixie Dust Attack. URL: <https://null-byte.wonderhowto.com/how-to/hack-wifi-using-wps-pixie-dust-attack-0162671/> (дата звернення: 09.02.2025).