УДК 004.722
Николин В. – ст. гр. КСМзм-51
*Тернопільський національний економічний університет*

# ЗАСОБИ ЗАХИСТУ БЕЗПРОВІДНИХ МЕРЕЖ СТАНДАРТУ 802.11

Науковий керівник: к.е.н, доцент Тимошенко Л.М.

Традиційно в наший країні найбільший інтерес до технологій безпровідного доступу (особливо широкосмугового) проявляють оператори мобільного зв'язку і провайдери Інтернету. Використанню безпровідних систем для корпоративних потреб приділяється значно менше уваги, хоча саме цей сегмент замовників є сьогодні одним з основних споживачів подібних рішень. Широке розповсюдження безпровідного доступу пояснюється швидкістю і якістю розгортанням інформаційної або технологічної мережі.

Інформаційна безпека безпровідної мережі завжди викликає занепокоєння в існуючих і потенційних користувачів, оскільки, на відміну від кабелю, захищеного від зовнішнього доступу, радіоефір доступний для "прослуховування".

Вирішити проблему безпеки у безпровідних мережах повинен був допомогти алгоритм WEP, що одержав широке поширення в серійних безпровідних пристроях стандарту 802.11. Цей алгоритм виявився уразливим для різного роду атак і не забезпечує достатньої надійності. Йому на зміну приходять стандарти IEEE 802.11i і WPA від Wi-Fi Alliance. В стандарті WPA передбачене використання протоколів захисту 802.1x, EAP, TKIP і RADIUS. Механізм аутентифікації користувачів заснований на протоколах 802.1x і EAP. Визначений за замовчуванням у стандарті IEEE 802.11i механізм забезпечення конфіденційності даних заснований на блоковому шифрі стандарту AES.

Коло потенційних проблем безпеки при експлуатації мережі зводиться до 3-х основних:

1. зловмисник може несанкціоновано підключитися до мережі з метою одержання доступу й крадіжки трафіка Інтернет;
2. прослуховування ефіру з метою крадіжки зловмисником важливої приватної інформації;
3. прослуховування ефіру й підміна "на льоту" переданих даних з певною метою.

Відповідно до специфіки організації безпровідної мережі виділяють наступні атаки: „людина посередині” і розміщення фальшивих точок доступу, атаки на системи аутентифікації, атаки на віртуальні приватні мережі, DoS атаки. Тому актуальними є наступні задачі: моніторинг мережі і реакція на події, аудит безпеки і стійкості мережі, забезпечення безпеки фізичного рівня, безпечне розміщення безпровідної мережі і віртуальної локальної мережі, удосконалення протоколів аутентифікації.

В даній роботі проведено аналіз структури існуючих засобів захисту безпровідних мереж, здійснено аналіз стійкості застосованих протоколів до різних типів атак. Проаналізовано стійкість протоколів аутентифікації та шифрування. В експериментальній частині наведено порівняння протоколів забезпечення безпеки фізичного рівня.