## Секція 6. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В БІЗНЕСІ

### МЕХАНІЗМИ ЗАХИСТУ WI-FI МЕРЕЖ

**Байдікова К.І., гр. БА-51м**
Науковий керівник – канд. екон. наук, доц. **Мілаш І.В.**
Харківський державний університет харчування та торгівлі

За останні роки бездротові мережі отримали широке поширення. І якщо раніше мова йшла переважно про використання бездротових мереж в офісах, то тепер вони широко використовуються як в домашніх умовах, так і для розгортання мобільних офісів. Однак, приймаючи рішення про перехід до бездротової мережі, не варто забувати, що на сьогоднішньому етапі їх розвитку вони мають одне вразливе місце. Мова йде про безпеку бездротових мереж. Проблема бездротових мереж зараз стоїть досить гостро. Останнім часом почастішали випадки злому wi-fi мереж. Це пов'язано в першу чергу з наростаючою популярністю бездротових мереж.

Основним стандартом при побудові даного виду мереж є стандарт 802.11. Цей стандарт для бездротових мереж передбачає кілька механізмів забезпечення безпеки мережі. Серед них поширені:

– Wired Equivalent Protocol, або WEP, розроблених автором стандарту 802.11; основна функція WEP – шифрування даних при передачі та запобігання неавторизованого доступу в бездротову мережу; для шифрування WEP використовує алгоритм RC4.

– WEP 2.0 – представлений в 2001 р. після виявлення безлічі дірок в першій версії, WEP 2 має поліпшений механізм шифрування і підтримку Kerberos V.

– Open System Authentication – система аутентифікації за замовчанням, яка використовується в протоколі 802.11. Власне системи як такої немає – аутентифікацію проходить будь-який, хто запитує; у разі застосування OSA не допомагає навіть WEP, так як в ході експериментів було з'ясовано, що пакет аутентифікації надсилається не зашифрованим.

– Access Control List – в протоколі не описується, але використовується багатьма як доповнення до стандартних методів. Основа такого методу – клієнтська MAC-адреса, унікальна для кожної картки; точка доступу обмежує доступ до мережі відповідно до свого списку MAC-адрес.

– Closed Network Access Control – адміністратор дозволяє будь-якому користувачеві приєднуватися до мережі, або в неї може увійти тільки той, хто знає її ім'я, SSID; мережеве ім'я в такому випадку служить секретним ключем.