

УДК 004.056

Гурський Г. А. – ст. гр. СН-51

*Тернопільський національний технічний університет імені Івана Пулюя*

## **ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ЗАХИСТУ БЕЗПРОВІДНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ WEP, WPA ТА WPA2**

Науковий керівник: к.т.н., доцент Фриз М.Є.

Сучасний стан розвитку засобів безпроводних комунікацій зробили реальним і доцільним широке впровадження безпроводних мереж типу Wi-Fi з метою підвищення швидкості проектування та реалізації комп'ютерних мереж, зручності їх використання в тих ділянках, де прокладання кабелю чи оптоволокна є доволі складним за затратним процесом. Проте із появою безпроводних мереж виникло і безліч проблем, пов'язаних з їхнім захистом від несанкціонованого доступу. Тому дана тематика є досить актуальною на сьогоднішній час.

Основною проблемою безпроводних мереж є те, що вони практично незахищені, адже безпроводні мережі використовують радіосигнал з чітко визначеним набором характеристик, тому будь-хто при певних затратах часу та сил зможе з легкістю знайти спосіб перехопити та прочитати дані, що в них містяться.

Цю проблему досить важко вирішити, навіть використовуючи допоміжні засоби захисту в поєднанні з протоколами безпеки WEP, WPA та WPA2. Використовуючи протокол WEP для захисту мережі, а також прихований SSID (набір основних служб), захищеність мережі від несанкціонованого доступу практично рівна нулю, адже даний захист мережі, використовуючи спеціалізоване програмне забезпечення, може бути зламаний до десяти хвилин без будь-яких зусиль.

Протоколи захисту WPA та WPA2 практично ідентичні між собою, проте відрізняються підтримуваними типом шифрування. У порівнянні із попереднім протоколом WEP, у даних протоколів змінено саму систему аутентифікації користувача, а також використовується більш складне шифрування даних. Проте WPA та WPA2 також не захищають мережі на максимальному рівні, але розшифрування паролльної фрази може зайняти як від кількох секунд, так до кількох сотень років. Це все залежить від вмісту символів (цифр, букв нижнього та верхнього регістрів, символів) у паролльній фразі.

Отже, для того щоб покращити рівень безпеки безпроводної мережі із використанням протоколів WEP, WPA та WPA2 потрібно використовувати допоміжні засоби захисту, тобто включати функцію фільтрації підключених клієнтів по унікальному MAC адресу, приховувати від відображення SSID, а також використовувати довгі та складні паролльні фрази, які б містили набір невпорядкованих букв великого та малого регістру, цифри та різного роду символи.