**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

# КВАЛІФІКАЦІЙНА РОБОТА

## на тему: «Удосконалення методів захисту WI-FI мереж від зовнішніх загроз»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

(підпис) Богдан ЧИРВА (Ім'я, ПРІЗВИЩЕ)

Виконав: здобувач вищої освіти
групи АРДМ-62
Богдан ЧИРВА

Керівник: Анатолій МАКАРЕНКО

Рецензент: О. Ткаленко

Київ –2023

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**

**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут телекомунікацій**

Кафедра Мобільних та відеоінформаційних технологій

Ступінь вищої освіти Магістр

Спеціальність 172 Телекомунікації та радіотехніка

Освітньо-професійна програма Апаратура радіозв'язку, радіомовлення і телебачення

**ЗАТВЕРДЖУЮ**
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
«» _____ 2023 року

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Чирві Богдану Миколайовичу

1. Тема кваліфікаційної роботи: «Удосконалення методів захисту Wi-Fi мереж від зовнішніх загроз»,
керівник кваліфікаційної роботи Анатолій МАКАРЕНКО, д.т.н., професор,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 19.10.2023 р. №145.

2. Строк подання кваліфікаційної роботи 25.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Теоретичні засади методів захисту Wi-Fi мереж.
   2. Діагностика захисту Wi-Fi мережі із застосуванням технологій WPA та WPA2.
   3. Шляхи вдосконалення методів захисту.
   4. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Вступ.
   2. Теоретичні засади методів захисту Wi-Fi мереж.
   3. Шляхи вдосконалення методів захисту.
   4. Висновки

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів магістерської роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Підбір науково-технічної літератури | 19.10.23 | Викон. |
| 2. | WI-FI мережі та методи їх захисту | 31.10.23 | Викон. |
| 3. | Дослідження технологій WPA та WPA2 для захисту WI-FI мережі | 15.11.23 | Викон. |
| 4. | Проблеми та напрямки їх вирішення у бездротових локальних мережах WI-FI | 29.11.23 | Викон. |
| 5. | Висновки, вступ, реферат | 11.12.23 | Викон. |
| 6. | Розробка презентації | 18.12.23 | Викон. |

**Здобувач вищої освіти** Богдан ЧИРВА

*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**Керівник кваліфікаційної роботи** Анатолій МАКАРЕНКО

*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**ВІДГУК РЕЦЕНЗЕНТА**
на кваліфікаційну магістерську роботу

здобувача вищої освіти Чирви Богдана Миколайовича

на тему:«Удосконалення методів захисту WI-FI мереж від зовнішніх загроз»

**Актуальність:**

Актуальність теми магістерської роботи зумовлена динамічним розвитком цифрових технологій і постійним зростанням кількості кібератак. У сучасному цифровому світі, де з'являється все більше пристроїв, підключених до Wi-Fi, важливість надійного захисту мережі не може бути переоцінена. Зловмисники використовують все більш витончені методи для проникнення в мережі,що ставить під загрозу конфіденційність і безпеку даних.

Тому розробка новітніх методів захисту Wi-Fi мереж є ключовою для забезпечення безпеки як індивідуальних користувачів,так і організацій різного рівня.

**Позитивні сторони:**

1. Зміст магістерської роботи відповідає завданню. Її автор, показав високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.

2. Текст викладений грамотно, ясно, послідовно. Графічний матеріал оформлений якісно. Широко використовується сучасна науково-технічна література, включаючи англомовні видання.

**Недоліки:**

1. В роботі занадто багато уваги приділено теоретичним WPA за технологією 802.11.

2. Потребують більш ширшого пояснення запропоновані шляхи вдосконалення методів захисту.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

**Висновок:**кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач ЧИРВА Богдан Миколайович заслуговує присвоєння кваліфікації: «Магістр з телекомунікацій та радіотехніки».

**Рецензент:** к.т.н., доц. каф. ПЗЗАС _____ Оксана ТКАЛЕНКО
*(науковий ступінь, вчене звання)* *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут телекомунікацій**

**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**
**на здобуття освітнього ступеня магістра**

Направляється здобувач Чирва Б.М. до захисту кваліфікаційної роботи
*(прізвище та ініціали)*

за спеціальністю 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Удосконалення методів захисту WI-FI мереж від зовнішніх загроз

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

**Висновок керівника кваліфікаційної роботи**

Здобувач Чирва Богдан Миколайович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з технологіями захисту бездротових мереж, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Чирви Богдана Миколайовича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з телекомунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Анатолій МАКАРЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2023 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута.Здобувач Чирва Б.М.
*(прізвище та ініціали)*

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2023 року

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 93 стор., 25 рис., 11 табл., 25 дж.

*Мета роботи* – обґрунтування науково-теоретичних засад захисту Wi-Fi мереж, його діагностика із застосуванням технологій WPA та WPA2 та виявлення напрямків його вдосконалення.

*Об'єкт дослідження* – Wi-Fi мережі та методи їх захисту на основі технологій WPA та WPA2.

*Предмет дослідження* – науково-теоретичні положення і система технічних підходів відносно захисту Wi-Fi мережі.

*Короткий зміст роботи*: У роботі був проведений аналіз сучасних протоколів безпеки Wi-Fi мереж. Виділені основні переваги та недоліки використання сучасних протоколів для організації захищених бездротових мереж. Розглянуто сучасні методи атак на бездротові точки доступу та перехоплення даних в них. Досліджено вимоги до налаштувань бездротових мереж стандарту IEEE 802.11,які потрібні для створення комплекса протидії зловмисникам. В даний час існують різні способи захисту Wi-Fi мереж які були розглянуті і опираючись на які було проаналізовано сучасний та актуальний комплекс наявних методів для забезпечення максимального захисту бездротових точок доступу Wi-Fi.

*КЛЮЧОВІ СЛОВА:* ЗАХИСТ ІНФОРМАЦІЇ, КОМП'ЮТЕРНА МЕРЕЖА, WI-FI МЕРЕЖА, АУТЕНТИФІКАЦІЯ, СТАНДАРТ IEEE 802.11, МЕТОДИ ЗАХИСТУ, КІБЕРБЕЗПЕКА, СИСТЕМА-ПРИМАНКА, ОЦІНКА ЗАХИЩЕНОСТІ.

## ABSTRACT

Text part of the master's qualification work: 93 pages, 25 pictures, 11 table, 25 sources.

*The purpose of the work* - substantiation of the scientific and theoretical foundations of Wi-Fi network protection, its diagnosis using WPA and WPA2 technologies, and identification of directions for its improvement.

*Object of research* – Wi-Fi networks and their protection methods based on WPA and WPA2 technologies.

*Subject of research* – scientific and theoretical provisions and a system of technical approaches regarding Wi-Fi network protection.

*Summary of the work:* The paper analyzed modern security protocols of Wi-Fi networks. The main advantages and disadvantages of using modern protocols for the organization of secure wireless networks are highlighted. Modern methods of attacks on wireless access points and interception of data in them are considered. The requirements for wireless network settings of the IEEE 802.11 standard, which are required for the creation of a complex against intruders, have been studied. Currently, there are various methods of protecting Wi-Fi networks, which were considered and based on which a modern and relevant set of available methods was analyzed to ensure maximum protection of wireless Wi-Fi access points.



*KEYWORDS:* INFORMATION SECURITY, COMPUTER NETWORK, WI-FI NETWORK, AUTHENTICATION, IEEE 802.11 STANDARD, PROTECTION METHODS, CYBER SECURITY, BAIT SYSTEM, SECURITY ASSESSMENT.

**ЗМІСТ**

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ..... 9
ВСТУП ..... 10
1. ТЕОРЕТИЧНІ ЗАСАДИ МЕТОДІВ ЗАХИСТУ WI-FI МЕРЕЖ ..... 11
1.1 Сутність захисту Wi-Fi мереж та їх специфіка ..... 11
1.2 Класифікація методів захисту Wi-Fi мереж ..... 18
1.3 Еволюція розвитку безпроводових технологій Wi-Fi ..... 30
2. ДІАГНОСТИКА ЗАХИСТУ WI-FI МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ WPA ТА WPA2 ..... 37
2.1 Механізм захисту Wi-Fi мережі при використанні технологій WPA та WPA2 ..... 37
2.2 Аналіз протоколу шифрування в технологіях WPA та WPA2 ..... 42
2.3 Оцінка параметрів методу автентифікації WPA та WPA2 для системі мереж стандарту ..... 45
2.4 Заміри швидкості перебору ключів за словником ..... 53
2.5 Відсоткове співвідношення кількості символів у словниках ..... 55
3. ШЛЯХИ ВДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ ..... 64
3.1 Проблеми та напрямки їх вирішення у бездротових ..... 64
локальних мережах Wi-Fi ..... 64
3.2 Кількість точок доступу з різними видами шифрування ..... 65
3.3 Шифрування точок доступу за виробником ..... 67
3.4 Розподіл точок доступу за назвами ..... 70
3.5 Сучасні альтернативні методи захисту ..... 73
ВИСНОВКИ ..... 87
ПЕРЕЛІК ПОСИЛАНЬ ..... 90
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ ..... 93

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

| | | |
|---|---|---|
| Wi-Fi | Wireless Fidelity | Бездротова правдивість відтворення |
| SSID | Service Set Identifier | Ідентифікатор мережі |
| DSSS | Direct Sequence Spread Spectrum | Розширений спектр прямої послідовності |
| FHSS | Frequency Hopping Spread Spectrum | Розширений спектр зі стрибками частоти |
| IEEE | Institute of Electrical and Electronics Engineers | Інститут інженерів з електротехніки та електроніки |
| CSMA / CA | Carrier Sense Multiple Access/Collision Avoidance | Багаторазовийдоступізсистемою Carrier Sense / Collision Avoidance |
| AP | AccessPoint | Точка доступу |
| WPS | Wi-Fi Protected Setup | Захищене налаштування Wi-Fi |
| WLAN | Wireless Local Area Network | Бездротова локальна мережа |
| WPA | Wi-FiProtectedAccess | Захищений доступ до Wi-Fi |
| EAP | Extensible Authentication Protocol | Розширюваний протокол автентифікації |
| VPN | Virtual Private Network | Віртуальна приватна мережа |
| DDoS-атака | Distributed Denial of Service attack | Розподілена атака на відмову в обслуговуванні |
| WEP | Wired Equivalent Privacy | стандарт безпеки для бездротової мережі Wi-Fi |
| KRACK | Key Reinstallation Attacks | Атака з перевстановлення ключа |
| БЛОМ | | Бездротові локальні обчислювальні мережі |

# ВСТУП

В наші часи бездротові локальні обчислювальні мережі (БЛОМ) набувають надзвичайної популярності в усіх сферах життя суспільства. З поширеністю доступності бездротових локальних мереж зростає необхідність забезпечення необхідного рівня їх захисту. Це пояснює постійне вдосконалення протоколів захисту, що затверджуються організаціями в якості стандартів для обов'язкового використання в апаратних засобах та програмному забезпеченні при побудові бездротових локальних мереж. Зокрема для популярного стандарту бездротового зв'язку передачі даних, що об'єднує декілька протоколів та ґрунтується на сімействі стандартів IEEE 802.11, більш відомого під торговою маркою Wi-Fi, існує декілька протоколів безпеки, затверджених у різні роки. Поширення бездротових мереж у світі почалося з впровадження технології 802.11, яка в свою чергу трансформувалася у802.11b, далі у 802.11g(a), і, нарешті, у 802.11n, яка є останньою розробкою. Оскільки середовище передачі у бездротових мережах відкрите (для отримання доступу до мережі потрібно мати лише клієнтський адаптер), дуже важливо організувати захист такої мережі від несанкціонованого доступу.

Wi-Fi був створений в 1998 році в лабораторії радіоастрономії CSIRO (Commonwealth Scientific and Industrial Research Organisation) в Канберрі, Австралія. Творцем бездротового протоколу обміну даними є інженер Джон О'Салліван.

# 1. ТЕОРЕТИЧНІ ЗАСАДИ МЕТОДІВ ЗАХИСТУ WI-FI МЕРЕЖ

## 1.1 Сутність захисту Wi-Fi мереж та їх специфіка

Середовище передачі у мереж стандарту 802.11 бездротове, але воно має межі для приймання клієнтським обладнанням, що зумовлено згасанням сигналуу вільному просторі. Отже, очевидно, що для успішного доступу до мережі зловмисник повинен бути в радіусі поширення сигналу цієї мережі. Є декілька способів протистояти поширенню радіосигналу. Можна використати так звану "зону, що охороняється", тобто весь радіус покриття точки доступу охороняється, наприклад, територія огороджена парканом. Такий спосіб дає змогу запобігти випадковому виявленню мережі, але він не допоможе при цілеспрямованому скануванні території направленою антеною. Якщо сигнал не повинен виходити за межі певної будівлі, можна використати екранування стін металевою сіткою, що значно послабить рівень сигналу. Найпростішим методом для звичайного користувача точки доступу, який використовує ресурси бездротової мережі у власних цілях, є звичайне зменшення рівня вихідного сигналу. Таку функцію на даний момент підтримують більшість точок доступу. При цьому користувач може впевнено користуватися ресурсами мережі лише у радіусі, який є меншим при меншому рівні сигналу. Ще одним способом називають приховування імені точки доступу (ESSID cloaking), але ця методика не допомагає у реальних умовах, оскільки точку можна визначити за активним спілкуванням з клієнтами. Сучасне програмне забезпечення ідентифікує таку точку доступу у режимі зазамовчуванням. [2].

Проблема безпеки мереж Wi-Fi з початку момента їх появи являється однією з найскладніших. Безпека Wi-Fi мережі – це два основних питання: конфіденційність даних інформації, а також захист від несанкціонованого доступу. Стовідсотково вирішити дані проблеми неможливо, але розробники мережевого обладнання та розробники програмного забезпечення приділяють велику увагу цій проблемі. На даний момент є достатньо необхідних

технічних засобів які призначені для того щоб запобігти злому або ускладнити злом бездротових точок доступу. Більшість бездротових мереж в яких встановлено стандартні параметри захисту мають достатній ризик бути зламаними. Крім того, проникнути в бездротову Wi-Fi мережу значно простіше, ніж в звичайну, немає необхідності підключатися до проводів, достатньо знаходитись в зоні прийому сигналу. Небезпечно підключати незахищену бездротову мережу до кабельноїмережі.

Незахищена точка доступу, під'єднана до локальної мережі, являє собою можливість злому для зловмисників. Для підприємств це загрожує тим, що конкуренти можуть отримати доступ до конфіденційних документів. Незахищені бездротові мережі дозволяють хакерам обійти міжмережеві екрани і налаштування безпеки, які захищають мережу від атак через мережу Internet. Хочадля забезпечення безпеки Wi-Fi-мереж можуть застосовуватись складні математично алгоритмічні аутентифікаційні моделі шифрування даних і контролю цілісності їх при передачі, але тим не менш, вірогідність доступу до інформації сторонніх осіб є дуже великою. У випадку якщо для мережі не приділити певної уваги зловмисник зможе: отримати доступ до ресурсів і дисків користувачів Wi-Fi-мережі, сканувати трафік, мати доступ до конфіденційної інформації, змінювати в мережі інформацію, використати інтернет-трафік, атакувати комп'ютери користувачів і сервери мережі, створювати підроблені точки доступу, розсилати спам або здійснювати інші протиправні дії від імені мережі яка зламана.

Поширеність бездротових мереж і доступність обладнання для їх організації породжує проблему їх безпеки. Дійсно, у багатьох пристроях доступу використовуються SSID і інші налаштування за замовчуванням: не вибраний оптимальний метод ідентифікації користувачів і існує ще маса можливостей для несанкціонованого доступу до даних, що передаються. Для забезпечення безпеки бездротових мереж, перш за все необхідно встановити, що може їм загрожувати. Перехоплення сигналів бездротової мережі аналогічне прослуховуванні радіопередач. Досить мати ноутбук або

смартфон і аналізатор бездротових протоколів. Широко поширена помилка, що несанкціоноване підключення до бездротової мережі поза офісом можна припинити, контролюючи вихідну потужність сигналу. Це не так, оскільки використання зловмисником бездротової карти підвищеної чутливості і спрямованої антени дозволяє легко це подолати. Навіть зменшивши вірогідність несанкціонованого підключення до мережі, не слід залишати без уваги можливість сканування трафіку, тому для безпечної роботи в бездротових мережах необхідно шифрувати передану інформацію.

Одним із способів авторизації користувачів у бездротовій мережі є фільтрація по MAC ідентифікатору. Кожний бездротовий адаптер має свій унікальний фізичний ідентифікатор, який встановлюється на заводі. При первинному підключенні до точки доступу адміністратор повинен додати такий ідентифікатор клієнта у спеціальний список точки доступу. Такий список зберігається на точці доступу. При підключенні будь-якого клієнта точка доступу перевіряє його фізичний ідентифікатор шляхом пошуку його у спеціальному списку ідентифікаторів. Якщо ідентифікатор знайдено, то точка доступу починає обслуговувати клієнта, якщо ж ні- просто ігнорує його. Недоліком такого способу захисту є можливість зміни фізичного ідентифікатора на сучасних клієнтських адаптерах. Дізнатися фізичний ідентифікатор іншого користувача також не є проблемою - для цього існує спеціальне програмне забезпечення, яке дозволяє прослуховувати ефір та ідентифікувати окремих користувачів. [7].

Важливо відзначити, що вказані методи не забезпечують конфіденційність даних, що передаються в мережі, вони просто обмежують доступ до мережі.Тобто, навіть якщо всі ці засоби включені на точці доступу, зловмисник зможе, включивши свій бездротової адаптер в режимі dmonitor modet, слухати ефір і виловлювати всю передану інформацію.

Очевидно, що для захисту мережі потрібно активізувати механізм захисту, що вбудований у обладнання, яке надає сервіс бездротових мереж. На данийомент налаштування захисту обладнання бездротових мереж вимагає

введення паролю. В деяких випадках (наприклад, недосвідчений користувач) пароль може бути найбільш вразливим місцем всієї системи. Все обладнання завжди має певні налаштування за замовчуванням. Інформація про ці налаштування повинна знаходитись у інструкції до цього обладнання. Іншими словами, така інформація є загальновідомою. Якщо користувач не змінить налаштування пароля для точки доступу, зловмисник зможе легко підібрати пароль і отримати доступ до всієї мережі. Також важливим фактором є складність паролю. Загальновідомо, що чим довший і складніший пароль, тим вищу він має криптостійкість, і для його підбору потрібно більше часу. Тому рекомендується використовувати випадково згенеровані паролі достатньої довжини. Рекомендується також змінювати пароль через певні проміжки часу. [3].

Підключення бездротових систем зв'язку на даний момент не потребує ліцензії, якщо вони не несуть комерційного призначення та знаходяться всередині приміщення. Характеристики дозволених передавачів: антена з коефіцієнтом підсилення до 6 Дб і потужністю сигналу до 500 мВт на частотах 2,4000- 2,4835 ГГц, згідно з рішенням № 914 "Про затвердження Переліку радіоелектронних засобів та випромінювальних пристроїв, для експлуатації яких не потрібні дозволи на експлуатацію" Національної комісії з питань регулювання зв'язку України від 06 вересня 2007).Тому в Україні швидко зростає кількість приватних та комерційних точок бездротового доступу, особливо в його центральній бізнес-частині міста Києва.

На сьогоднішній день, в Україні, кількість користувачів, що виходять в інтернет з мобільних пристроїв перевищила кількість тих, що користуються стаціонарними пристроями. Відповідно зросла і кількість бездротових мереж. При цьому, через відносну простоту розгортки таких мереж, часто це відбувається без залучення спеціалістів, наприклад відкриті точки доступу кафе, ресторанів, кінотеатрів, торгових центрів, тощо. В той же час, як правило, відповідні точки доступу підключаються до локальних мереж закладів та установ, що в сукупностіз некваліфікованим налаштуванням та

адмініструванням дає зростання можливих кіберзагроз в декілька разів. За даними перевірки департаментом кіберполіції близько 75% всіх бездротових мереж Wi-Fi можуть бути успішно атаковані. У кожній другій системі з бездротової мережі можливий доступ до локальної комп'ютерної мережі установ приватного та державного секторів. При цьому способи атак на корпоративні та державні інфраструктури, як і раніше, базуються на використанні поширених загальновідомих вразливостей і недоліків програмного забезпечення. Проведений спеціалістами департаменту аналіз свідчить про те, що уразливості критичного рівня присутні в майже половині інформаційних інфраструктур приватного та державного секторів. Приватні дослідники зазначають, що значну частку таких уразливостей (40%) становлять помилки у налаштуванні програмного забезпечення, помилки у програмному коді (27% систем) та відсутність, або не своєчасність оновлень безпеки (20% систем). Таким чином створення ефективної системи захисту бездротових мереж на основі існуючих методів є актуальним завданням в умовах постійно зростаючої мобільності кінцевих пристроїв. Візуально це наведено в рис.1.1. [1, 2, 3].

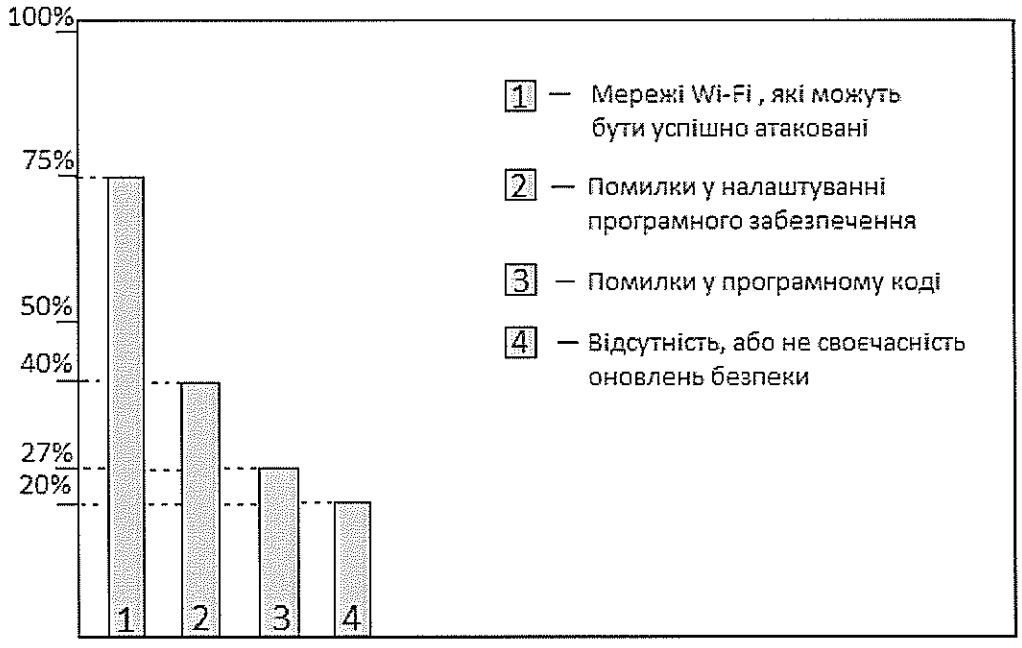



Рис. 1.1. Мережі, що можуть бути атаковані та причини успішних атак

Бездротові мережі Wi-Fi відрізняються від кабельних мереж на фізичному (Phy) і частково на канальному (MAC) рівнях моделі взаємодії OSI. Фізичним рівнем Wi-Fi є радіоканал, що характеризує параметри фізичного середовища передавання даних. У стандарті IEEE 802. llx використано два методи передавання сигналу інформації, що відрізняються за способом модуляції, але використовують однакову технологію розширення спектра, а саме: прямоїпослідовності (DSSS - Direct Sequence Spread Spectrum); частотних стрибків (FHSS - Frequency Hopping Spread Spectrum). Канальний рівень здійснює управління доступом до середовища передавання та забезпечує пересилання кадрів між будь-якими двома пристроями бездротової мережі. На канальному рівні в Wi-Fi мережі у підрівні MAC використано напівдуплексний режим передавання даних. Як методи доступу до середовища передавання даних використано методи множинного доступу з контролем несучої інформації і попередженням колізій або зіткнень (CSMA / CA - Carrier Sense Multiple Access / Collision Avoidance).

Бездротова мережа Wi-Fi може працювати в двох режимах: режим клієнт/сервер, що характеризується наявністю як мінімум однієї точки доступу AP(AccessPoint) та певною кількістю 100 кінцевих станцій; режим точка-точка, де зв'язок між станціями встановлено напряму без реалізації спеціальних точок доступу. [11, 6].

Технологія бездротової передачі даних має такі переваги:

- Можливість розгортання мережі без використання фізичного кабелю зв'язку, що зменшує вартість організації та подальшого розширення мережі, а також важливо в місцях, де відсутня можливість прокладання кабелю;
- Надання доступу до локальної мережі та мережі Інтернет через використання різних мобільних пристроїв, зокрема комп'ютерів та ноутбуків;
- Широке поширення на ринку Wi-Fi-пристроїв, а також їх гарантована сумісність завдяки обов'язковій сертифікації обладнання Wi-FiAlliance;
- Низький рівень випромінювання Wi-Fi-пристроями в момент передавання даних (у 10 разів менше, ніж у мобільного телефону). Мобільність (легко переносити старі і додавати нові робочі місця,свобода переміщення при

використанні ноутбуків або інших мобільних пристроїв, можна встановлювати мережеві пристрої загального користування, наприклад принтери);

- Легкість розширення мережі;
- Сумісність дротових і бездротових мереж;
- Швидкість обміну;
- Безпека (сучасні методи захисту бездротових мереж не поступаютьсядротовим);
- Роумінг (можливість налаштувати вільне пересування в зоні з декількохточок доступу).

Бездротові мережі на базі протоколів IEEE 802.11 мають такі складнощі захисту порівняно з кабельними комп'ютерними мережами: для підключення до бездротової мережі не потрібен фізичний доступ до кабелю мережі, а достатньо перебувати у робочій зоні покриття маршрутизатора з використанням обладнання того типу, на якому побудовано мережу; передача даних по бездротовому каналу може бути перехоплена і оброблена навіть без пристрою доступу, спеціальними апаратними або програмними засобами. Також є труднощі з конфігурацією покриття (важко обмежити роботу Wi-Fi тільки всередині приміщення, тому що не можливо ефективно екранувати всі приміщення, в яких встановлені точкидоступу, тому частково мережі діють і ззовні). Важко обмежити фізичний доступ зловмисників до мережі. [11, 9].

До стандартних заходів захисту належать програмні й апаратні засоби, призначені для вирішення таких завдань: запобігання несанкціонованому підключенню до бездротової мережі сторонніх користувачів; запобігання доступу до заборонених ресурсів вже підключених користувачів; збирання та аналіз інформації у випадку несанкціонованого доступу для запобігання наступному подібному інциденту.

Переважно використовують такі стандартні заходи з підвищення рівня захисту бездротової мережі :

1) Заміна ключів доступу на більш комплексні; зміна протоколів

2) Шифрування на сучасніші і стійкіші до злому методом перебору;

3) Відключення технології WPS; відключення транслювання імені SSID;

4) Включення фільтрації MAC-адрес;

5) Установка програмного забезпечення для протоколювання доступу користувачів до ресурсів усередині мережі.

Необхідно зазначити, що своєчасне оновлення та використання основних пристроїв при побудові WLAN забезпечить підвищення ефективності захисту, адже в них використовуються нові стандарти безпеки WPA та WPA2 (Wi-FiProtectedAccess).

### 1.2 Класифікація методів захисту Wi-Fi мереж

Класифікувати методи захисту можна за різними ознаками, в першу чергу існують методи фізичного, технічного та програмного захисту. В даному дослідженні акцент робиться на останньому, як такому, що найбільше піддається налаштуванню. Що ж стосується методів програмного захисту, вони в свою чергу поділяються на декілька категорій: методи обмеження доступу; методи автентифікації та шифрування. На рис.1.2. зображено класифікація методів захисту мереж. [5].

1. Фільтрування MAC-адрес. Даний метод дозволяє визначити список пристроїв і дозволити лише цим пристроям доступ до вашої мережі WiFi (whitelist), або навпаки заборонити певним пристроям доступ (blacklist). На жаль цей метод ефективний лише в теорії, на практиці такий захист складно налаштовувати і дуже легко обійти. Це одна із функцій маршрутизатора Wi-Fi,яка створює помилкове відчуття безпеки. [15].

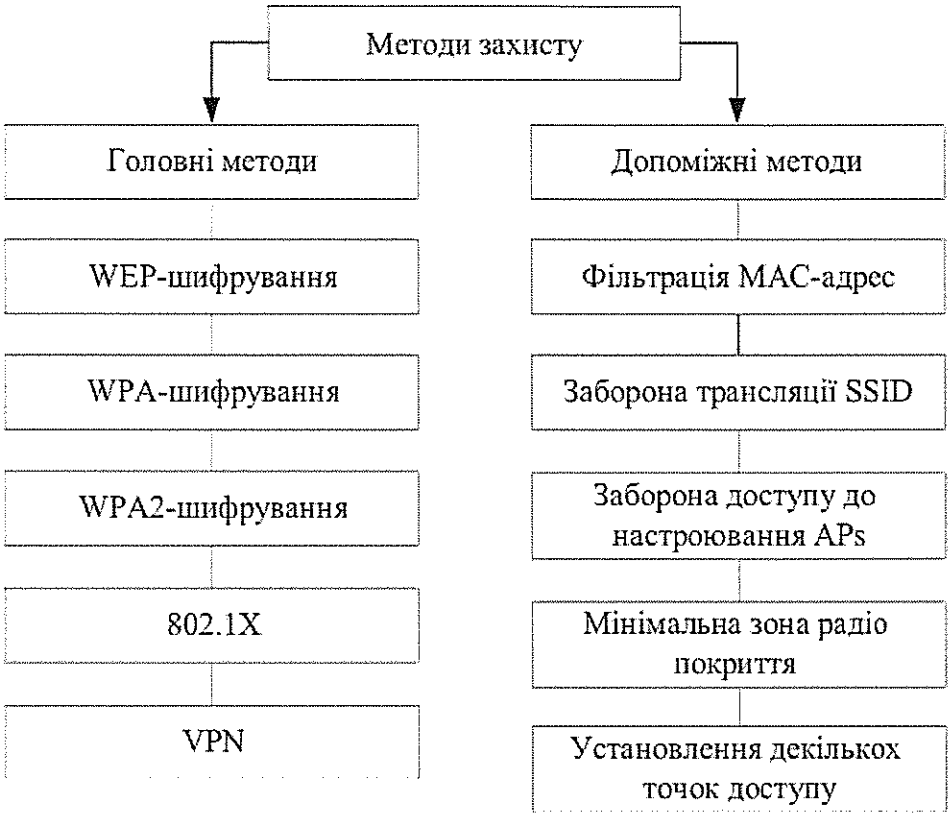



Рис. 1.2. Класифікація методів захисту бездротових локальних мереж

До методів обмеження доступу належать:

Працює цей метод дуже просто, кожен мережевий пристрій має унікальну фізичну адресу (MAC-адресу), яка ідентифікує його в мережі. Як правило, маршрутизатор дозволяє будь-якому пристрою підключатися, якщо він знає відповідну парольну фразу. За допомогою фільтрації MAC-адреси маршрутизатор спочатку порівнює MAC-адресу пристрою з затвердженим списком MAC-адрес і надає пристрою доступ до мережі, лише в разі якщо його MAC-адреса була схвалена. Звучить досить добре, проте MAC-адреси можуть легко підробляти(клонувати) в багатьох операційних системах, тому будь-який пристрій може претендувати на одне з дозволених унікальних MAC-адрес. MAC-адреси також легко отримати. Вони надсилаються по повітрю, коли кожен пакет переходить до пристрою та з нього, оскільки MAC-адреса використовується для того, щоб кожний пакет потрапляв на правильний пристрій. Все що потрібно зловмиснику, це стежити за трафіком Wi-Fi декілька секунд, дослідити пакети, що були передані за цей час, щоб знайти

MAC-адресу дозволеного пристрою, змінитиMAC-адресу свого пристрою на таку дозволену MAC-адресу та підключатися на місце цього пристрою.

Це зробити неможливо, поки довірений пристрій підключений до мережі, але атака "deauth" (деавтентифікація) або "deassoc" (деассоціація), які примусово відключають пристрій від мережі Wi-Fi, дозволить зловмисникові зайняти його місце. Зловмисник з набором інструментів, таких як KaliLinux, може використовувати програму Wireshark для перехоплення пакету, запустити швидку команду для зміни своєї MAC-адреси, використовувати aireplay-ng для надсилання пакетів deassociation для цього клієнта, а потім підключитися на його місце. Цей процес може зайняти менше 30 секунд. І це лише ручний метод, який передбачає виконувати кожен крок вручну - не слід також забувати про автоматизовані інструменти або скрипти, які можуть зробити це швидше. Тож цей метод, хоча і існує, проте не забезпечує ефективного захисту мережі. [2].

2. Режим прихованого SSID (ServiceSetIdentifier). SSID – це ідентифікатор мережі, який за замовченням надсилається маршрутизатором або точкою доступу бездротової мережі у режимі broadcast, тобто усім. Зазвичай точки доступу мережі Wi-Fi надсилають своє мережеве ім'я як один з інформаційних елементів, які входять до деяких кадрів керування, ці елементи,або маяки, з інформаційним елементом, ідентифікатором якого є 0. Ця структура параметрів показана на рис.1.3.

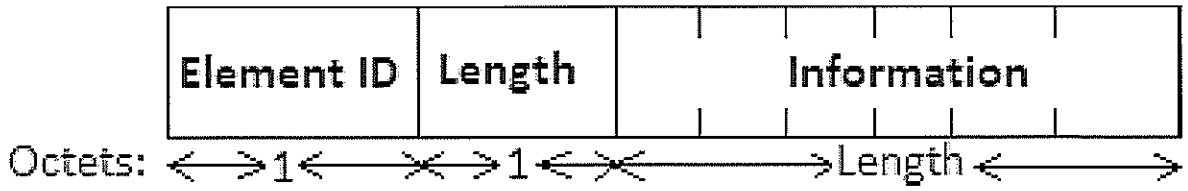



Рис. 1.3. Структура параметрів кадру керування

Ідентифікатор SSID регулярно передається точками радіодоступу в спеціальних фреймах Beacon. Будь-яка приймально-передавальну станцію, що розташована в радіусі дії і підтримує стандарт 802.11, може визначити SSID за допомогою аналізатора трафіку протоколу 802.11. Деякі точки радіодоступу,

в тому числі D-Link, дозволяють адміністративно заборонити трансляцію передачу SSID всередині фреймів Beacon.Однак і в цьому випадку SSID можна легко визначити шляхом захоплення фреймів Probe Response, що посилаються точками радіодоступу. SSID не забезпечує конфіденційність даних, даний ідентифікатор статті не розроблявся для використання в якості механізму забезпечення безпеки. Крім цього, відключення широкомовної передачі SSID точками радіодоступу може серйозно відбитися на сумісності обладнання бездротових мереж різних виробників при використанні в одній бездротовій мережі.

Приховати SSID, тобто припинити його транслювати в ефір, також вважається одним ізметодів захисту. Проте, на нашу думку, це іще один не ефективни і скоріше оманливий метод захисту. За словами одного з фахівців Microsoft, Steve Riley : SSID – це мережеве ім'я, а не пароль. Бездротова мережа має SSID, щоб відрізняти її від інших бездротових мереж поблизу. SSID ніколи нерозроблявся, щоб бути прихованим, і тому не забезпечить вашу мережу будь-якимзахистом, якщо ви намагаєтесь сховати його.

Відповідь на запитання чому вищеописаний метод не є ефективним дуже проста. Дуже легко знайти ідентифікатор "прихованої" мережі - все, що для цього потрібно зробити - це використовувати програму, таку як inSSIDer, NetStumbler або Kismet, щоб короткочасно сканувати ефір та показати всі існуючі мережі в радіусі доступу. [8].

3) Статична IP-адресація. Даний методи захисту полягає у відключені динамічного призначення локальних IP-адрес центральною станцією (маршрутизатором), натомість вимагаючи від користувачів вручну налаштовувати відповідні параметри мережі (адресу, маску, DNS – сервер, шлюз, тощо). Про тецей метод також не э ефективним, адже обійти його може навіть низько кваліфікований зловмисник з мінімальними знаннями про комп'ютерні мереж. До того ж такий спосіб адресації значно ускладнює адміністрування мережі, зокрема в частині додавання нових вузлів, погіршує масштабування мережі, що неприпустимо в бездротових мережах, адже за визначенням вони, навпаки, мають покращувати цей параметр.

Тож вищеописані методи обмеження доступу на сьогодні не є ефективними при побудові системи захисту від кібер загроз бездротових мереж.

Наступна категорія методів захисту, це методи аутентифікації. Основні з них наведені в табл. 1.1.

Стандарт IEEE 802.11 з традиційною безпекою (Tradition Security Network, TSN) передбачає два механізми аутентифікації бездротових клієнтів: відкриту аутентифікацію (Open Authentication) і аутентифікацію із загальним ключем (Shared Key Authentication). Для аутентифікації в бездротових мережах також широко використовуються два інших механізму, які не є частиною стандарту 802.11, а саме - призначення ідентифікатора бездротової локальної мережі (Service Set Identifier, SSID) і аутентифікація клієнта по його MAC-адресу (MAC Address Authentication). [9].

Таблиця 1.1

**Основні методи аутентифікації та їх опис**

| Методи аутентифікації | Опис методу |
|---|---|
| Відкрита автентифікація (Open). | Відкрита автентифікація дозволяє будь-якому бездротовому пристрою автентифікуватись, а потім намагатися встановити зв'язок з точкою доступу. Це не завжди означає, що одразу після автентифікації буденадано доступ до мережі. Після автентифікації може бути запитано пароль, ключову фразу, додаткові ідентифікаційні дані, тощо. Про те такий метод аутентифікації також не захищає мережу і може використовуватись лише на точках доступу, що відділені від основної мережі додатковими засобами захисту, наприклад брандмауером. |

| | |
|---|---|
| Автентифікація зі спільнимключем (WEP, WPA). | Даний метод автентифікації є найпопулярнішим, а його ефективність залежить від стандартузахисту, який використовується для його реалізації. Під час автентифікації за допомогою спільного ключа ключі клієнта та точки доступу повинні співпадати. |

Захист в бездротових мережах забезпечується як за рахунок аутентифікації, так і завдяки шифруванню рис.1.4. Жоден з названих механізмів окремо не здатний забезпечити захист бездротової мережі

У стандарті IEEE 802.1x аутентифікація користувачів на канальному рівні виконується по протоколу EAP. Протокол EAP подібний протоколу CHAP (Challenge Handshake Authentication Protocol - протокол взаємної аутентифікації), який застосовується в PPP (Point to Point Protocol - протокол з'єднання "точка-точка"), він призначений для використання в локальних мережах. EAP є "узагальненим" протоколом в системі аутентифікації, авторизації та обліку (authentication, authorization, and accounting, AAA), що забезпечує роботу різноманітних методів аутентифікації.AAA-клієнт (сервер доступу по термінології AAA в бездротової мережі представлений точкою доступу), що підтримує EAP, може не розуміти конкретних методів, використовуваних клієнтом і мережею в процесі аутентифікації. Сервер доступу тунелює повідомлення протоколу аутентифікації, якими обмінюються клієнт і сервер аутентифікації. Сервер доступу цікавить лише факт початку і закінчення процесу аутентифікації. [12].

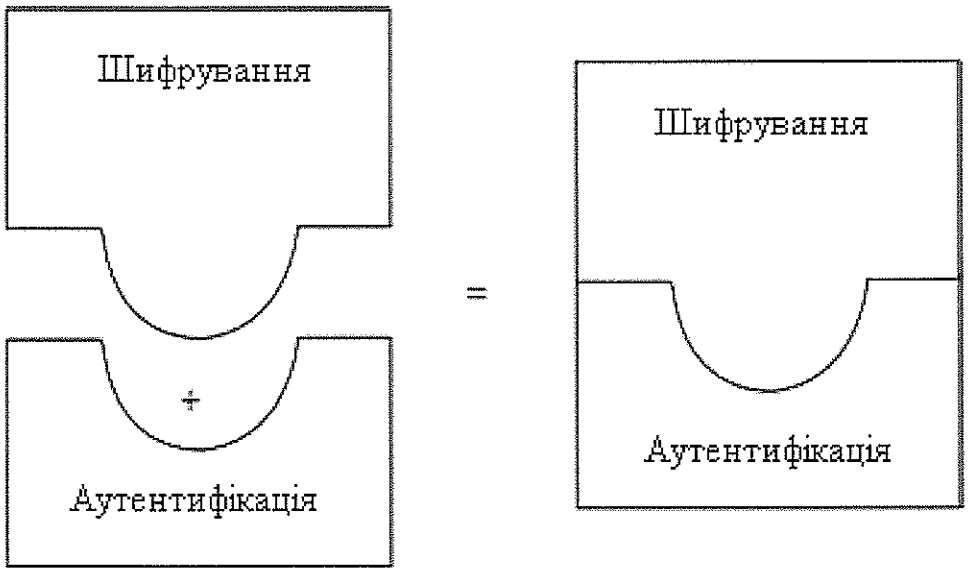



Рис. 1.4.Захист в бездротових мережах забезпечується за рахунок аутентифікації і шифрування

Є кілька варіантів EAP, спроектованих за участю різних компаній-виробників. Така різноманітність вносить додаткові проблеми сумісності, так що вибір відповідного обладнання і програмного забезпечення для бездротової мережі стає непростим завданням. Можливі варіанти EAP при конфігуруванні способу аутентифікації користувачів в бездротової мережі показані в табл. 1.2

Таблиця 1.2

**Варіанти EAP при конфігуруванні способу аутентифікації користувачів**

| Види EAP | Інформація про даний варіант |
|---|---|
| EAP-MD5 | Це обов'язковий рівень EAP, який повинен бути присутнім у всіх реалізаціях стандарту 802.1x, саме він був розроблений першим. З точки зору роботи він дублює протокол CHAP. Протокол EAP-MD5 непідтримує динамічний розподіл ключів. Крім того, він вразливий для атаки "людина посередині" із застосуванням фальшивої точки доступу і для атакина сервер аутентифікації, так як автентифіковані тільки клієнти. І нарешті, в ході аутентифікації |
| | зловмисник може підслухати запит і зашифрованийвідповідь, після чого провести атаку з відомим відкритим або шифрованих текстом. |

| | |
|---|---|
| EAP-TLS (EAP-Transport LayerSecurity - протокол захисту транспортного рівня) | Протокол захисту транспортного рівня) підтримує взаємну аутентифікацію на базі сертифікатів. EAP-TLS заснований на протоколі SSLv3 і вимагає наявності засвідчує центру. Протоколи TLS і SSL використовують ряд елементів інфраструктури PKI(Public Key Infrastructure). Клієнт повинен мати діючий сертифікат, щоб ідентифікувати по відношенню до мережі. AAA-сервер повинен мати діючий сертифікат, щоб ідентифікувати по відношенню до клієнта. Центр сертифікації з супутньою інфраструктурою управляє сертифікатами суб'єктів PKI. Клієнт і RADIUS- сервер повинні підтримувати метод аутентифікаціїEAP-TLS. Точка доступу повинна підтримувати процес аутентифікації в рамках 802.1x / EAP, хоча може і не знати деталей конкретного методу аутентифікації. |
| EAP-LEAP (Lightweight EAP - полегшений EAP) | Був першою (і протягом тривалого часу єдиною) схемою аутентифікації в стандарті IEEE 802.1x, заснованої на паролі. Сервер аутентифікації посилаєклієнту запит, а той повинен повернути пароль, попередньо виконавши його згортку з рядком запиту. Будучи заснований на застосуванні паролів, EAP-LEAP аутентифікує користувача, а не пристрій. У той же час очевидна вразливість цього варіанту для атак методом повного |

| | |
|---|---|
| | перебору і за словником, не характерна для методів<br>аутентифікації із застосуванням сертифікатів. |
| PEAP (Protected EAP - захищенийEAP) і EAP-TTLS (Tunneled Transport Layer Security EAP - протокол захисту транспортного рівня EAP) | Досить популярні і підтримуються виробниками мережевого устаткування, в тому числі D-link. Дляроботи EAP-TTLS потрібно, щоб був<br>сертифікований тільки сервер аутентифікації, а у |
| | претендента сертифіката може і не бути, так що процедура розгортання спрощується. EAP-TTLS підтримує також ряд ранніх методів аутентифікації,в тому числі PAP, CHAP, MS-CHAP, MS-CHAPv2 і навіть EAP-MD5. Щоб забезпечити безпеку при використанні цих методів, EAP-TTLS створює зашифрований по протоколу TLS тунель, усерединіякого ці протоколи і працюють. Протокол Peap дуже схожий на EAP-TTLS, тільки він не підтримуєметоди аутентифікації типу PAP і CHAP.Замість них підтримуються протоколи PEAP-MS-CHAPv2 іPEAP-EAP-TLS, що працюють всередині |

| | |
|---|---|
| | безпечного тунелю. Підтримка Peap реалізована в пакеті програм точок доступу D-link і добре реалізована в найбільш популярних операційних системах персональних комп'ютерів. |

У загальному вигляді схема обміну PEAP зображена на рис.1.5.

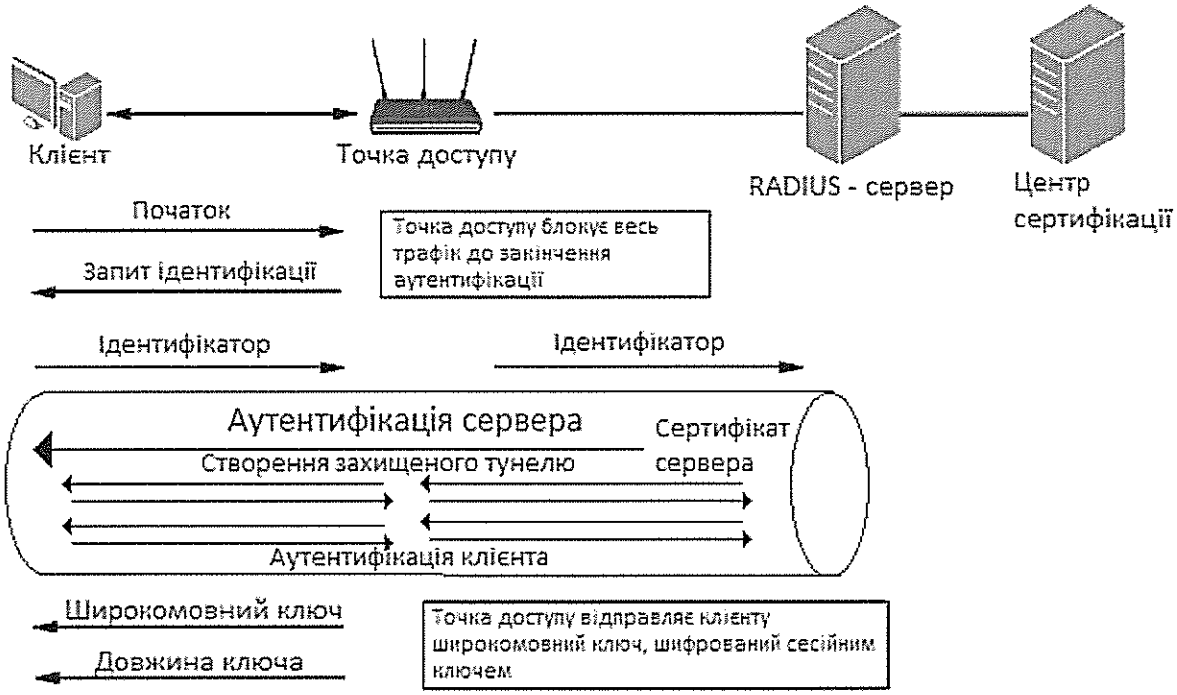



Рис. 1.5. Схема обміну PEAP

Важливу роль у захисті на високому рівні інформації відіграє Віртуальна приватна мережа (VPN). Це метод, що дозволяє скористатися мережевою інфраструктурою загального користування, наприклад мережею Інтернет, для надання віддаленим офісам або окремим користувачам безпечного доступу до локальної мережі організації. Оскільки бездротові мережі 802.11 працюють в неліцензованому діапазоні частот і легкодоступні для випадкового або зловмисного прослуховування, то саме в них розгортання і обслуговування VPN набуває особливої важливості, якщо необхідно забезпечити високий рівень захисту інформації. [10].

Захищати потрібно як з'єднання між хостами через бездротову локальну мережу, так і двоточкові канали між бездротовими мостами. Для забезпечення безпеки особливо секретних даних не можна покладатися на якийсь один механізм або на захист лише одного рівня мережі. У разі двоточкових каналів простіше і економічніше розгорнути VPN, яка покриває дві мережі, ніж реалізовувати захист на базі стандарту IEEE 802.11i включає RADIUS-сервер і базу даних про користувачів.

VPN і технології безпеки бездротових мереж не конкурують, а доповнюють один одного. VPN працює поверх поділюваних мереж загального користування, забезпечуючи в той же час конфіденційність за рахунок спеціальних заходів безпеки та застосування тунельних протоколів, таких як тунельний протокол канального рівня (Layer Two Tunneling Protocol, L2TP).Сенсїх у тому, що, здійснюючи шифрування даних на відправляючому кінці і дешифруванні на приймаючому, протокол організовує тунель, в який не можуть проникнути дані, незашифровані належним чином. Додаткову безпеку може забезпечити шифрування не тільки самих даних, але і мережевих адрес відправника і одержувача. Бездротову локальну мережу можна порівняти з розділяючою мережею загального користування, а в деяких випадках вона такою іє (наприклад, хот-споти). [4, 5].

VPN-мережу не є стійким до DoS- або DDoS-атакам і не може гарантуватидоступність на фізичному рівні просто в силу своєї віртуальної

природи і залежності від нижчих протоколів.

Дві найбільш важливі особливості VPN, особливо в бездротових середовищах, де є лише обмежений контроль над поширенням сигналу - це цілісність і, що ще більш істотно, конфіденційність даних. Припустимо ситуацію, коли зловмисникові вдалося подолати шифрування по протоколу WEP і підключитися до бездротової локальної мережі. Якщо VPN відсутня, то він зможе прослуховувати дані і втручатися в роботу мережі.

Але якщо пакети автентифіковано, то атака "людина посередині" стає практично марною, хоча перехопити дані, як і раніше легко. Включення в VPN елемента шифрування зменшує негативні наслідки перехоплення даних. VPN забезпечує не стільки повну ізоляцію всіх мережевих взаємодій, скільки здійснення таких взаємодій в більш контрольованих умовах з чітко визначеними групами допущених учасників.

## 1.3 Еволюція розвитку безпроводових технологій Wi-Fi

Wi-Fi - це технологія бездротового зв'язку, яка дозволяє підключати пристрої до мережі Інтернет через радіохвилі. Вона зазвичай використовується для підключення комп'ютерів, смартфонів, планшетів, інших пристроїв та роутерів до мережі Інтернет в домашньому оточенні, в офісах, громадських місцях тощо.

Wi-Fi 5 (також відомий як 802.11ac) - це п'яте покоління технології Wi-Fi, яке було вперше впроваджене в 2013 році. Він пропонує значно вищу швидкість передачі даних порівняно з попереднім стандартом Wi-Fi 4 (802.11n).

Основні характеристики Wi-Fi 5 включають в себе:
1. Швидкість: Wi-Fi 5 підтримує швидкості до 3,5 Гбіт/с, що робить його ідеальним для високошвидкісного інтернет-з'єднання та потокового відео.
2. Діапазон: Він працює в частотному діапазоні 5 ГГц, що дозволяє уникати перевантаження інших пристроїв, які працюють в діапазоні 2,4 ГГц, і

покращує зв'язок в областях з великою густотою пристроїв.

3. Технології MIMO: Wi-Fi 5 підтримує технологію MIMO (Multiple Input, Multiple Output), яка дозволяє одночасно передавати та приймати дані з використанням кількох антен, покращуючи стабільність і швидкість підключення.

4. Підтримка більшої кількості одночасних підключень: Wi-Fi 5 дозволяє підключити більше пристроїв одночасно без втрати якості сигналу.

Wi-Fi 6 (або 802.11ax) - це шосте покоління бездротової технології Wi-Fi, яке було розроблене з метою покращення продуктивності та ефективності бездротових мереж.

Основні характеристики Wi-Fi 6 включають в себе:

1. Збільшена швидкість передачі даних: Wi-Fi 6 надає значно більшу швидкість передачі даних порівняно зі стандартами попередніх поколінь. Він може досягати швидкостей до 9,6 Гбіт/с, що робить його ідеальним для завдань, таких як потокове відео 4K та онлайн-ігри.

2. Підтримка багатьох одночасних пристроїв: Wi-Fi 6 впроваджує технологію OFDMA (Orthogonal Frequency Division Multiple Access), яка дозволяє розділяти бездротовий канал на багато менших підканалів. Це дозволяє підключати більше пристроїв одночасно і знижує конфлікти між ними.

3. Покращена ефективність використання смуги пропускання: Wi-Fi 6 використовує технологію BSS Coloring, яка допомагає уникнути перешкод від інших бездротових мереж в одній і тій же області, покращуючи при цьому ефективність передачі даних.

4. Збільшена дальність дії та краща проникність через стіни: Wi-Fi 6 впроваджує технологію Target Wake Time (TWT), яка дозволяє пристроям сплячого режиму включатися у мережу лише тоді, коли це необхідно, що зменшує споживання енергії та підвищує дальність дії сигналу.

Wi-Fi 6 розроблений з урахуванням зростаючого попиту на бездротову

мережу в домашньому оточенні та офісах, а також з урахуванням зростаючої кількості підключених пристроїв, таких як смартфони, планшети, смарт-телевізори, IoT-пристрої та інші. Цей стандарт допомагає вирішити проблеми з перевантаженням мережі і забезпечує кращу продуктивність та якість обслуговування для всіх підключених пристроїв.

В даний час Wi-Fi 7 (або 802.11be) ще не був стандартизований і офіційно не існує. Проте розробники і стандартизаційні органи активно працюють над подальшим розвитком бездротових технологій, і можливо, що в майбутньому буде представлений Wi-Fi 7 або інше подібне покоління Wi-Fi.

Зазвичай кожне нове покоління Wi-Fi створюється з метою покращення продуктивності, швидкості передачі даних, ефективності та забезпечення кращої якості обслуговування для підключених пристроїв. Потенційні покращення Wi-Fi 7 можуть включати в себе ще більше високошвидкісних підключень, збільшену кількість одночасних пристроїв, поліпшену стійкість до перешкод, менше споживання енергії та інші інноваці

Існує безліч методів модуляції, які використовуються для передачі даних через різноманітні комунікаційні канали,але самими поширеними методами модуляції є:

1) Амплітудна модуляція (AM - Amplitude Modulation): В амплітудній модуляції інформація кодується зміною амплітуди несучого сигналу при передачі даних. AM використовується, наприклад, в радіо-трансляції AM.

2) Частотна модуляція (FM - Frequency Modulation): В частотній модуляції інформація кодується зміною частоти несучого сигналу. FM використовується у FM-радіо та інших системах передачі аудіосигналів.

3) Фазова модуляція (PM - Phase Modulation): В фазовій модуляції інформація кодується зміною фази несучого сигналу. PM використовується в різних комунікаційних системах, включаючи деякі цифрові бездротові мережі.

4) Бінарна фазова модуляція (BPSK - Binary Phase Shift Keying): Це вид фазової модуляції, де інформація кодується зміною фази несучого сигналу між двома станими, зазвичай 0 і 180 градусів.

5) Квадратурна амплітудно-фазова модуляція (QAM - Quadrature Amplitude Modulation): QAM комбінує амплітудну і фазову модуляцію, інформація кодується через одночасну зміну як амплітуди, так і фази несучого сигналу. QAM широко використовується у цифрових комунікаціях і телекомунікаціях.

6) Поляризаційна модуляція: В цьому виді модуляції інформація кодується зміною поляризації електромагнітних хвиль. Цей метод використовується в супутниковому зв'язку і оптичних комунікаціях.

7) Амплітудно-фазова модуляція (APSK - Amplitude and Phase Shift Keying): APSK поєднує амплітудну і фазову модуляцію для більш ефективного використання каналу і покращення пропускної спроможності.

8) Упакована модуляція (FSK - Frequency Shift Keying): У цьому методі інформація кодується зміною частоти несучого сигналу між двома або більше частотами.

Кожен з цих методів має як свої переваги так і свої недоліки,може бути оптимальним для певного типу передачі даних.

OFDMA (Orthogonal Frequency Division Multiple Access) - це технологія передачі даних в бездротових комунікаційних системах і мережах, яка поєднує в собі два ключових концепти: OFDM (Orthogonal Frequency Division Multiplexing) та доступ до каналу з багатьма каналами (Multiple Access).

1) OFDM: OFDMA базується на OFDM, яка розділяє широкосмуговий канал на багато вузькосмугових підканалів. Це дозволяє передавати дані на високій швидкості та зменшує вплив мультиплексування на витрату енергії та інтерференцію.

2)Доступ з багатьма каналами: OFDMA дозволяє декільком користувачам одночасно використовувати один і той же канал частоти. Це досягається за допомогою розділення доступу до каналу в часі та частотному домені. Кожному користувачеві відводиться певний підканал і певний час для передачі даних.

3)Множина станцій-абонентів: OFDMA часто використовується в бездротових мережах, таких як Wi-Fi, LTE (Long-Term Evolution), і 5G, для

забезпечення одночасного обслуговування багатьох станцій-абонентів з різними потребами в швидкості передачі даних.

OFDMA дозволяє ефективно використовувати радіочастотний спектр і зменшити вплив інтерференції. Ця технологія є важливою для розвитку швидких та надійних бездротових комунікаційних систем і грає ключову роль у бездротових стандартах, таких як 4G і 5G.

MU-MIMO (Multi-User, Multiple Input, Multiple Output) - це технологія бездротового зв'язку, яка дозволяє точці доступу (AP) або маршрутизатору обслуговувати одночасно кілька користувачів чи пристроїв з використанням багатьох антен (MIMO). Ця технологія представляє собою значний крок у розвитку бездротових мереж, оскільки дозволяє підвищити ефективність та пропускну спроможність мережі.

1) Багатокористувацькість: MU-MIMO дозволяє передавати дані одночасно до кількох користувачів або пристроїв на одній і тій же частоті. Це дуже корисно в обстановках, де багато пристроїв використовують одну точку доступу, наприклад, в домашній мережі або в офісному середовищі.

2) Багатоантенність (MIMO): MU-MIMO використовує багатоантенність на стороні точки доступу та на стороні пристроїв. Це означає, що як точка доступу, так і підключені пристрої мають більше однієї антени для передачі та прийому даних. Це дозволяє збільшити пропускну спроможність та стійкість до перешкод.

3) Збільшення продуктивності: MU-MIMO покращує продуктивність мережі, дозволяючи одночасно передавати дані до кількох пристроїв без зниження швидкості. Це особливо важливо в об'ємних мережах з багатьма пристроями.

MU-MIMO є важливою частиною сучасних бездротових стандартів, таких як 802.11ac (Wi-Fi 5) і 802.11ax (Wi-Fi 6). Вона сприяє покращенню якості обслуговування користувачів і зростанню продуктивності бездротових мереж, особливо в ситуаціях, коли є багато одночасно підключених пристроїв.

Таблиця 1.3

Різниця поколінь Wi-Fi

| | **Wi-Fi 5** | **Wi-Fi 6** | **Wi-Fi 7** |
|---|---|---|---|
| Дата запуску | 2013 | 2019 | 2024 (попередньо) |
| IEEE стандарт | 802.11ac | 802.11ax | 802.11be |
| Максимальна швидкість | 3.5 Гбіт/с | 9.6 Гбіт/с | 46 Гбіт/с |
| Частота | 5 ГГц | 2.4 ГГц,5 ГГц | 2.4 ГГц,5 ГГц, 6 ГГц |
| Ширина каналу | 20,40,80,80+80, 160 МГц | 20,40,80,80+80, 160 МГц | До 320 МГц |
| Модуляція | 256-QAM OFDMA | 1024-QAM OFDMA | 4096-QAM OFDMA (with extensions) |
| MIMO | 4x4 MIMO DL MIMO | 8x8 UL/DL MU-MIMO | 16x16 UL/DL MU-MIMO |
| RU | / | RU | Multi-RUs |
| MAC | / | / | MLO |

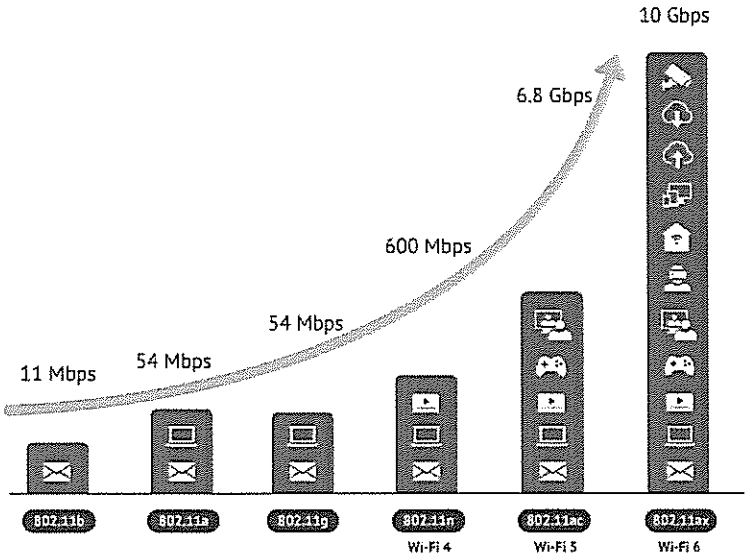



Рис.1.6. Стандарти IEEE

| | 802.11 (Legacy) | 802.11b (Legacy) | 802.11a (Legacy) | 802.11g (Legacy) | 802.11n (HT) | 802.11ac (VHT) | 802.11ax (HE) |
|---|---|---|---|---|---|---|---|
| Year Ratified | 1997 | 1999 | 1999 | 2003 | 2009 | 2014 | 2019 (Expected) |
| Operating Band | 2.4 GHz/IR | 2.4 GHz | 5 GHz | 2.4 GHz | 2.4/5 GHz | 5 GHz | 2.4/5 GHz |
| Channel BW | 20 MHz | 20 MHz | 20 MHz | 20 MHz | 20/40 MHz | 20/40/80/160 MHz | 20/40/80/160 MHz |
| Peak PHY Rate | 2 Mbps | 11 Mbps | 54 Mbps | 54 Mbps | 600 Mbps | 6.8 Gbps | 10 Gbps |
| Link Spectral Efficiency | 0.1 bps/Hz | 0.55 bps/Hz | 2.7 bps/Hz | 2.7 bps/Hz | 15 bps/Hz | 42.5 bps/Hz | 62.5 bps/Hz |
| Max # SU Streams | 1 | 1 | 1 | 1 | 4 | 8 | 8 |
| Max # MU Streams | NA | NA | NA | NA | NA | 4 (DL only) | 8 (UL & DL) |
| Modulation | DSSS, FHSS | DSSS, CCK | OFDM | OFDM | OFDM | OFDM | OFDM, OFDMA |
| Max Constellation / Code Rate | DQPSK | CCK | 64-QAM, 3/4 | 64-QAM, 3/4 | 64-QAM, 5/6 | 256-QAM, 5/6 | 1024-QAM, 5/6 |
| Max # OFDM tones | NA | NA | 64 | 64 | 128 | 512 | 2048 |
| Subcarrier Spacing | NA | NA | 312.5 kHz | 312.5 kHz | 312.5 kHz | 312.5 kHz | 78.125 kHz |

Рис.1.7. Історія та основні характеристики стандартів IEEE

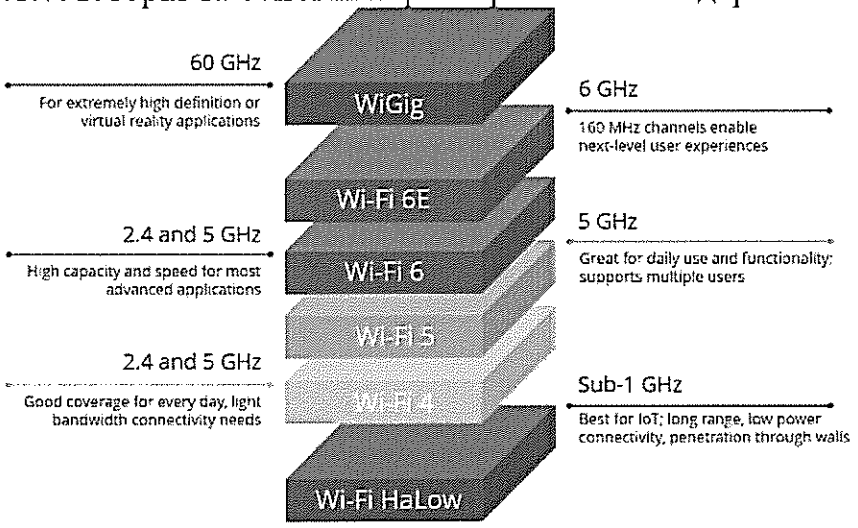



Рис.1.8. Розуміння відмінностей між Wi-Fi HaLow та Wi-Fi

# 2. ДІАГНОСТИКА ЗАХИСТУ WI-FI МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ WPA ТА WPA2

## 2.1 Механізм захисту Wi-Fi мережі при використанні технологій WPA та WPA2

Набір стандартів для комунікації в бездротовій локальній мережевій зоні (WLAN) частотних діапазонів 2.4, 3.6 і 5 ГГц. визначає два типи устаткування: клієнт і точка доступу. Клієнт — комп'ютер з бездротовою мереженою інтерфейсною картою (NetworkInterfaceCard, NIC). Точка доступу (Accesspoint, AP) виконує роль моста між бездротовою і дротовою мережами. Точка доступу звичайно складається з прийомопередатчика, інтерфейсу дротової мережі (802.3),а також програмного забезпечення для обробки даних. В якості бездротової станції може виступати ISA, PCI або PC Card мережева карта в стандарті 802.11, або вбудовані рішення, наприклад, телефонна гарнітура 802.11. [6].

Стандарт IEEE 802.11 визначає два режими роботи мережі: режим "Ad-hoc" (або точка-точка) и клієнт/сервер (або іншими словами режим інфраструктури, infrastructure mode). В режимі клієнт/сервер бездротова мережа складається із мінімум однієї точки доступу, підключеної до дротової мережі, і набору бездротових кінцевих станцій. Така конфігурація називається базовим набором служб (Basic Service Set, BSS). Два або більше BSS з однієї підмережі формують розширений набір служб (Extended Service Set, ESS).

Режим "Ad-hoc" (або незалежний базовий набір служб, IBSS) — це проста мережа, в якій зв'язок між станціями встановлюється напряму без використання спеціальної точки доступу. Такий режим використовується, якщо інфраструктура бездротової мережі на сформована або за якоюсь причиною не може бути сформована.

На фізичному рівні визначено два широкосмугових радіочастотних метода передачі і один в інфрачервоному діапазоні. Радіочастотні методи

працюють в ISM діапазоні 2,4 ГГц і звичайно використовують смугу 83 МГц від 2,400 ГГц до 2,483 ГГц. Технології широкосмугового сигналу в радіочастотних методах збільшують надійність, пропускну спроможність, дозволяють багатьом незв'язаним між собою пристроям працювати в одній частотній смузі з мінімальними перешкодами друг для друга.

Стандарт 802.11 використовує метод прямої послідовності (DirectSequenceSpreadSpectrum, DSSS) та метод частотних скачків (FrequencyHoppingSpreadSpectrum, FHSS). Ці методи кардинально відрізняються і несумісні між собою. [6].

Для модуляції сигналу FHSS використовують технологію FrequencyShiftKeying (FSK). При роботі на швидкості 1 Мбіт/с використовується FSK модуляція за Гаусом другого рівня, а при швидкості 2 Мбіт/с — четвертого. Метод DSSS використовують технологію модуляції PhaseShiftKeying (PSK). При цьому на швидкості 1 Мбіт/с використовується диференційна двійкова PSK, а на швидкості 2 Мбіт/с — диференційна квадратична PSK модуляція.

Заголовки фізичного рівня завжди передаються на швидкості 1 Мбіт/с, а дані можуть передаватися зі швидкостями 1 або 2 Мбіт/с.

Метод DSSS ділить діапазон 2,4 ГГц на 14 каналів, які частково перетинаються. Для того, щоб декілька каналів могли одночасно використовуватися в одному місці, необхідно, щоб вони не перетинались для виключення взаємних перешкод. Таким чином, водному місці можуть одночасно використовуватися максимум 3 канали. Дані пересилаються з використанням одного з цих каналів без перемикання на інші канали. Щоб компенсувати сторонні шуми, використовується 11-ти бітна послідовність Баркера, в якій кожний біт даних користувача перетворюється в 11 біт даних. Така висока надмірність для кожного біта дозволяє значно підвищити надійність передачі, прицьому значно знизивши потужність сигналу. Навіть якщо частина сигналу буде втрачена, він в більшості випадків все рівно буде відновлений, таким чином зменшується кількість повторних подач даних.

Для стандарту IEEE 802.11 кількість доступних каналів в різних країнах різна у зв'язку з різницею в законодавчій базі та правилах ліцензування (наприклад в США доступно тільки 11 каналів). Ширина каналу 802.11b становить 22 МГц (відстані між найближчими каналами становить 25 МГц), а для 802.11g — 20 МГц. В таблиці 2.1 приведено розподіл каналів за частотами, а на рисунку 1 приведено діапазон розподілу каналів для 802.11b. [10].

Таблиця 2.1

**Розподіл каналів за частотами**

| № каналу | Частота, ГГц |
|---|---|
| 1 | 2.412 |
| 2 | 2.417 |
| 3 | 2.422 |
| 4 | 2.427 |
| 5 | 2.432 |
| 6 | 2.437 |
| 7 | 2.442 |
| 8 | 2.447 |
| 9 | 2.452 |
| 10 | 2.457 |
| 11 | 2.462 |
| 12 | 2.467 |
| 13 | 2.472 |
| 14 | 2.484 |

Частота 14-го каналу може інколи відрізнятися від прийнятого в специфікації, наприклад, 2,482 ГГц замість 2,484 ГГц. Зменшується частота, щоб входити у дозволений діапазон, тобто бути меншою за 2,483 ГГц. Такий підхід може призводити до часткового перекриття каналів, але користувач найчастіше непомітить різниці. Це зображено на рис.2.1.

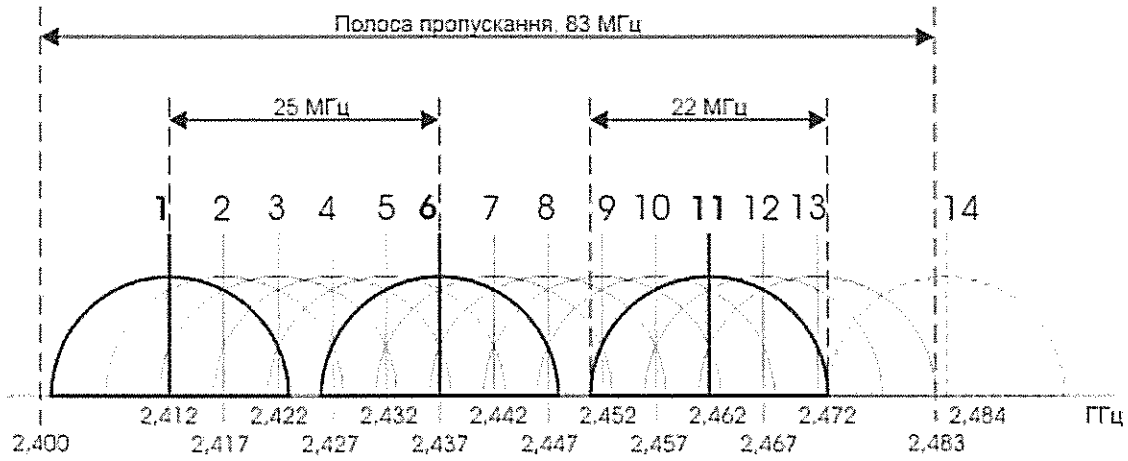



Рис. 2.1. Часткове перекриття каналів в полосі пропускання, 83 МГц

Кожному пристрою апаратно вбудований ідентифікатор, який є індивідуальним для кожного пристрою та називається MAC-адресою (Media Access Control). Схема розподілу MAC-адрес для специфікації IEEE 802 була запропонована компанією Xerox. Використовується 48-бітна адреса (248 можливих варіантів адреси), в якій вказані шістнадцятирічні цифри (як показано на рисунку 2). Використовується кілька роздільників для частин MAC-адреса: дефіс або дві крапки розділяють адресу на шість частин або крапка — на три частини. Наприклад, одну і ту саму адресу можна записати так: [22].

1) 00-11-22-aa-bb-cc;

2) 00:11:22:aa:bb:cc;

3) 0011.22aa.bbcc.

MAC-адреса розділяється на дві частини: з 6-го по 4-й байт — ідентифікація виробника або специфічна інформація та з 3-го по 1-й байт — унікальний номер пристрою. Інформацію про виробника можна отримати з офіційних джерел міжнародної сертифікаційної організації IEEE. Якщо MAC-адреса містить

специфічну інформацію, то 7-й та 8-й біти 6-го байту будуть кодувати ці стани, яксаме наведено на рис.2.2. нижче.

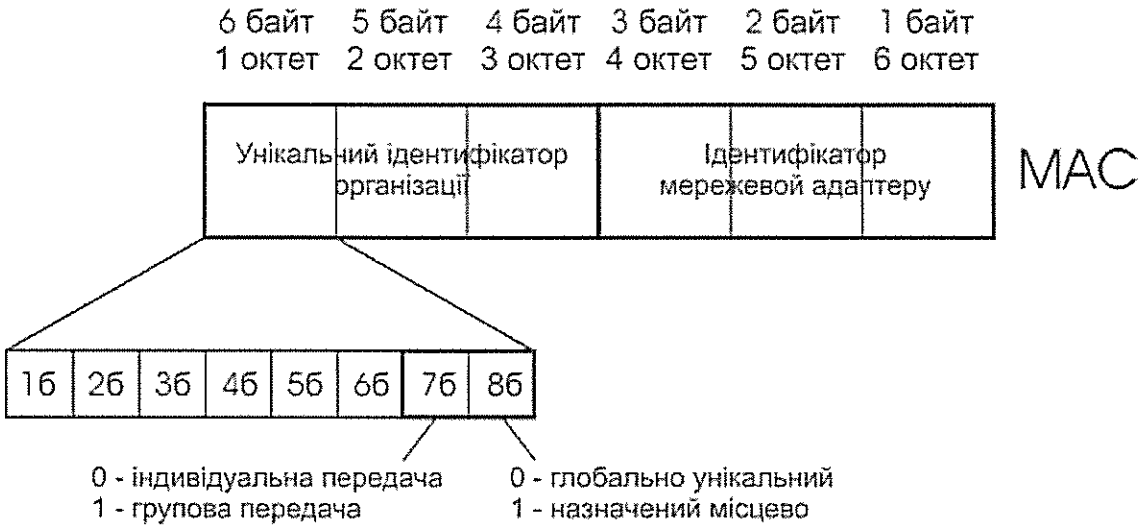



Рис. 2.2. Кодування 7-м та 8-м бітами 6-го байту станів

До інших методів захисту можна віднести:

1. Фільтрація за MAC-адресою (на деяких пристроях можливо задіяти цю функцію і дозволити доступ в мережу для деяких адрес). Це спричиняє додаткову перепону зломщику, хоча і не дуже серйозну, бо MAC-адресу можна підмінити.
2. Приховування SSID (ідентифікатора бездротової мережі). Більшість обладнання дозволяє його приховати, таким чином, при скануванні стандартними утилітами мережу не буде видно. Але і це не дуже серйозна перепона, якщо зломщик використовує більш складний сканер мережі.
3. Заборона доступу до налаштувань точки доступу або роутера через бездротову мережу. Проте це не захистить від перехвату трафіка або від проникнення в мережу. [15].

Процедура WEP-шифрування виглядає наступним чином. Спочатку передані в пакеті дані перевіряються на цілісність (алгоритм CRC-32) для отримання значення контролю цілісності (Integrity Check Value, ICV), який додається в кінець вихідного повідомлення. Далі генерується 24-бітний вектор

ініціалізації (IV), а до нього додається статичний (40 або 104-бітний) секретний ключ. Отриманий таким чином 64 або 128-бітний ключ і є вихідним ключем для генерації псевдовипадкового числа, яке використовується для шифрування даних. Далі дані змішуються (шифруються) за допомогою логічної операції XOR з псевдовипадковою ключовою послідовністю, а вектор ініціалізації додається в службове поле кадру. Це видно на рис.2.3.

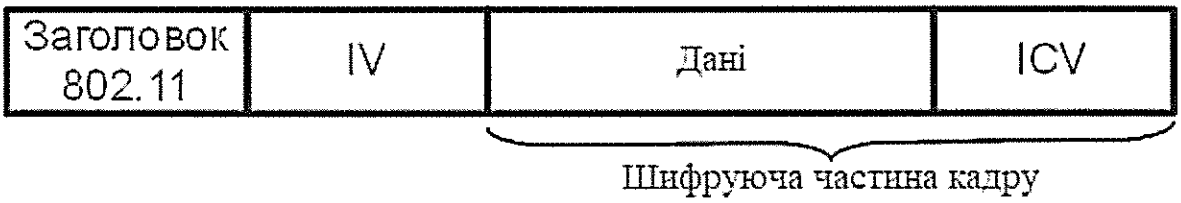



Рис. 2.3. Формат WEP-кадру

Як і будь-яка інша система безпеки на основі паролів, надійність WEP залежить від довжини і складу ключа, а також частоти його зміни. Перший серйозний недолік - застосування статичного ключа - за відносно невеликий час ключ можна підібрати перебором. І другий недолік WEP-шифрування - самосинхронізація для кожного повідомлення, оскільки вектор ініціалізації передається незашифрованим текстом з кожним пакетом і через невеликий проміжок часу він повторюється. В результаті протокол шифрування WEP на основі алгоритму RC4 в даний час не є стійким. [11].

## 2.2 Аналіз протоколу шифрування в технологіях WPA та WPA2

В основі стандарту WPA2 лежить метод шифрування AES, що прийшов на зміну стандартам DES і 3DES в якості галузевого стандарту. Вимагаючи великого обсягу обчислень, стандарт AES потребує апаратної підтримки, яка не завжди є в старому обладнанні БЛОМ.

WPA2 використовує протокол CBC-MAC

(CipherBlockChainingMessageAuthenticationCode) для аутентифікації і забезпечення цілісності даних, а для шифрування даних і контрольної суми MIC –режим лічильника (CounterMode, CTR). WPA2 забезпечує цілісність даних для незмінних полівзаголовку 802.11 за допомогою контрольної суми в якості коду цілісності повідомлення (MIC). Це відрізняє стандарт від WEP і WPA. Таким чином підтримується можливість розшифрування пакетів або компрометації криптографічної інформації за допомогою атак типу packetreplay.

Використовується так званий вектор ініціалізації (InitializationVector, IV), що складається з 128 розрядів і впливає на значення MIC. Для отримання даного вектору застосовується метод AES і тимчасовий ключ. На виході отримується 128-розрядний результат, що разом з наступними даними об'ємом 128 біт зазнають опрацювання операцією "виключне АБО". Її результат зашифровується за допомогою AES і тимчасового ключа TK. Далі над отриманим результатом і наступними 128 біт даних знову виконується операція "виключне АБО". Повторення процедури відбувається до того часу, доки не буде вичерпане усе корисне навантаження. Перші 64 розряди результату отриманого на останньому кроці використовуються для обчислення значення MIC. [7].

При шифруванні даних і MIC використовується алгоритм заснований на режимі лічильника (CTR). Виконання цього алгоритму також починається з завантаження лічильника довжиною у 128 розрядів, де у полі лічильника замість значення, що відповідає довжині даних, береться значення лічильника, встановлене в одиницю. Тому для шифрування кожного окремого пакету фактично використовується свій лічильник. З застосуванням AES та TK шифруються перші 128 біт даних, над результатом цього шифрування виконується операція "виключне АБО". Перші 128 біт даних дають перший 128- розрядний зашифрований блок. Попередньо завантажене значення лічильника інкрементується і шифрується за допомогою AES і ключа шифрування даних. Потім над результатом цього шифрування і наступними

128 біт даних знову виконується операція "виключне АБО". Процедура повторюється до тих пір, доки усі 128-розрядні блоки даних не будуть зашифровані. Після цього в якості остаточного значення у полі лічильника записується нуль, лічильник шифруєтьсяз використанням алгоритму AES, а потім над результатом шифрування і MIC виконується операція "виключне АБО". Результат останньої операції додається дозашифрованого кадру.

Підрахувавши MIC, виконується його шифрування разом з даними. До отриманого результату додається заголовок стандарту 802.11 і поле номеру пакету CCMP. Також додається закінчення стандарту 802.11, після чого пакет є готовим до відправлення.

Розшифрування даних виконується в зворотному порядку. Для витягання лічильника застосовується той самий алгоритм, що і для його шифрування. При дешифруванні лічильника застосовуються алгоритм розшифровки заснований на режимі лічильника і ключ TK. На виході отримуються контрольна сума MIC та розшифровані дані. За допомогою алгоритму CBC-MAC, здійснюється перерахунок MIC для отриманих розшифрованих даних. При збіганні значеньрозшифровані дані вважаються достовірними, інакше пакет відкидається. [8].

Хоча підтримка WPA2 і є загальнообов'язковою у сертифікаованих пристроях Wi-Fi, можлива проблема зворотної сумісності зі старими пристроями в зв'язку з потребами у апаратній підтримці алгоритму шифрування AES, що використовується в протоколі WPA2. Стандарт 802.11i використовує концепцію підвищеної безпеки (RobustSecurityNetwork, RSN), яка передбачає забезпечення бездротовими пристроями додаткових можливостей, що вимагають змін в апаратній частині та програмному забезпеченні. Отже мережа, повністю відповідна RSN, є несумісною з існуючим обладнанням WEP. Була визначена підтримка як обладнання RSN, так і WEP у перехідний період, однак зараз пристрої WEP вже поступаються місцем пристроям з повноцінною підтримкою виключно RSN. WPA2 в залежності від різних реалізацій може застосовувати TKIP, але за

замовчуванням RSN використовує AES і CCMP.

## 2.3 Оцінка параметрів методу автентифікації WPA та WPA2 для систем і мереж стандарту

Як відомо, метод автентифікації WPA2 на сьогодні є найстійкішим до атак, та, все ж існують методи його подолання. Існує дві модифікації даного методу WPA2 Personal та WPA2 Enterprise. Різниця між WPA2 Personal та WPA2 Enterprise полягає у тому, що ключі шифрування алгоритму AES зберігаються у різних місцях. WPA2 PersonalвикористовуєтьсяздебільшогоуSmallorHomeOffice (SOHO) мережах.Ключ у механізмі WPA2 Personal є однаковим для всіх користувачів. Для корпоративних застосувань використовується динамічний ключ, індивідуальний для кожного користувача. За генерацію пар логін-пароль у WPA2 Enterprise відповідає спеціальний сервер, здебільшого RADIUS.

Протокол WPA2-PSK (Pre-Sharedkey) дозволяє мобільним пристроям обмінюватись даними з точками доступу за допомогою методу шифрування AES. У криптографії PSK – це ключ, який попередньо ідентифікується між двома вузлами за допомогою певного безпечного каналу, перш ніж він буде використаний. PSK отримується з ключа, використовуючи стандарт формування ключа на основі паролю PBKDF2 із алгоритмом хешування SHA1 як псевдовипадковою функцією. PSK є 32 байтним (256 бітним), часто відображається у вигляді 64 шістнадцяткових символів. [14].

Стандарт PBKDF2 у свою чергу описується стандартом PKCS#5. У цьому випадку пароль повинен бути довжиною від 8 до 63 символів. Символи конвертуються у машинний код за допомогою таблиці кодування ASCII, а отже у паролі можуть використовуватись лише ці символи.

У PBKDF2 бінарний пароль використовується як ключ до функції HMAC. В якості солі використовується ім'я точки доступу (SSID). Сіль із значенням лічильника використовується для початкового входу в функцію HMAC. Після цього попередні вихідні дані використовуються як вхідні допоки не відбудеться повторення 4096 HMAC. На жаль, він повертає дані у форматі

256 біт, в той час якSHA1 всього лиш повертає 160 біт.

Вихідні дані функції PBKDF2 і є PSK. PSK використовується безпосередньо як і PairwiseMasterKey (PMK) у чотиристоронньому процесі рукостискання в формулі (2.1):

$$PSK = PBKDF\,2(HMAC - SHA\,1 \mid Passphrase \mid SSID \mid 4096 \mid 256\,) \quad (2.1)$$

Паролі, які використовують рядові споживачі сучасного обладнання Wi-Fізазвичай є не складними. Це може бути комбінація цифр від одиниці до дев'яти, літер на клавіатурі які розташовані поряд, чи дата народження. Сьогодні існує велика кількість згенерованих словників із не складними фразами, які використовуються рядовими користувачами. Такі словники можна знайти у відкритому доступі в мережі Інтернет, а також у спеціальних операційних системах, таких як Black Arch, ArchStrike, Kali Linux та ін.

Загальна кількість символів, яка може бути використана при створенні ключа дорівнює 95, це показано в таблиці 2.2.

Таблиця 2.2

**Символи доступні для завдання ключа у методі автентифікації WPA/WPA2**

| № | Набір символів | Кількість символів у наборі | Може використовуватись у словнику, як атомарна одиниця |
|---|---|---|---|
| 1 | [0-9] | 10 | + |
| 2 | [a-z] | 26 | + |
| 3 | [A-Z] | 26 | + |
| 4 | Спеціальні символи (`~!@#$%^&*()+-=/\|<>[]'".,?:;{} ) | 32 | + |
| 5 | Пробіл | 1 | - |

На основі проаналізованих популярних словників в таблиці 2.2,

формулюються найбільш доцільні комбінації наборів, які описані в таблиці 2.3. [10].

Таблиця 2.3

**Комбінація символі на основі таблиці 2.2.**

| № | Комбінація символів | Кількість символів у наборі |
|---|---|---|
| 1 | [0-9] + [a-z] | 36 |
| 2 | [0-9] + [A-Z] | 36 |
| 3 | [a-Z] + [A-Z] | 52 |
| 4 | [0-9] + [a-Z] + [A-Z] | 62 |
| 5 | [0-9] + [a-Z] + [A-Z] + спеціальні символи | 94 |
| 6 | [0-9] + [a-Z] + [A-Z] + спеціальні символи + пробіл | 95 |

Для того, щоб отримати доступ до мережі зловмиснику необхідно перехопити пакет рукостискання і запустити процес дешифрування. Операція дешифрування паролю відбувається за допомогою центрального або графічного процесорів. [12].

Після того, як відбувся перебір за словником і в ньому пароль не було знайдено, очевидно, що потрібно використати наступний словник. Якщо це словник, у якому не збільшується довжина ключа, але збільшується кількість символів з яких будуть генеруватись ключі, то логічно виключати ті комбінації,які вже були присутні у попередніх словниках, за формулою (2.2):

$$D = \sum_{i=1}^{n} d_i = l_i - l_{i-1}, \quad (2.2)$$

де D – загальний словник, d – поточний словник, l – набір ключів у словнику, формула (2.3) :

$$l_i = \{k_1, k_2 ... k_n\}, \quad (2.3)$$

де k – ключ.

Існує імовірність, що в базовому словнику ключа не буде знайдено. У цьому випадку повинен бути згенерований новий словник. Після базового словника логічно, що наступним має бути словник, у якому забезпечено мінімальну довжину ключів і найменший набір символів з таблиці 2.2. Це може бути словник, який складається лише з цифр. Як видно, ті ключі, які вже було використано в базовому словнику, не повинні перевикористовуватись. [9].

Якщо було опрацьовано словник, у якому 10^8 варіантів ключів, згенерованих з мінімального набору символів, ключ не буде знайдено, тоді наступний словник буде згенеровано із кількістю ключів 109 і з тим же ж мінімальним набором символів (тобто, це символи від 000000000, до 999999999).Для цього потрібно розгорнуто в 10 разів більше обчислювальних ресурсів для пошуку ключів із тою ж швидкістю. В іншому випадку, замість збільшення розміру ключа можна збільшувати кількість символів у наборі, тобто змінювати варіанти з таблиці 2.2.

Час, за який буде витрачено на підбір ключа за словником можна визначити за формулою (2.4): $t_{BF} = \frac{C_d}{S}$,

(2.4)

де Cd – кількість ключів у словнику, а S – швидкість перебору, отриманаіз застосуванням прапорця – S.

Для того, щоб обійти захист технології Wi-Fi із методом автентифікації WPA2, окрім необхідних знань зловмисник повинен володіти певною обчислювальною потужністю. Проведення лобової атаки на пароль здійснюється за рахунок центрального процесора (ЦП), або графічного процесора (ГП). Швидкість роботи ГП у проведенні лобової атаки є значно вищою, але не кожен комп'ютер оснащується дискретною графічною карткою.

Для пришвидшення лобової атаки, дана задача може виконуватись розподілено в кластері комп'ютерів.

Рівень захищеності приманки, яка імітує певну систему, не повинен бути значно вищим за рівень та можливості зловмисника, який очікується до взаємодії. Тобто, чим складніший ключ, тим потужнішою обчислювальною технікою потрібно володіти.

Введемо поняття обчислювальної одиниці, якою будемо вважати певний ресурс, який повинен виконати операцію перебору одного словника.

Як вже було згадано, для лобової атаки можна використовувати розподілені системи. Сьогодні задля оптимізації використання обчислювальних ресурсів використовуються різні типи комп'ютерної віртуалізації. Серед них повна, часткова, пара-віртуалізація і віртуалізація на рівні ОС. Розглянемо такі два типи віртуалізації, як повна віртуалізація і віртуалізація на рівні операційної системи, яка ще також називається контейнеризацією.

Згідно з дослідженнями компанії IBM технологія віртуалізації KVM на операційній системі SUSE Linux Enterprise 11 збільшує споживання ресурсів в загальному на 15%. Також при використанні віртуалізації додаткові витрати у споживанні процесорного часу становлять на 3–4% більше, аніж без застосування віртуалізації.

У технології контейнеризації гіпервізор не використовується, що зменшує навантаження на апаратне забезпечення. Усі контейнери функціонують на базі лише серверного ядра. Для кожного контейнера створюється своє окреме, ізольоване середовище. [13].

Як вже будо згадано вище, будь-яка технологія ізоляції приносить додаткові витрати. У випадку контейнеризації ці витрати складають від 0,1%–1%, за рахунок того, що використовуються прості перетворення. Наприклад ізоляція PID процесів виконується за допомогою додавання 4-байтного ідентифікатора, який позначає, якому контейнеру належить процес.

На рис.2.4. наведено принципову відмінність між контейнеризацією та віртуалізацією.




Рис. 2.4. Схематичне зображення відмінності між контейнеризацією та віртуалізацією: а – віртуалізація, б – контейнеризація

Для перевірки умовної захищеності системи приманки велике значення має швидкість обробки даних, а отже перевага буде віддаватись технології, яка справляється із задачами перебору за словником швидше. Задля оцінки складності подолання захисту методу автентифікації WPA/WPA2 зробимо його оцінку за рахунок коефіцієнтів методу аналізу ієрархій на основі таких критеріїв, як довжина ключа та кількість можливих символів у словнику. Даний метод дозволяє отримати співвідношення шкал від парних порівнянь із невеликим відхиленням [10–12]. В якості коефіцієнтів використовується фактичне вимірювання або суб'єктивна думка. На виході отримується співвідношення ваг та індекс узгодженості.

У стандартному виконанні методу аналізу ієрархій здійснюється оцінка будь-якої групи характеристик за допомогою шкали коефіцієнтів від 1 до 9. Кожна із характеристик порівнюється між собою, і виводиться матриця ваги кожного з елементів по відношенню одне до одного, формула (2.5):

$$N = \begin{vmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{12}^{-1} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}^{-1} & a_{2n}^{-1} & \cdots & 1 \end{vmatrix}. \tag{2.5}$$

З матриці N знаходяться суми коефіцієнтів для кожного стовпця, формула (2.6), для подальшої нормалізації матриці N, формула (2.7):

$$S_i = \sum_{i=1}^{n} a_i = a_{i1} + a_{i2} + ... + a_{in}\ . \tag{2.6}$$

$$|N| = \begin{vmatrix} \frac{1}{S_1} & \frac{a_{12}}{S_2} & \cdots & \frac{a_{1n}}{S_n} \\ \frac{a_{12}^{-1}}{S_1} & \frac{1}{S_2} & \cdots & \frac{a_{2n}}{S_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}^{-1}}{S_1} & \frac{a_{2n}^{-1}}{S_2} & \cdots & \frac{1}{S_n} \end{vmatrix}. \tag{2.7}$$

Просумувавши коефіцієнти кожного рядка нормалізованої матриці і розділивши суму на кількість коефіцієнтів рядка за допомогою формули (2.8), можна отримати вагу кожного з оцінюваних елементів:

$$x = \begin{bmatrix} \sum \frac{row_1}{n} \\ \sum \frac{row_k}{n} \\ \cdots \\ \sum \frac{row_k}{n} \end{bmatrix}. \tag{2.8}$$

Сума усіх ваг повинна бути рівною 100%, а отже, щоб отримати відсоткове значення складності ключа певної довжини, потрібно додати його

вагу до суми попередніх. [16]

У виведенні базового словника для лобової атаки було використано ресурсоперацийної системи Kali Linux. Kali Linux – це операційна система сімейства Linux, яка базується на дистрибутиві Debian, є безкоштовною і знаходиться у вільному доступі. Прямим призначенням даної операційної системи є тестування на проникнення. Але окрім тестувань власних систем не виключено, що такі операційні системи можуть використовуються зловмисниками для атак.

Автором було проаналізовано словники, які поставляються з операційною системою Kali Linux, і знаходяться у директорії /usr/share/wordlists. Дані словники фільтруються таким чином, щоб з них виключались усі слова-комбінації які менші за 8 символів, і ті, які не складаються із символів системи кодування ASCII цілком. Дані словники інтегруються в один, з якого виключаються не унікальні слова-комбінації(Лістинг 1).

Лістинг 1. Виведення базового словника для проведення лобової атаки на пакет рукостискання методу автентифікації WPA/WPA2 у операційній системі KaliLinux: (catdirbuster/*.txtfern-wifi/*rockyou.txtfasttrack.txtmetasploit/*.lstmetasploit/*.txt | grep ..... | grep -P -v “[^[:ascii:]]” | sort —unique).

Звичайно ж кожне тестування залежить від типу апаратного забезпечення, конфігурації програмного забезпечення. Автором було досліджено швидкість обчислення ключа для методу автентифікації WPA2 з попередньо перехопленого пакету «рукостискання».

Дослід проводився у контейнері віртуальної машини CoreOS, якій було виділено 1 Гб оперативної пам’яті і одне ядро процесора IntelCorei5-4590 з тактовою частотою 3,3 ГГц.

Попередньо було здійснено тестування за допомогою команди aircrack-ng- S, яка дозволяє здійснити замір швидкості лобової атаки у співвідношенні ключів за секунду. [12].

Після виконання команди з лістингу 1 і підрахувавши кількість ключів, отримуємо значення Cd = 9801317.

Замір швидкості лобової атаки на двох різних системах віртуалізації і контейнеризації було проведено по 10 разів, результати представлено у таблиці та на рис. 2.5.

Таблиця 2.4

**2.4 Заміри швидкості перебору ключів за словником**

| Спроба / Тип віртуалізації | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Повна віртуалізація (ключів/секунду) | 922 | 956 | 954 | 955 | 927 | 911 | 949 | 947 | 933 | 912 |
| Контейнеризація (ключів/секунду) | 1053 | 1038 | 1038 | 1041 | 1031 | 1032 | 1038 | 1038 | 1054 | 1054 |

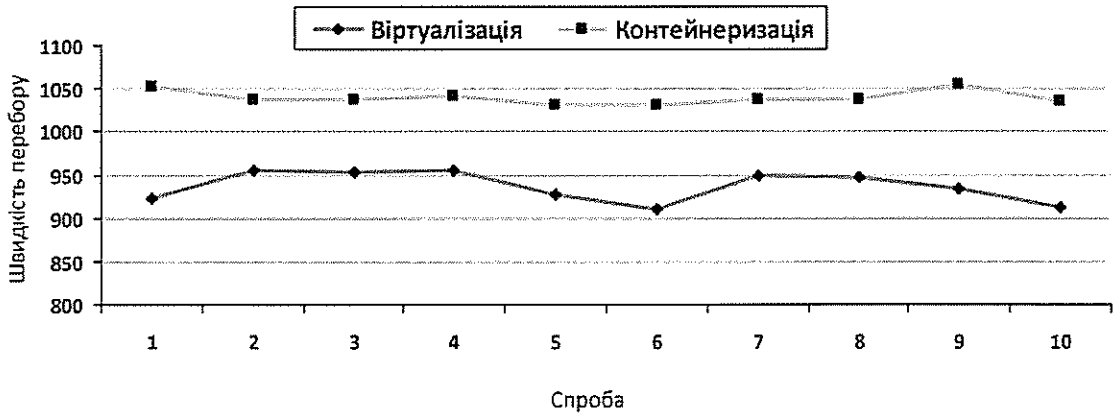



Рис. 2.4. Візуалізація порівняння швидкості перебору ключів за допомогоювіртуалізації і контейнеризації

Використаємо формулу (2.5) і обчислимо середню швидкість для віртуалізації:

$$\overline{S_F} = \frac{922+956+954+955+927+911+949+947+933+912}{10} = 936{,}6.$$

Використаємо формулу (2.5) і обчислимо середню швидкість для контейнеризації:

$$\overline{S_C} = \frac{1053+1038+1038+1041+1031+1032+1038+1038+1054+1036}{10} = 1039{,}9.$$

Володіючи даними про кількість ключів у базовому словнику і швидкістьз якою опрацьовуються ключі можемо скористатись формулою (4) і знайти приблизний час за який буде здійснено перебір усього базового словника:

$$t_{BF} = \frac{9801317}{1039{,}9} \approx 9425\,\text{сек.}$$

Якщо ж у базовому словнику ключ не буде знайдено, то пошук ключа будерозпочато із восьмисимвольного словника. Як вже було згадано вище, WPA2дозволяє задати ключ довжиною від 8 до 63 символів, що еквівалентно 56 варіантам довжини ключа. Це означає, що кількість варіантів буде збільшено в десятеро при переході на наступний словник, а отже й потужності буде затребувано в десятеро більше. [9].

Щоб застосувати метод аналізу ієрархій для даного дослідження, потрібнооцінити характеристики по відношенню одне до одного за шкалою від 1 до 9. Оскільки складність словника збільшується лінійно, тобто, щоразу у десять разів, то на відрізку від 1 до 9 ціною переходу від одного словника до іншого буде додавання до попереднього значення коефіцієнт 0,145454545, рис.2.5.

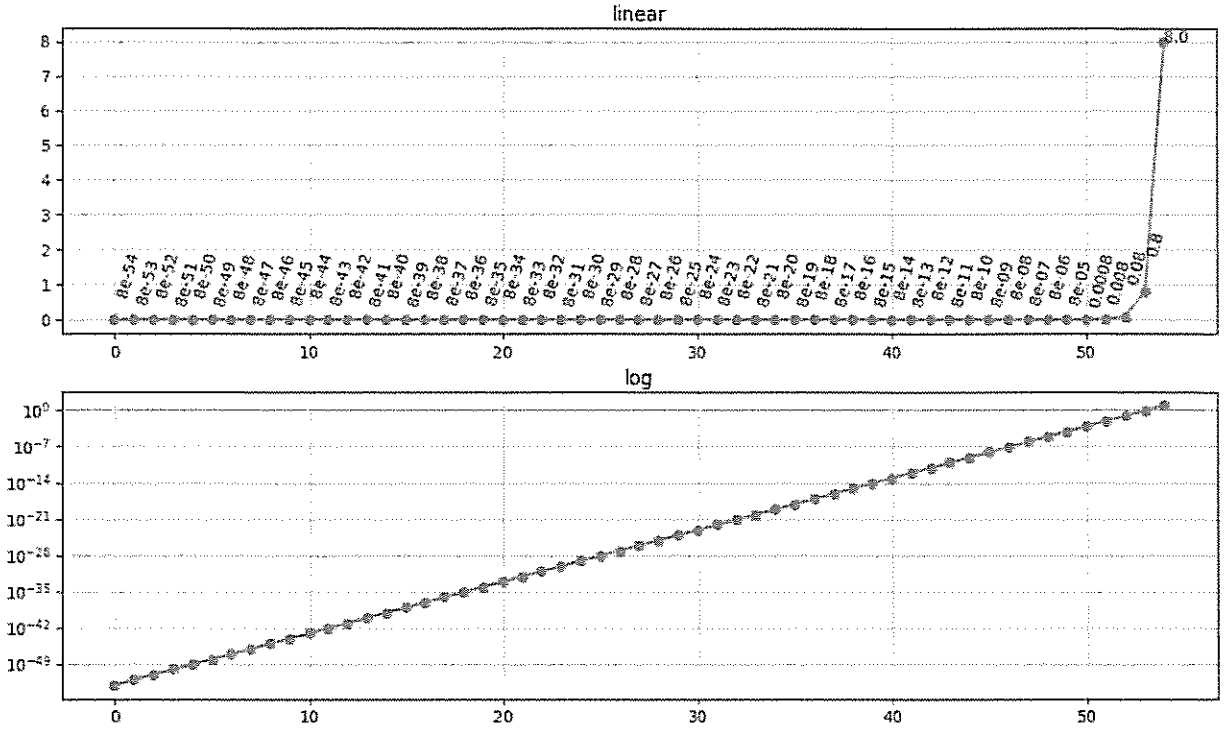



Рис. 2.5. Лінійне та логарифмічне представлення зміни складності словника уметоді аналізу ієрархій

Як вже було зазначено, довжина ключа не є єдиним критерієм оцінки його складності. Набір символів присутніх у словнику є також важливим критерієм. Наоснові таблиць 1 та 2 можемо зробити висновки про те, які комбінації символів у словниках є логічними для використання. Максимальна кількість символів, які можуть бути використані в паролі становить 95, тобто 95 символів складає 100%. Відповідно до цього отримуємо таблицю 2.5. [17].

Таблиця 2.5

**2.5 Відсоткове співвідношення кількості символів у словниках**

| Кількість символів | 95 | 94 | 62 | 52 | 36 | 32 | 26 | 10 |
|---|---|---|---|---|---|---|---|---|
| Відсоткове | 100 | 98,9 | 65,2 | 54,1 | 37,8 | 33,6 | 27,3 | 10, |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| представлення( w) | | 5 | 6 | 7 | 9 | 8 | 6 | 5 |

Як можемо бачити, один контейнер опрацює базовий словник приблизно за дві з половиною години, коли віртуальній машині для цієї ж операції знадобиться приблизно три години. А отже, можемо зробити висновок, що контейнеризація є кращим варіантом для проведення розподіленої лобової атаки на ключ методу автентифікації WPA/WPA2 технології бездротового зв'язку Wi-Fi. З використанням контейнеризації продуктивність зростає приблизно на 11%.

Задля правильної оцінки умовної захищеності системи-приманки важливо, щоб система, яка проводить таку оцінку, якомога точніше відтворювала поведінкузловмисника. Звичайно ж, ні вякій системі не можливо врахувати людський фактор, та все ж певне наближення є можливим. [11].

Особа яка атакує певну систему в будь-який момент може вирішити, що подальше продовження атаки є не доцільним, через час, який йде на дешифрування ключа, чи коштів, які вже вкладені в обчислювальну потужність.

Найпростішим варіантом з якого починають зловмисники – це використовувані ключі, що найбільше використовуються користувачами. Дотакими ключами може бути інформація, яка несе в собі якусь логіку, наприклад, дані про саму ж точку доступу, її власника чи місце, де вона знаходиться. Тому очевидно, що атаку варто починати зі словника, який містить в собі таку інформацію.

Якщо у базовому словнику ключа не буде знайдено, то для обробки буде взятий найпростіший словник,згенерований лише з цифр від 0 до 9, довжина ключів в якому не перевищуватиме 8 символів. Процес підбору словника буде виконуватись до моменту, поки ключ не буде знайдений. Відповідно, чим складніший словник – тим більший ресурс буде виділено для пошуку ключа, і тим вищою буде оцінка захищеності умовного захисту

системи-приманки. Найскладнішим буде словник, ключі якого генеруються з 95 різних символівтаблиці ASCII, а довжина його складає 63 символи.

Власники бездротового обладнання Wi-Fi нечасто встановлюють складні паролі на доступ до мережі, і цим користуються зловмисники. Тому логічно, що атака не буде розпочата зі словника, у якому ключі є довжиною 63 символи. Складність ключа певної довжини буде дорівнювати сумі коефіцієнта його ваги з усіма попередніми. Відповідно до цього можемо вивести шкалу складності подолання методу автентифікації WPA2 для розміру ключа. Виключенням з правил може бути випадок, якщо зловмисник знає довжину ключа. Перед тим, як обирати наступний словник, система оцінки повинна зробити вибір того критерію, який повинен бути змінений у наступному словнику

– довжина ключів чи кількість символів, з яких можуть бути згенеровані ключі. Автором пропонується робити приорітетним словник, у якому середнім значенням від суми відсоткових співвідношень кількості символів і довжини ключа у наступних словниках є менше з двох варіантів.

Словник, на якому закінчується атака, і буде вважатись точкою для оцінкирівня кваліфікації і технічного оснащення зловмисника.

Даний підхід допоможе якнайшвидше провести оцінку рівня захищеності системи-приманки для бездротових мереж в яких використовуються методи автентифікації WPA/WPA2. [11].

Функції аутентифікації покладаються на протокол EAP, який сам по собі єлише каркасом для методів аутентифікації. Вся принадність протоколу в тому, щойого дуже просто реалізувати на аутентифікаторі (точки доступу), так як їй не потрібно знати ніяких специфічних особливостей різних методів аутентифікації.

Аутентифікатор служить лише передавальною ланкою між клієнтом і серверомаутентифікації. Методів ж аутентифікації, яких існує досить багато:

- EAP-SIM, EAP-AKA - використовуються в мережах GSM

мобільногозв'язку;

- LEAP - пропреоретарний метод від Cisco systems;
- EAP-MD5 - найпростіший метод, аналогічний CHAP (не стійкий);
- EAP-MSCHAP V2 - метод аутентифікації на основі логіна / пароля користувача в MS-мережах;
- EAP-TLS - аутентифікація на основі цифрових сертифікатів;
- EAP-SecureID - метод на основі одноразових паролів.

Крім перерахованих вище, слід зазначити наступні два методи, EAP-TTLS і EAP-PEAP. На відміну від попередніх, ці два методи перед безпосередньою аутентифікацією користувача спочатку утворюють TLS-тунель між клієнтом ісервером аутентифікації. А вже всередині цього тунелю здійснюється сама аутентифікація, з використанням як стандартного EAP (MD5, TLS), або намагаючись не-EAP методів (PAP, CHAP, MS-CHAP, MS-CHAP v2), останні працюють тільки з EAP-TTLS (PEAP використовується тільки спільно з EAP методами). Попереднє тунелювання підвищує безпеку аутентифікації, захищаючи від атак типу «man-in-middle», «session hihacking» або атаки по словнику. [14].

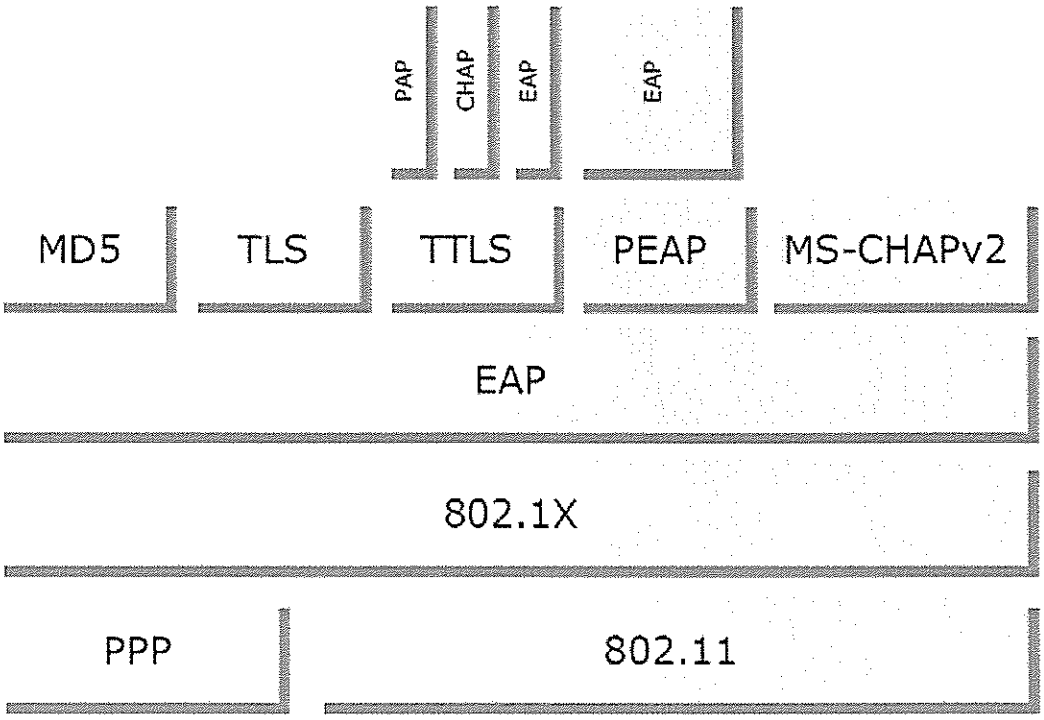



Рис. 2.6. Структура EAP-кадру

На рис.2.6. показана структура EAP кадру. Протокол PPP засвітився там тому, що спочатку EAP планувався до використання поверх PPP тунелів. Але так як використання цього протоколу тільки для аутентифікації по локальній мережі - зайва надмірність, EAP-повідомлення упаковуються в «EAP over LAN» (EAPOL) пакети, які і використовуються для обміну інформацією між клієнтом і аутентифікатором (точкою доступу).

Схема аутентифікації складається з трьох компонентів:

1) Supplicant - софт, запущений на клієнтській машині, яка намагаєтьсяпідключитися до мережі;
2) Authenticator - вузол доступу, аутентифікатор (бездротова точка доступу абопровідний комутатор з підтримкою протоколу 802.1x).
3) Authentication Server - сервер аутентифікації (зазвичай це RADIUS-сервер).

Тепер розглянемо сам процес аутентифікації. Він складається з наступнихстадій: [15].

1. Клієнт може надіслати запит на аутентифікацію (EAP-start message) в сторону точки доступу;
2. Точка доступу (Аутентифікатор) у відповідь посилає клієнту запит на ідентифікацію клієнта (EAP-request / identity message). Аутентифікатор може послати EAP-request самостійно, якщо побачить, що який-небудь з його портів перейшов в активний стан;
3. Клієнт у відповідь висилає EAP-response packet з необхідними даними, якийточка доступу (аутентифікатор) перенаправляє в бік Radius-сервера (сервераутентифікації);
4. Сервер аутентифікації посилає аутентифікатору (точки доступу) challenge- пакет (запит інформації про справжність клієнта). Аутентифікатор пересилає його клієнту;
5. Далі відбувається процес взаємної ідентифікації сервера і клієнта. Кількість стадій пересилки пакетів туди-сюди варіюється в залежності від методуEAP, але для безпроводових мереж підходить лише «strong» аутентифікація зі взаємною аутентифікацією клієнта і сервера (EAP-TLS, EAP-TTLS, EAP- PEAP) і попередніми шифруванням каналу зв'язку;
6. На наступний стадії, сервер аутентифікації, отримавши від клієнта необхідну інформацію, дозволяє (accept) чи забороняє (reject) тому доступ, з пересилкою даного повідомлення аутентифікатору. Аутентифікатор (точка доступу) відкриває порт для Supplicant-а, якщо з боку RADIUS-сервера прийшла позитивна відповідь (Accept);
7. Порт відкривається, аутентифікатор пересилає клієнту повідомлення проуспішне завершення процесу, і клієнт отримує доступ в мережу;
8. Після відключення клієнта, порт на точці доступа знову переходить в стан «закритий»[3].

Початкова аутентифікація проводиться на основі загальних даних, про які знають і клієнт, і сервер аутентифікації (як то логін / пароль, сертифікат і т.д.) - нацьому етапі генерується Master Key. Використовуючи Master Key,

сервер аутентифікації і клієнт генерують Pairwise Master Key (парний майстер ключ), який передається аутентифікатору з боку сервера аутентифікації. А вже на основі Pairwise Master Key і генеруються всі інші динамічні ключі, яким і закривається переданий трафік. Необхідно відзначити, що сам Pairwise Master Key теж підлягаєдинамічній зміні.

Нижче на рис.2.7. візуально показано, як проводиться аутентифікація по стандарту 802.11.

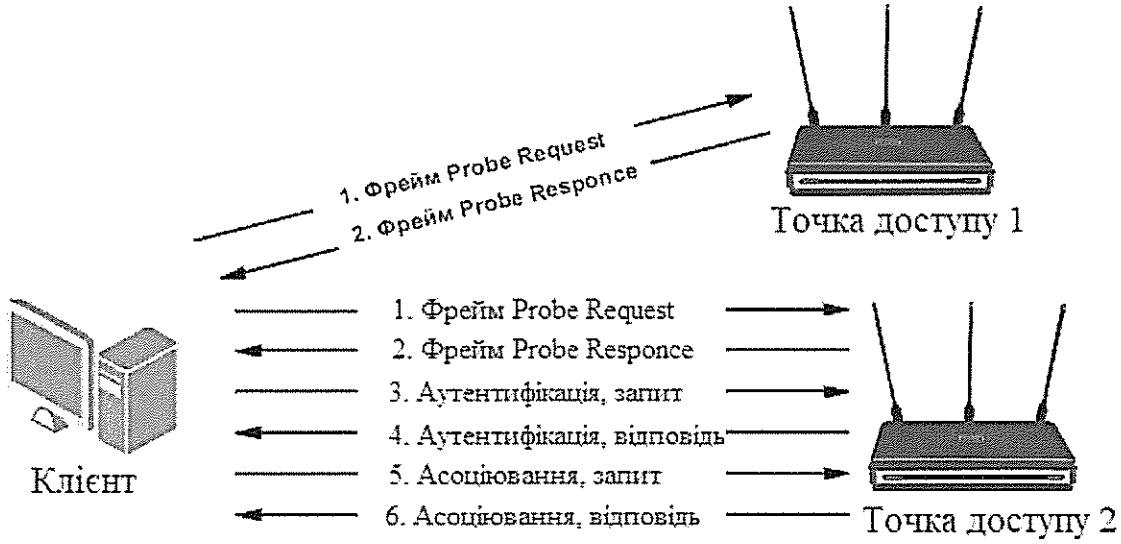



Рис. 2.7. Аутентицікація по стандарту 802.11

Аутентифікація з загальним ключем є другим методом аутентифікації стандарту IEEE 802.11. Процес аутентифікації з загальним ключем аналогічний процесу відкритої аутентифікації, відрізняючись тим, що даний метод вимагає настройки статичного ключа шифрування WEP, ідентичного на клієнтському пристрої (бездротовий адаптер) і на бездротової точки доступу.

Аутентифікація клієнта по його MAC-адресу підтримується багатьма виробниками обладнання для бездротових мереж, в тому числі D-Link. При аутентифікації по MAC-адресу відбувається порівняння MAC-адреси клієнта абозі списком дозволених (або заборонених) адрес клієнтів, внесеним в MAC-таблицю точки доступу, або за допомогою зовнішнього сервера аутентифікації , це показано на рис.2.8..Аутентифікація по MAC-адресу

використовується на додаток до відкритої аутентифікації і аутентифікації з загальним ключемстандарту IEEE 802.11 для зменшення ймовірності доступу сторонніх користувачів. [13].




Рис. 2.8. Аутентифікація за допомогою зовнішнього серверу

Функція фільтрації MAC-адрес надає істотну можливість підвищити безпеку. Рекомендується протидіяти атаці яка має назву ром-0 (тобто доступ до секретних даних, що зберігаються на роутері: комбінацію ім'я/пароль і пароль WiFi) тобто перенаправити порт 80 на неіснуючу адресу.

Стандарт IEEE 802.11i (WPA2) розроблений на базі перевірених технологій, однак деякі механізми безпеки були спроектовані з нуля в тісній співпраці з кращими фахівцями з криптографії і вважаються одним з найефективніших рішень проблем захисту бездротових мереж. Хоча жодна система безпеки повністю не застрахована від можливості взлому, WPA2 – це рішення, на яке можна покладатися, воно уникло недоліків попередніх протоколіві вважається одним з найбільш стійких, розширюваних і безпечних рішень, що призначене в першу чергу для великих підприємств, де управління ключами і адміністрування створювали найбільше проблем.

На даний момент у звичайних користувачів та системних адміністраторів бездротових мереж є всі потрібні засоби для гарантовано надійного захисту Wi- Fiмережі, і при відсутності значних помилок (людський фактор) можна забезпечити рівень безпеки, відповідний цінності інформації, що знаходиться в такій мережі. На сьогоднішній день бездротову мережу можна вважати захищеною, якщо в ній працюють три основних складових системи безпеки: конфіденційність даних, цілісність даних при їх передачі, аутентифікація користувача. Для отримання належного рівня безпеки

потрібно скористатися певними правилами при організації і налаштуванні приватної Wi-Fi-мережі.

Можна зробити висновок, що WEP є далеко не ідеальним рішенням для забезпечення безпеки. WPA забезпечує набагато більш високий рівень безпеки, ніж WEP, але і WPA не може дати надійної захищеності мережі. Самим надійним та безпечним рішенням є WPA2. Використання цього протоколу у поєднання з VPN О оптимальне рішення для корпоративних користувачів.

# 3. ШЛЯХИ ВДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ

## 3.1 Проблеми та напрямки їх вирішення у бездротових локальних мережах Wi-Fi

Був проведений аналіз Wi-Fi точок доступу в центральній частині міста Києва (використовувалося пасивне сканування та аналіз трафіку). Збір даних проводився за допомогою рухомого приймача. Повна довжина шляху склала 25 км, а площа охоплення — приблизно 15 км$^2$.

Для отримання даних про мережу необхідно, щоб в даній мережі відбувався обмін даними, і чим більш активно обмін відбувається, тим меншечасу потрібно для отримання інформації про мережу. Тому сканування проводилося між 13 та 16 годинами, на які припадає один з трьох піків активностікористувачів в мережі Інтернет (ранковій пік активності співпадає з часом пік вцентрі міста, а вечірній зумовлений користувачами зі спальних районів міста).[15]Інформацію було отримано за допомогою вбудованого Wi-Fi приймача DellWireless 1390 WLANMini-Card на мікросхемах серії BroadcomBCM94311MCG. Прийом та аналіз даних проводився за допомогою Wi-Fi драйвера bcm43xx (для ОС GentooLinux, версія ядра 2.6.24-r4) та аналізатора пакетів (так званого, сніфера) Aircrack-ng версії 0.9.1 (http://www.aircrack-ng.org/).Підчас поїздки було отримано інформацію від 1278 унікальних бездротовихмереж. Через брак часу на сканування кожної окремої мережі (до того ж деякімережі нечасто обмінюються даними) не вдалося точно визначити методишифрування для всіх точок, а також менше ніж у одного відсотка мереж невдалося отримати жодних даних. Втаблиці 3.1 подана статистика за просканованими мережам (ТД – скорочено від „точки доступу”).

### 3.2 Кількість точок доступу з різними видами шифрування

Дані з таблиці можна звести до діаграми, яка показана на рис.3.1. (далі в статистиці не враховуються точки доступу, про які нічого не відомо).

Таблиця 3.1

| Інформація про ТД | Кількість | % |
|---|---|---|
| WEP | 476 | 37.2 |
| WPA | 547 | 42.8 |
| Без шифрування | 209 | 16.4 |
| Закритий IP | 35 | 2.7 |
| Нічого не відомо | 11 | 0.9 |
| Загалом: | 1278 | 100 |

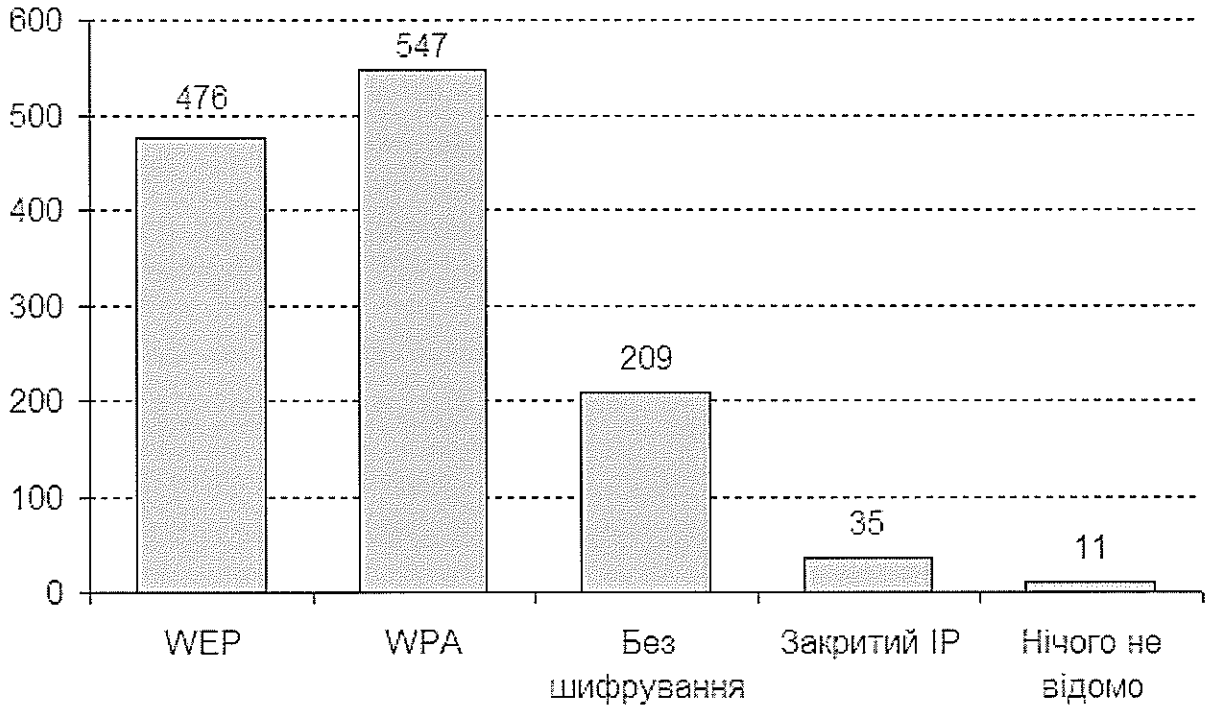



Рис. 3.1. Статистика точок доступу за різними видами шифрування

Якщо не враховувати точки доступу з закритим IP і точки доступу, проякі неможливо дізнатися додаткову інформацію (найбільш невразливі мережі), торозподіл за відсотками методів шифрування буде мати вигляд, показаний на рис.3. 2.[16]

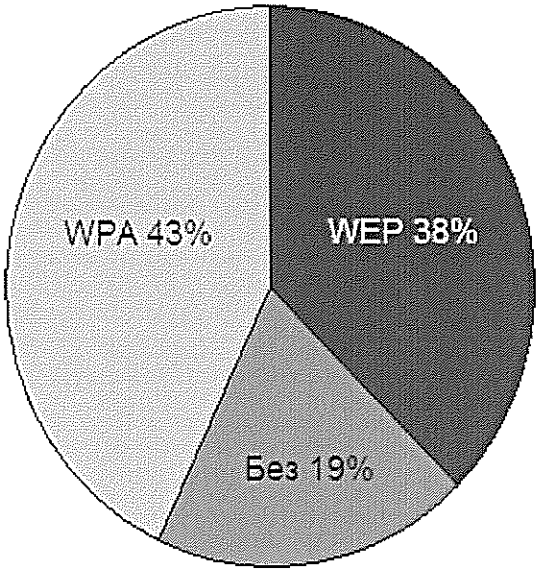



Рис. 3.2. Розподіл методів шифрування за відсотками

Використано різно-направлену антену, на рис.3.3. показана діаграма спрямованості використаної антени в двох площинах. В горизонтальній площині ширина променя складає 360°, а в вертикальній від 7° до 80°.

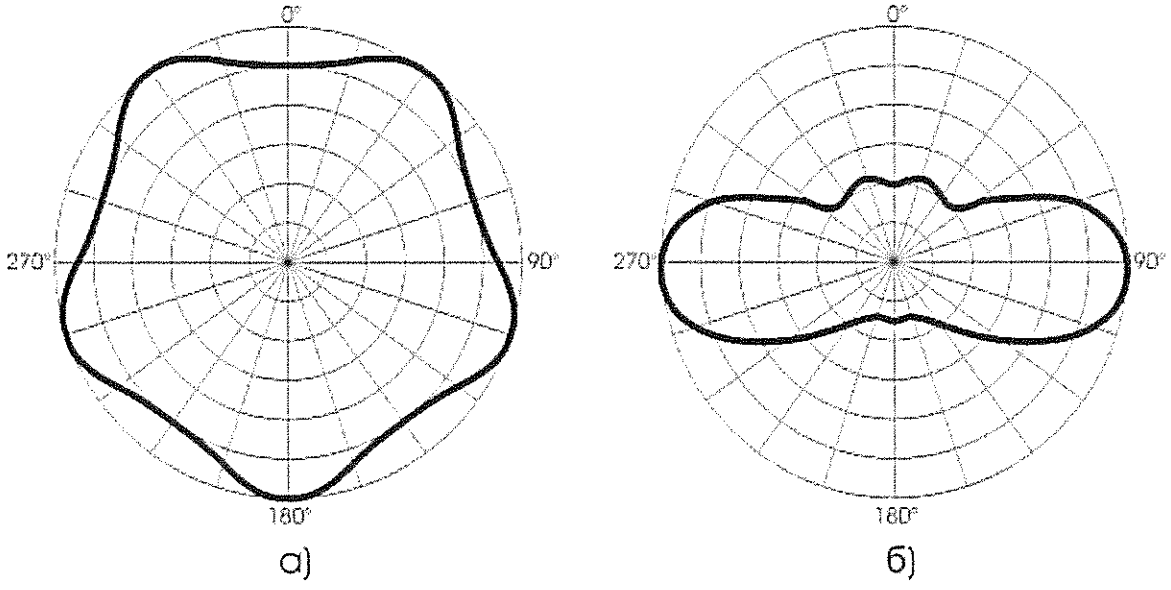



Рис. 3.3. Діаграма спрямованості використаних джерел в двох площинах

За MAC-адресами можна визначити виробників, як описано вище. В таблиці 3.2 приведені дані про кількість точок доступу п'яти найбільш розповсюджених виробників. Різні підрозділи однієї і тієї самої корпорації приведені під однією торгівельною маркою (наприклад, Cisco Systems Electronic Manufacturing і Cisco Systems Industries Industry). Так як MAC-адреси можна змінювати, то не завжди можна визначити виробника. В таблиці 3 приведені дані також про невизначених виробників (стовпчик „Невід." — невідомий). Крім приведених в таблиці були зареєстровані такі виробники: Asus (42), Apple (26), Askey (20), TP-Link (18), Planet (13), 3Com (10), Z-Com (10) та інші (87).

Таблиця 3.2

### 3.3 Шифрування точок доступу за виробником

| | Виробники | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | D-link | | Cisco | | Невідомо | | Motorola | |
| | К-сть | % | К-сть | % | К-сть | % | К-сть | % |
| WEP | 271 | 43.29 | 64 | 29.22 | 14 | 18.18 | 61 | 79.22 |
| WPA | 281 | 44.89 | 102 | 46.58 | 22 | 28.57 | 10 | 12.99 |
| Без шифрування | 74 | 11.82 | 53 | 24.20 | 41 | 53.25 | 6 | 7.79 |
| Загалом: | 626 | 100 | 219 | 100 | 77 | 100 | 77 | 100 |

Розподіл шифрування точок доступу за виробником можна відобразити на діаграмах, зображених на рис.3.4. та рис.3.5.

З діаграми та таблиці видно, що найкраще захищені мережі, побудовані на апаратному забезпеченні фірми Cisco, так як у 46,6% випадків використовується WPA шифрування. Таке використання Cisco зумовлене авторитетом виробника і вибором обладнання Cisco мережевимим адміністраторами, як стабільного в роботі. Щодо D-Link, то цей виробник є найпопулярнішим в Україні і на цьому обладнанні побудовані більшість централізованих мереж. Захищеність для D-Linkза протоколами WEP (43,3%) і WPA (44,9%) приблизно співпадає, а також має високий рівень у порівнянні з іншими виробниками, що пояснюється високою технічною грамотністю мережевих адміністраторів, які прокладають централізовані мережі.[5]

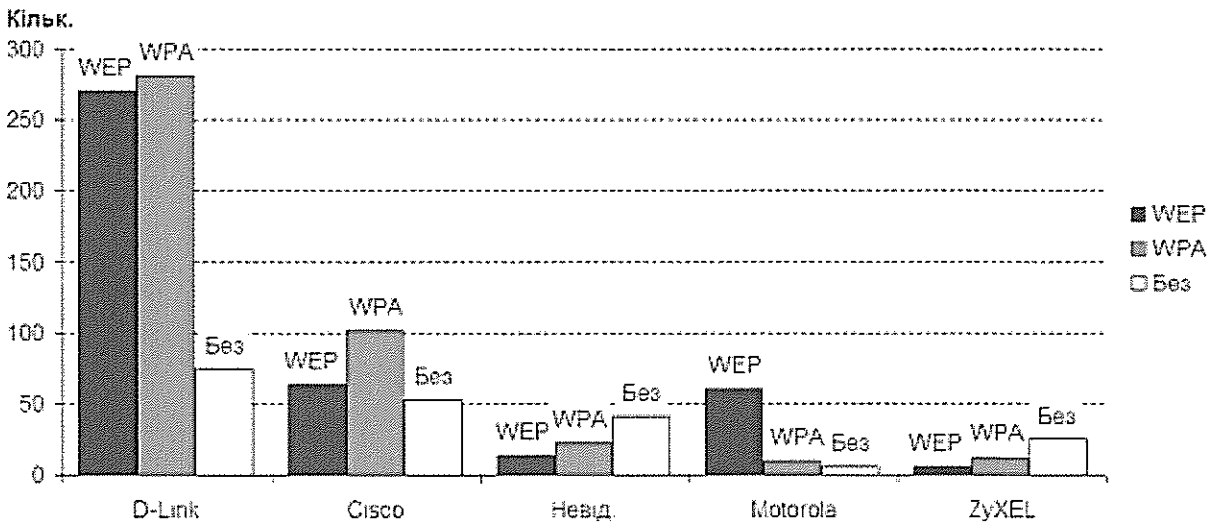



Рис. 3.4. Діаграма кількості точок доступу різного шифрування за виробником

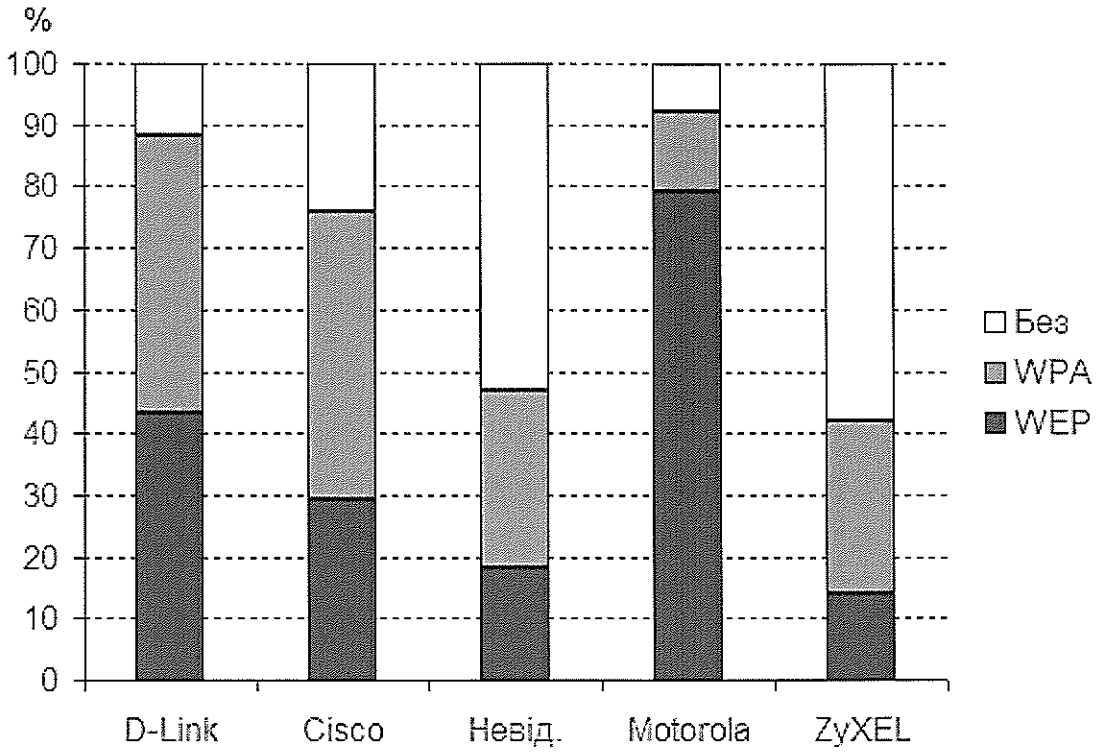



Рис. 3.5. Діаграма співвідношення точок доступу з різним типом шифрування завиробником

За назвою точки доступу можна частково визначити можливий рівень їїзахищеності. Всі точки доступу можна поділити на три типи:

- За виробником (наприклад, dlink, linksys);
- За назвою, в якій фігурує назва бездротової мережі (наприклад, wireless);
- За назвами користувачів (наприклад, home, work)

Числові дані про розподіл за групами приведено в таблиці 3.3. Назва виробника встановлюється за замовчуванням і часто співпадає з даними із MAC- адреси. В душках вказана загальна кількість точок доступу даного виробника, розглянута раніше. Втаблиці для виробника Hewlett Packard спостерігається невідповідність кількості точок доступу, визначених за допомогою MAC-адреси, та точок доступу, які визначених за назвою. Як показую статистика, що не більше 20% користувачів лишають назву виробника за замовчуванням. Невідповідність даних для

Hewlett Packard пояснюється прикладним програмним забезпеченням, за допомогою якого можна легко змінити MAC-адресу точки доступу.[14].

Таблиця 3.3

**3.4 Розподіл точок доступу за назвами**

| Виробники | | Стандартні назви | | Користувачі | |
|---|---|---|---|---|---|
| Dlink (D-link) | 62 (634) | volia | 81 | Organization | 207 |
| Linksys (Cisco) | 47 (220) | default | 64 | Специфічні назви | 204 |
| HG520s (Huawei) | 13 (20) | WI-FI | 46 | Ім'я користувача | 125 |
| Apple | 7 (26) | radiospot | 23 | Без назви | 123 |
| TP_LINK | 8 (18) | net | 16 | Number | 113 |
| ZyXEL | 8 (43) | wireless | 14 | Home | 84 |
| hpsetup | 6 (3) | AirLAN | 4 | Office | 12 |
| 3com | 3 (10) | | | Work | 8 |
| Загалом вгрупі | 154 | | 248 | | 876 |

Примітка: точки доступу з назвою HG520s відносяться до компанії HuaweiTechnologies, але виготовлені на базі мікросхем Askey, тому в таблиці у душках вказана кількість для Askey.

Перші два типи разом складають назви за замовчуванням, тому при

аналізі їх протоколів ці групи можна розглядати разом. Обидві діаграми приведені на рисунку 3.6

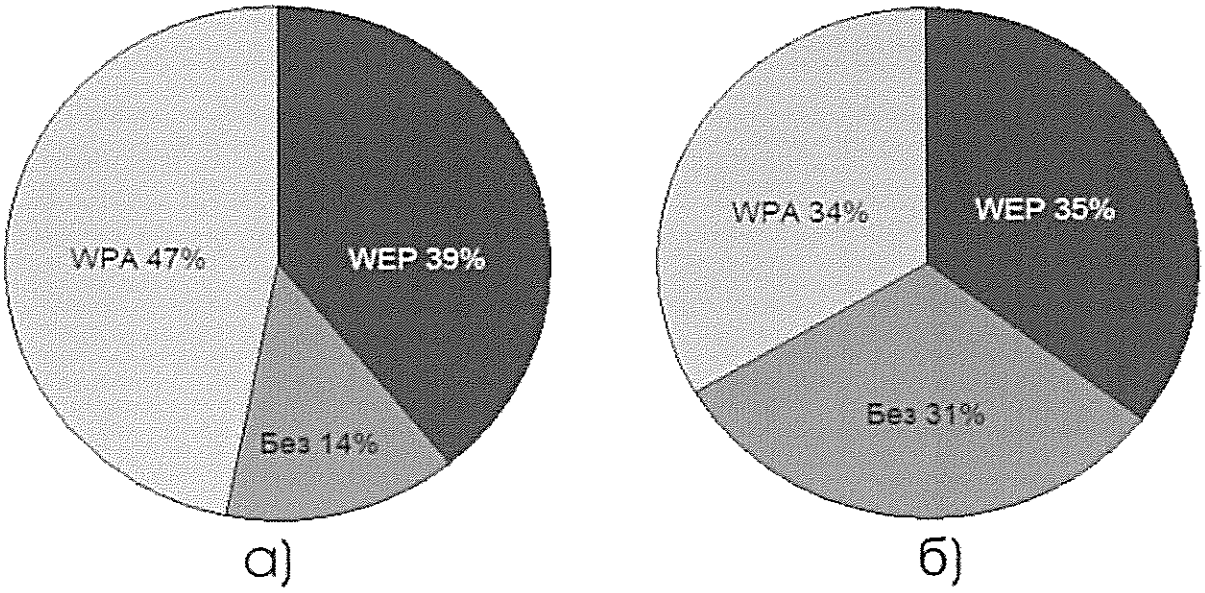



Рис. 3.6. Загальні діаграми точок доступу з шифруванням і без нього

З діаграм видно, що мережі з назвами користувачів мають більший відсотоквідкритих мереж, а також співвідношення протоколів шифрування WPA (34%) <WEP (35%) вказує на менш серйозне відношення до захисту мереж.[32]Також на рівень серйозності користувачів опосередковано свідчить назва (в таблиці поле „специфічні назви"). Наприклад, до несерйозного ставлення до точок приватних доступу свідчать такі назви, як „preved", „Faino", „uhahaha", „ViVA", „yJIuTKO" і навіть „Yawifiko!". Загальна кількість таких точок доступу від загальної кількості становить 1-2%.

Найбільш вразливими є мережі, які налаштовані за допомогою стандартного програмного забезпечення. У більшості випадків доступ до таких мереж в загалі залишають відкритим. Найбільш вразливими мережами є мережі в місцях загального користування (кафе, вокзали, учбові заклади

тощо).

Для підвищення надійного захисту у мережі Wi-Fi необхідно дотримуватися таких вимог:

1) При створенні на фізичному рівні необхідно обмежити доступ домережі;
2) Оптимального налаштування параметрів конфігурації механізмів аутентифікації та шифрування для забезпечення ефективності роботи, надійності та безпеки мережі;
3) Використання програмних засобів захисту пристроїв користувача та контролю усієї мережі;
4) Постійний моніторинг мережі для запобігання створенню в корпоративній мережі несанкціонованих точок доступу чи підключення;
5) Використання VPN (VirtualPrivateNetwork) для усіх пристроїв корпоративних клієнтів, що забезпечить захист при використанні різних точок доступу, що не належать корпоративної інфраструктурі, а також широкі можливості з вибору алгоритмів аутентифікації, шифрування та перевірки цілісності потоку даних;
6) Формування політики безпеки та складання відповідної документації;
7) Проведення інструктажів та семінарів для ознайомлення

корпоративних робітників з основами правил безпеки під час роботи з офісною технікою та засобами зв'язку, зокрема і мережі Інтернет.

Протягом багатьох років одним з надійних засобів захисту комп'ютерних мереж залишаються мережеві екрани (брандмауер, firewall, фільтрувальні маршрутизатори). Вони бувають апаратні та програмні, що дає змогу забезпечити високий рівень захисту. Мережевий екран є одним з декількох механізмів, що використовуються для управління і спостереження за доступом до мережі з метоюїї захисту, зокрема до бездротових мереж. Крім цього, використання комплексних засобів захисту, що містять засоби

антивірусної безпеки та мережевих екранів, гарантує дуже надійний рівень захисту[16].

### 3.5 Сучасні альтернативні методи захисту

Нещодавно була опублікована технологія захисту бездротових мереж WPA3. Об'єднання Wi-Fi Alliance, розвиваюче стандарти для бездротових мереж, опублікувало специфікацію WPA3 (Wi-Fi Protected Access), при розробці якої зроблена спроба усунення концептуальних недоробок, виявлених авторами атаки KRACK проти WPA2. WPA3 продовжує ґрунтуватися на базових технологіяхWPA2, доповнюючи їх сучасними засобами забезпечення безпеки, такими як надійні методи шифрування, обов'язкове використання PMF (Protected Management Frames) для контролю за цілісністю трафіку і виключення з специфікацій небезпечних протоколів.

Підтримка WPA2 поки залишається обов'язковою для сертифікованих WiFi-пристроїв, але з часом, після появи повсюдної підтримки WPA3, для всіх WiFi-пристроїв в розряд обов'язкових будуть переведені нові вимоги до безпеки. Для забезпечення сумісності, пристрої WPA2 зможуть підключатися до точок доступу WPA3 за допомогою спеціального перехідного режиму роботи.[18]

Передбачено два режими роботи WPA3: WPA3-Personal і WPA3- Enterprise:

1) У WPA3-Personal забезпечений надійний захист навіть при установці користувачем ненадійного пароля доступу, легко підбирається в результаті словникових атак. Для захисту від атак з підбору пароля (brute-force) введено обмеження на число спроб аутентифікації в рамках одного handshake (обмеженняне дозволить підбирати пароль в offline-режимі). Замість PSK (Pre-Shared Key) ключа в WPA3 реалізована технологія SAE (Simultaneous Authentication of Equals),вже застосовується в mesh-мережах і описаної в стандарті IEEE 802.11s. SAEбазується на протоколі обміну ключами Діффі - Хеллмана з використаннямкінцевих циклічних груп. Результуючий сесійний ключ, який отримує кожна сторона з'єднання для аутентифікації сеансу,

виробляється на основі інформації зпароля, ключів кожної системи і MAC-адрес обох сторін. Компрометаціязакритого ключа однієї зі сторін не призводить до компрометації сесійного ключа,тобто навіть дізнавшись пароль атакуючий не зможе розшифрувати ранішеперехоплений трафік.

2) У WPA3-Enterprise застосовується шифрування на основі як мінімум

192-розрядних ключів, які відповідають вимогам CNSA (Commercial National Security Algorithm), виробленим комітетом NSS для захисту урядових, військових та промислових мереж. Зокрема, для аутентифікованого шифрування рекомендовано застосування 256-розрядних ключів GCMP-256 (Galois / Counter Mode Protocol), для передачі і підтвердження ключів використовується HMAC з хешамі SHA384 (HMAC-SHA384), для узгодження ключів і аутентифікації використовуються ECDH (Elliptic Curve Diffie-Hellman) і ECDSA (Elliptic Curve Digital Signature Algorithm) з 384-розрядними еліптичними кривими, для захисту цілісності кадрів застосовується протокол BIP-GMAC-256 (Broadcast / Multicast Integrity Protocol Galois Message Authentication Code).18]

Додатково запропоновано програму "Wi-Fi Easy Connect" з реалізацією можливості спрощеної налаштування пристроїв без екранного інтерфейсу. Налаштування здійснюється з використанням іншого більш просунутого пристрою, вже підключеного до бездротової мережі. Наприклад, параметри для IoT-пристрої без екрану можна задати зі смартфона на основі знімка QR-коду, надрукованого на корпусі. Wi-Fi Easy Connect грунтується на застосуванні аутентифікації по відкритих ключах (в QR-коді передається відкритий ключ) і може використовуватися в мережах з WPA2 і WPA3. Особливістю Wi-Fi Easy Connect також є можливість заміни точки доступу без необхідності переконфігуруванні клієнтських пристроїв.

Для створення загальнодоступних публічних бездротових мереж представлена програма Wi-Fi Enhanced Open, що передбачає шифрування всіх потоків даних між клієнтом і точкою доступу, що дозволить захистити приватність користувача в загальнодоступних відкритих мережах не потребують аутентифікації. Для генерації ключів шифрування в відкритих мережах

застосовується процес узгодження з'єднання, що реалізовується розширенням Opportunistic Wireless Encryption.

Автор атаки KRACK на WPA2 виступив з критикою WPA3 і вважає, що Wi-Fi Alliance упустив шанс реально підняти безпеку бездротових мереж. Основні претензії до нової специфікації зводяться до того, що дуже багато поставлено на догоду забезпечення сумісності з WPA2 і обов'язковою є лише секція "A More Secure Handshake", яка визначає застосування більш надійного методу узгодженняз'єднання SAE (також відомий як "dragonfly"). Вимоги щодо збільшення розміру сесійних ключів застосовні тільки при використанні режиму WPA3-Enterprise,який є не обов'язковим. Wi-Fi Easy Connect і Wi-Fi Enhanced Open не включені до складу WPA3.

По суті виробнику для отримання сертифіката сумісності з WPA3 досить реалізувати тільки підтримку SAE і не витрачати ресурси на інші механізми захисту. Підтримка PMF (Protected Management Frames) не специфічна для WPA3 і з початку року також необхідна для WPA2, але дослідники безпеки впевнені, що знайдеться спосіб обходу PMF для примусового від'єднання клієнта від мережі. Впровадження SAE ускладнить проведення словникових атак, але не виключить їх, а лише зробить більш тривалими. Для обходу захисту в відкритих мережах атакуючий як і раніше зможе розгорнути свою точку доступу і перехоплювати будь-який трафік підключилися до неї користувачів.[19]

Користувачі WPA3-Personal отримують більш надійну парольну аутентифікацію і захист від брутфорсу навіть в тих випадках, якщо вибирають занадто короткий або простий пароль. Це реалізується за рахунок заміни старого протоколу Pre-shared Key (PSK) на протокол Simultaneous Authentication of Equals (SAE) від Дена Перкінса. SAE відноситься до протоколів типу PAKE (password-authenticated key agreement): інтерактивний метод, де дві або більше сторони встановлюють криптографічні ключі, засновані на знанні однієї або декількома сторонами пароля.

Ключова властивість PAKE - людина в середині не може отримати достатньо інформації, щоб провести повноцінний «офлайновий» брутфорс в

пасивному режимі. Йому обов'язково потрібна взаємодія зі сторонами для перевірки кожного варіанта. Це означає, що навіть зі слабкими паролями забезпечується набагато краща безпеку, ніж раніше.

WPA3-Personal більше орієнтований на простоту у використанні.

Користувачі як і раніше можуть вибирати довільні паролі.

Передбачається, що при виборі 192-бітного режиму будуть використовуватися всі перераховані інструменти, що гарантує правильну комбінацію протоколів як базову платформу безпеки всередині мережі WPA3.[16] WPA3 заснований на криптографічному протоколі Simultaneous Authentication of Equals (SAE) від Дена Харкінс (Dan Harkins). Цей фахівець також є автором сумнозвісного протоколу Dragonfly (RFC 7664). Потрібно сказати, що процедура затвердження RFC 7664 в IETF супроводжувалася бурхливими дебатами. Голова робочої групи з криптостандарта CFRG, яка стверджувала Dragonfly, Кевін Айгоу (Kevin Igoe) імовірно є співробітником АНБ. В результаті все-таки в глобальному сенсі не можна з усією впевненістю говорити про криптографічну стійкість і загальну надійність протоколу SAE і стандарту WPA3 в цілому.

Wi-Fi Alliance очікує, що пристрої з підтримкою WPA3 поширяться на ринку в 2019 році, разом з пристроями, які підтримують нову, більш швидку версію самого Wi-Fi - 802.11ax. Після цього підтримка WPA3 може стати обов'язковою умовою для сертифікації будь-якого пристрою Wi-Fi.

Найголовніший момент в захисті мережі настає, коли новий пристрій починає з'єднуватися. Ворог повинен залишатися за воротами, тому WPA2 і WPA3 приділяють багато уваги аутентифікації нових з'єднань і гарантії того, що вони не будуть спробами хакера отримати доступ.

SAE - новий метод аутентифікації пристрою, що намагається підключитися до мережі. SAE - це варіант, що використовує криптографію для запобігання вгадування пароля зловмисником. Він говорить про те, як саме новий пристрій, або користувач, має «вітати» мережевий маршрутизатор при обміні

криптографічними ключами.

SAE йде на заміну методу Pre-Shared Key (PSK) [попередньо розданого ключа], використовуваного з моменту презентації WPA2 в 2004-му. PSK також відомий, як чотирьох-етапне встановлення зв'язку, оскільки стільки саме повідомлень, або двосторонніх «рукостискань», необхідно передати між маршрутизатором і можуть бути під'єднані, щоб підтвердити, що вони домовилися з приводу пароля, при тому, що жодна зі сторін не повідомляє його інший . До 2016 року PSK здавався безпечним, а потім була відкрита атака з перевстановлення ключа (Key Reinstallation Attacks, KRACK).[7] KRACK перериває серію рукостискань, прикидаючись, що з'єднання з маршрутизатором тимчасово перервалося. Насправді він використовує повторювані можливості з'єднання для аналізу рукостискань, поки не зможе здогадатися про те, який був пароль. SAE блокує можливість такої атаки, а також найбільш поширені офлайнові атаки по словнику, коли комп'ютер перебирає мільйони паролів, щоб визначити, який з них підходить до інформації, отриманої під час PSK-з'єднань.

Як випливає з назви, SAE працює на підставі припущення про рівноправність пристроїв, замість того, щоб вважати один пристрій відправляє запити, а друге - встановлює право на підключення (традиційно це були пристрій, що намагається з'єднатися, і маршрутизатор, відповідно). Будь-яка зі сторін може відправити запит на з'єднання, і потім вони починають незалежно відправляти засвідчує їх інформацію, замість того, щоб обмінюватися повідомленнями по черзі, туди-сюди. А без такого обміну у атаки KRACK не буде можливості «вставити ногу між дверима і косяком», і атаки по словнику стануть марними.[10] SAE пропонує додаткове посилення безпеки, якого не було в PSK: пряму секретність [forward secrecy]. Припустимо, атакуючий отримує доступ до зашифрованих даних, які маршрутизатор відправляє і отримує з інтернету. Ранішеатакуючий міг зберегти ці дані, а потім, в разі успішного підбору пароля, розшифрувати їх. З використанням SAE при кожному новому з'єднанні встановлюється новий шифруючий пароль, тому навіть якщо атакуючий в якийсьмомент і проникне в мережу, він зможе вкрасти тільки пароль від

даних, переданих після цього моменту.

Версія WPA3, призначена для роботи в урядових та фінансових установах, а також в корпоративному середовищі, володіє шифруванням в 192 біта. Такий рівень шифрування для домашнього маршрутизатора буде надлишковим, але йогомає сенс використовувати в мережах, що працюють з особливо чутливою інформацією.[10]

Щоб гарантувати належний рівень безпеки всієї мережі, від початку до кінця, WPA3-Enterprise буде використовувати 256-бітний протокол Galois /Counter Mode для шифрування, 384-бітний Hashed Message Authentication Mode режим для створення і підтвердження ключів, і алгоритми Elliptic Curve Diffie-Hellman exchange, Elliptic Curve Digital Signature Algorithm для аутентифікації ключів. У них багато складної математики, але плюс в тому, що на кожному кроці буде підтримуватися шифрування в 192 біта.

Easy Connect - це визнання наявності в світі величезної кількості пристроїв, приєднаних до мережі. І хоча, можливо, не всі люди захочуть обзавестися розумними будинками, у середньої людини до домашнього маршрутизатора сьогодні, швидше за все, підключено більше пристроїв, ніж в 2004 році. Easy Connect - спроба Wi-Fi альянсу зробити під'єднання всіх цих пристроїв більш інтуїтивним.[16]

Enhanced Open - ще один окремий протокол, розроблений для захисту користувача у відкритій мережі. Відкриті мережі - такі, якими ви користуєтеся в кафе або аеропорту - несуть в собі цілий комплекс проблем, які зазвичай не стосуються вас, коли ви встановлюєте з'єднання будинку або на роботі.

Багато атак, що відбуваються у відкритій мережі, відносяться до пасивних. Коли до мережі підключається купа людей, атакуючий може зібрати дуже багато даних, просто фільтруючи проходить повз інформацію.

Enhanced Open використовує опортуністичне бездротове шифрування (Opportunistic Wireless Encryption, OWE), певний в стандарті Internet Engineering Task Force RFC 8110, щоб захищатися від пасивного підслуховування. Для OWE не потрібний додатковий захист з аутентифікації - воно концентрується на

поліпшенні шифрування даних, що передаються по публічних мереж, з метою запобігти їх крадіжку. Воно також запобігає т.зв. просту ін'єкцію пакетів [unsophisticated packet injection], в якій атакуючий намагається порушити роботу мережі, створюючи і передаючи особливі пакети даних, що виглядають, як частина нормальної роботи мережі.

Enhanced Open не дає захисту з аутентифікацією через особливості організації відкритих мереж - вони за визначенням призначені для загального використання. Enhanced Open був розроблений для поліпшення захисту відкритих мереж проти пасивних атак, так, щоб не вимагати від користувачів введеннядодаткових паролів або проходження додаткових кроків.

Наступним кроком в даній роботі буде доцільно виділити системи виявлення вторгнення в бездротових мережах.[6]

Системи виявлення вторгнення (Intrusion Detection System, IDS) - це пристрої, за допомогою яких можна виявляти і своєчасно запобігати вторгнення в обчислювальні мережі. Вони діляться на два види: на базі мережі і на базі вузла.

Мережеві системи (Network Intrusion Detection Systems, NIDS) аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил (експертні системи). Підмножиною мережевих систем виявлення вторгнень є системи для спостереження тільки за одним вузлом мережі (Network Node IDS).

Інший вид систем виявлення вторгнень представляють системи на базі вузла (Host Intrusion Detection Systems, HIDS). Вони встановлюються безпосередньо на вузлах і здійснюють спостереження за цілісністю файлової системи, системних журналів і т.д.

NIDS діляться в свою чергу на дві великі категорії: на основі сигнатур і на основі бази знань. Сигнатурні IDS найбільш поширені. У таких системах події, що відбуваються в мережі, порівнюються з ознаками відомих атак, які і називаються сигнатурами. Бази даних, що містять сигнатури, необхідно надійно захищати і часто оновлювати. IDS на основі бази знань стежать за мережею, збирають статистику про її поведінку в нормальних умовах, виявляють різні відхилення і позначають їх як підозрілі. Тому такі IDS ще називають заснованими

на поведінці або статистичними.[7]

Для ефективної роботи статистичної IDS необхідно мати надійну інформацію про те, як поводиться мережу в нормальних умовах, так звану точку відліку. Хоча таку IDS обдурити складніше, але і у неї є свої проблеми: помилкові спрацьовування і труднощі при виявленні деяких видів комунікацій по таємного каналу. Помилкові спрацьовування особливо ймовірні в бездротових мережах через нестабільність середовища передачі. Крім того, атаки, проведені на ранніх стадіях періоду фіксації точки відліку, можуть спотворити процедуру навчання статистичної IDS.

Тільки зібравши значний обсяг статистичних даних про роботу конкретної мережі, можна вирішити, що є аномальним поведінкою, а що - ні, і ідентифікувати проблеми зі зв'язком, помилки користувачів і атаки. Багаторазові запити на аутентифікацію по протоколу IEEE 802.1x / LEAP можуть свідчити про спробу атаки методом повного перебору. Але це може пояснюватися і тим, що користувач забув свій пароль або роботою погано написаного клієнтського додатка, яке продовжує спроби увійти в мережу, поки не буде введений правильний пароль.[14]

Збільшення числа фреймів-маяків може бути ознакою DoS-атаки або присутності в мережі фальшивої точки доступу, але не виключено, що вся справа в несправної або неправильно сконфигурированной законної точки доступу. Події, що фіксуються IDS на верхніх рівнях стека протоколів, наприклад велике число фрагментованих пакетів або запитів TCP SYN, може вказувати на сканування портів або DoS-атаку, але, можливо, це просто результат поганої зв'язку на фізичному рівні.[13, 17]

Нижче на рис.3.7 наведені характеристики систем виявлення вторгнення в бездротових мережах.

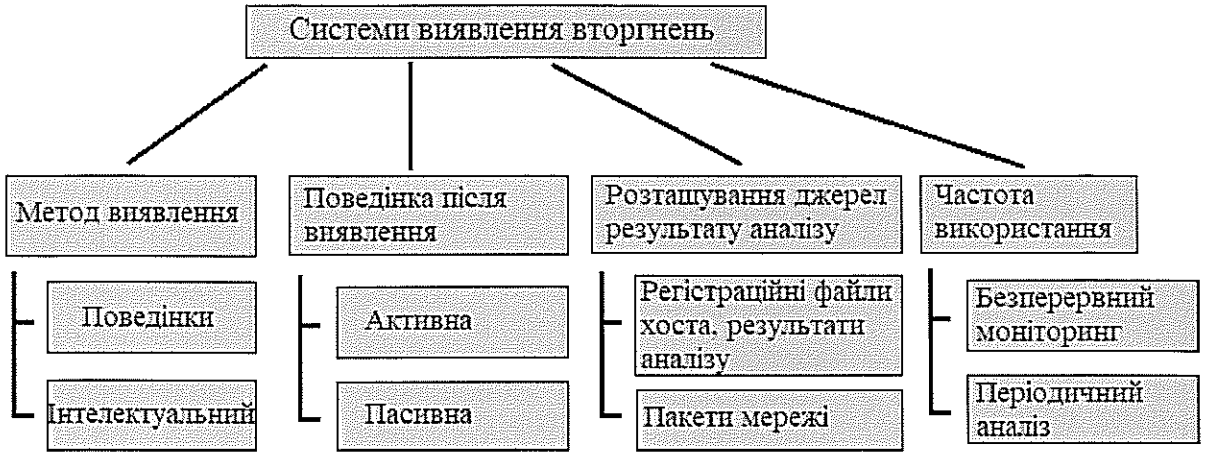



Рис. 3.7. Характеристики систем виявлення вторгнень

Компанія D-Link має цікаве рішення, пов'язане зі створенням уніфікованих комутованих локальних мереж (дротових і бездротових), якізабезпечують високу продуктивність при безпечної передачі інформації і масштабованість з можливістю управління і контролю.[18]

Система Уніфікованого Доступу (Unified Access System) - комплексне рішення від компанії D-Link. Дозволяє розгортати безпечні бездротові мережі WLAN (Wireless LAN), забезпечуючи впровадження сучасних бездротових мережевих можливостей, в тому числі безшовний роумінг рівнів L2 та L3 для кінцевих користувачів.

У наведеному на рис. 3.8. прикладі організації локальної мережі точки доступу відділів 1 і 2 управляються комутатором Unified Access.

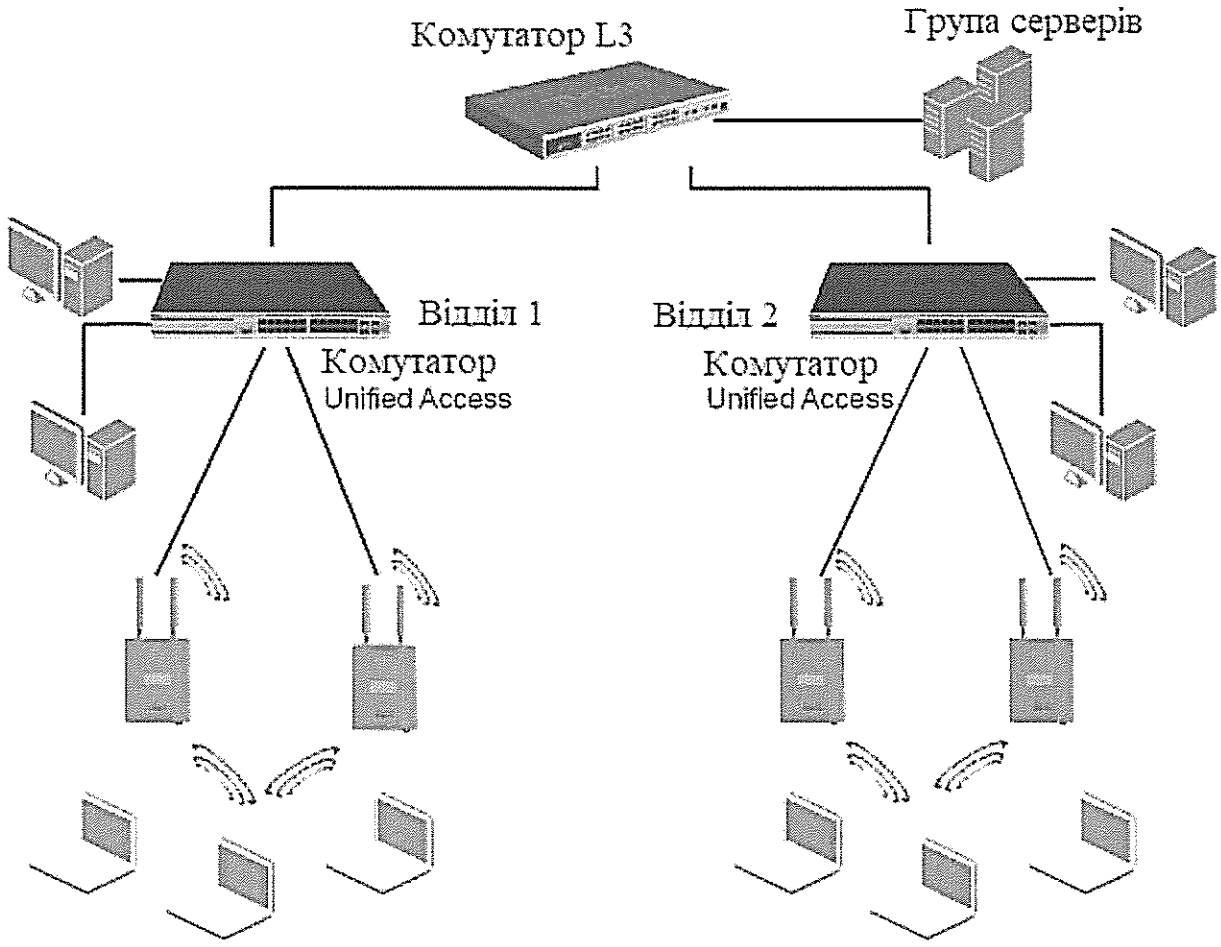



Рис. 3.8. Організація локальної мережі з використанням UnifiedAccessSystem

Компоненти D-Link Unified Access System:

1) Уніфіковані дротові / бездротові комутатори Gigabit Ethernet, серії D-Link DWS-3024 / 3024L / 3026/4026: ;
2) Комутовані бездротові точки доступу типу DWL -8500 / 8600AP - уніфіковані бездротові точки доступу, управління якими здійснюється при підключенні до бездротового комутатора DWS-3024 / 3024L / 3026/4026.[14, 13]

Кожен клієнт, що підключається до бездротової мережі, проходить через процес суворої аутентифікації, що гарантує максимальну безпеку. Неважливо, чиє клієнт постійним користувачем, гостем або просто має доступ до мережі відділу,комутатори DWS-3024 / 3024L / 3026/4026 захищають мережеву інфраструктуру за допомогою великого наборуфункцій безпеки, включаючи: WEP-шифрування даних, WPA / WPA2, аутентифікацію

користувачів 802.1x і стандарт безпеки 802.11i, адаптивний портал і аутентифікацію MAC-адрес.[16]

Комутатори забезпечують визначення і виявлення несанкціонованих точокдоступу для запобігання нелегального вторгнення у внутрішню мережу, а також надають такі сервіси, як членство в віртуальної приватної групі (SSID), аутентифікацію, визначення місцезнаходження та видачу статистики про мережі. Під час роумінгу користувач зберігає авторизацію, тому що всі комутатори DWS- 3024 / 3024L / 3026/4026 мають загальну базу даних, гарантуючи безпечний доступ до відповідних ресурсів мережі. Поряд з перевіркою облікових даних підключаються користувачів в локальній базі даних, також може бути здійснена аутентифікація користувачів на зовнішньому сервері RADIUS.[14]

Крім того, DWS-4026 підтримує новітню функцію Wireless Intrusion Detection System (WIDS), призначену для виявлення несанкціонованих точок доступу і несанкціонованих клієнтів, а також різних загроз безпеки бездротової мережі. За допомогою функції WIDS адміністратори можуть виявити різні загрозиі використовувати сканування радіочастотних каналів для огляду бездротової мережі з метою запобігання будь-яких потенційних загроз безпеки. Для дротових клієнтів DWS-4026 використовує функцію Dynamic ARP Inspection (DAI) і DHCP Snooping для забезпечення максимальної безпеки. Спільне використання функцій Dynamic ARP Inspection (DAI) і DHCP Snooping запобігає загрози найвищого рівня, наприклад, "man-in-the-middle" і ARP poisoning.

Завдяки централізованим радіочастотним політикам, автоматичному вибору найменш використовуваного каналу і балансуванню навантаження точок доступу, комутатори DWS-3024 / 3024L / 3026/4026 можуть ефективно управляти бездротової смугою пропускання для оптимізації трафіку WLAN.

Комутатори підтримують централізовану базу даних з інформацією щодо доступу бездротових користувачів до ресурсів, наприклад, MAC-адреси і ключі аутентифікації. У мережі з декількома комутаторами ця інформація

забезпечується обміном даними між ними. У міру переміщення користувачів по офісу з використанням бездротового обладнання, може змінюватися використовувана для підключення точка доступу.[15, 12]

Провівши аналіз теоретичних даних можна виділити наступні чотири основні загрози безпеці:

- Атаки на ОС і прикладне ПО клієнтів бездротової мережі;
- Перехоплення трафіку при використанні незахищених бездротових з'єднань;
- Атаки «Maninthemiddle», які можуть бути використані для реалізації іншихатак;
- Використання бездротових клієнтів в якості каналу віддаленого доступу докорпоративної мережі.

Дослідження основних протоколів безпеки виявило вразливі місця, через які атакуючий може отримати повний доступ до мережевого трафіку. Найпоширенішими видами атак на Wi-Fi мережі є:

1) Для протоколу WEP:
   - Plaintext-атака;
   - Повторне використання шифра;
   - Атака Fluhrer-Mantin-Shamir;
2) Атака Low-Hanging-Fruit.
3) Для протоколів WPA / WPA2:
   - Атака перебором всіх можливих комбінацій ключа до його визначення;
   - Атака з використанням вразливостей фіксованого пароля;
   - Атаки по словнику;
   - Глушіння клієнтської станції.

4) Для протоколу WPS:

- Перехоплення ключа на основі розбиття пароля навпіл.

Дії зловмисника також можуть бути спрямовані на виведення бездротової

Wi-Fi мережі з ладу. Цьому можуть сприяти деякі проблеми. Ними є, наприклад:

- Можливість проведення атаки на відмову в обслуговуванні на фізичному рівні шляхом глушіння радіосигналу або канальному рівні шляхом експлуатації уразливості методу доступу до несучої;
- Реалізація функції енергозбереження, тобто коли легальний користувач може не отримати чи призначалася йому інформації при виході з режиму очікування;
- Наявність уразливості протоколу аутентифікації PEAP дозволяє послати клієнту помилкові фрейми успішної аутентифікації або від'єднання від мережі.

Використання сучасного обладнання та апаратно-програмних засобів можуть забезпечити відповідний рівень захисту комерційних бездротових локальних мереж Wi-Fi. Але необхідно зазначити, що розглянуті в роботі заходи дають змогу захистити від так званого "силового" методу проникнення до інфраструктури з мережею Wi-Fi, отже, тільки комбінуванням різних методів і підходів можна забезпечити захист від несанкціонованого доступу. Необхідно зазначити також, що найбільше втрат інформації та порушень безпеки відбуваються внаслідок необізнаності та недотримання елементарних правил безпеки корпоративними співробітниками. Однією з таких помилок може бути використання в комерційних цілях публічних точок доступу до мережі Інтернет, неперевіреної техніки, що належить третім особам, чи підозрілого програмного забезпечення. На думку авторів, цікавим напрямом подальшого розвитку є впровадження та використання біометричних систем

безпеки через мобільні пристрої та додатки.

Провівши аналіз та порівнявши особливості вищеописаних методів захисту можна зазначити, що технології обмеження доступу не є надійними при побудові систем захисту комп'ютерних мереж стандарту IEEE 802.11, що ж стосується методів авторизації та шифрування, то лише використання комбінації сучасних протоколів/алгоритмів та коректне налаштування мережевого обладнання дозволяє отримати прийнятний рівень безпеки. В той же час, для створення надійної системи захисту, окрім програмного захисту слід також враховувати необхідність постійного моніторингу роботи мережі, організацію технічного та фізичного захисту.

Пройде, щонайменше, кілька років, до того, як WPA3, Easy Connect і Enhanced Open стануть нормою. Широке поширення WPA3 відбудеться тільки після заміни або поновлення маршрутизаторів. Однак якщо вас турбує безпека вашої особистої мережі, ви зможете замінити свій поточний маршрутизатор на інший, що підтримує WPA3, як тільки виробники почнуть продавати їх, що може статися вже через кілька місяців.

# ВИСНОВКИ

Провівши дослідження щодо розгляду теоретичних засад методів захисту WI-FIмереж, оцінки всіх існуючих на сьогодні методів та технологій, які застосовуються для захисту мереж, можна зробити наступні висновки:

1. Поширення бездротових мереж у світі почалося з впровадження технології 802.11, яка в свою чергу трансформувалася у 802.11b, далі у 802.11g(a), і, нарешті, у 802.11n, яка є останньою розробкою. Оскільки середовище передачі убездротових мережах відкрите (для отримання доступу до мережі потрібно мати лише клієнтський адаптер), дуже важливо організувати захист такої мережі від несанкціонованого доступу.

2. Проведено аналіз наявних методів і способів захисту точок бездротового доступу які відносяться до стандарту IEEE 802.11 (Wi-Fi). Було оглянуто вразливості які в них присутні. Розглянуто сучасні методи атак на бездротові точки доступу та перехоплення даних в них. Проаналізовано вимоги до налаштувань бездротових мереж стандарту IEEE 802.11 які потрібні для створення комплекса протидії зловмисникам. В даний час існують різні способи захисту Wi Fi мереж які були розглянуті і опираючись на які було розроблено сучасний та актуальний комплекс наявних методів для забезпечення максимального захисту бездротових точок доступу Wi-Fi.

3. Для забезпечення високого рівня безпеки бездротових мереж було розроблено комплекс заходів. Бездротова мережа може мати достатній рівень захисту лише при виконанні розглянутих вимог безпеки. Відповідно до високих вимог безпеки бездротову мережу можна вважати захищеною, якщо в ній працюють три основних складових системи безпеки: конфіденційність даних, цілісність даних при їх передачі. аутентифікація користувача . В даний час існують різні способи захисту Wi Fi мереж які були розглянуті і за умови правильного налаштування, э певна гарантія в забезпеченні необхідного рівня безпеки. На даний момент, більш безпечними можна вважати мережі стандарту 802.11, які захищені за допомогою стандарту WPAv2 при умові

використання протоколів EAP різних типів з підтримкою тунелювання і двосторонньої аутентикації обох кінців тунелю. До додаткових типів протоколів EAP відносяться EAP-TLS і EAP-FAST. При цьому, для використання EAP-TLS потрібна наявність сертифікатів аутентифікації на клієнтських пристроях. На основі отриманих даних при обчисленні злому Пін-коду для стандарту WPS можна оцінити складність злому цієї функції. Оскільки увімкнений механізм WPS лише погіршує захищеність точки доступу то комбінація даного механізму навіть з використанням методів аутентифікації стандартів WPA/WPA2 може представляти собою загрозу бездротовій мережі. В даній роботі метод аутентифікації WPA2 представлений як найстійкіший механізм захисту бездротових мереж.

4. В цілому можна згрупувати види атак на бездротові точки доступу Wi-Fi наступним чином:
    - Атака на WEP алгоритм;
    - Злом паролів алгоритмів WPA/WPA2;
    - Злом Пін-коду для стандарту WPS;
    - Пониження WPA алгоритму;
    - Заміна істинної точки доступу фальшивою;
    - Шахрайська точка доступу;
    - Атака на Wi-Fi точки доступу з глобальної та локальної мереж;
    - Атаки виду відмова в обслуговуванні (DoS Wi-Fi).

5. Для запобігання CSRF атак не рекомендовано використовувати IP адреси ідіапазони адрес за замовчуванням. Іншим методом підвищення рівня безпеки бездротових Wi-Fi мереж, є використання статичних ip-адрес для пристроїв. В маршрутизаторах з стандартними налаштуваннями може бути включений сервер DHCP. Під час підключення комп'ютера чи можливо пристрою до бездротової мережі, пристрій робить запит маршрутизатору про

IP-адресу і DHCP-сервер призначає її. Якщо відключити DHCP-сервер, то кожен пристрій повинен бути налагоджений вручну для того, щоб підключитися до мережі Рекомендується використання VLAN мережі для більш надійного захисту мережі, слід також Ивикористовувати мережеві екрани з підвищеними налаштуваннями політики безпеки. Також рекомендується вимкнути IPv6 на маршрутизаторі, або, в разі якщо є необхідність послуги IPv6, необхідно обрати маршрутизатор з сертифікованим IPv6 стандартом. Щодо конфігурації точки бездротового доступу рекомендується не використовувати в цьому випадку веб-браузер. Краще робити такі дії за допомогою SNMP утиліти налаштування, яка йде в комплекті з усіма точками доступу, або telnet-клієнта (або за допомогою підключення до послідовного порту точки доступу), якщо ця можливість передбачена виробником, причому саме з проводового сегмента мережі.

6. Для захисту мереж стандарту 802.11 повинен бути передбачений наступний комплекс заходів щодо безпеки передачі даних. Необхідно встановити маршрутизатор в безпечному місці, де бездротовий сигнал доступний тільки всередині будинку. Рекомендується обновити ПЗ маршрутизатора, щоб виправитийого відомі уразливості. Необхідно вимкнути віддалене управління маршрутизатором через Інтернет. Необхідно використовувати WPA2-шифрування і складний та стійкий пароль. Якщо використовувати простий пароль для шифрування WPA2, то він може бути зламаний.

7. Рекомендовано створювати стійкий пароль, при цьому можна використати генератори пароля чи фразу, яку можливо легко запам'ятати. Цілком відповідним паролем буде являтися пароль в 10-15 символів, бажано з великими і малими буквами та цифрами і рекомендується використати спецсимволи. Якщо використовується шифрування WPA2 з складним паролем і WPS в роутері відключений - мережа в певній мірі достатньо захищена. Необхідно приховувати SSID-ім'я бездротової мережі. Необхідно вимкнути функцію WPS.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Д. Мехед, Ю. Ткач, В. Базилевич, Т. Петренко "Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11", Захист інформації, №4, С. 285–291,2015.

2. О. Юдін, Г. Конахович, О. Корченко, Захист інформації в мережах передачі даних:підруч.К.:Вид-во ТОВНВП“ІНТЕРСЕРВІС”,2009,714с.

3. Tanenbaum A. Комп'ютерні мережі / A. Tanenbaum, D. Wetherall. – Новий Джерсі,Пірсон, 2012. – 959 с. – (5те видання).

4. Wireless LAN (WLAN) [Електронний ресурс]. – 2017. – Режим доступу до мережі: http://www.hitchhikersguidetolearning.com/wireless-lan-wlanarticles/

5. Кіберполіція:захист мереж WI-FI-на дуже низькому рівні,2017.[Електронний ресурс].Режим доступу:https://www.ukrinform.ua/rubric-technology/2281044-kiberpolicia-zahist-merez-wifi-na-duzenizkomu-rivni.html.

6. Пролетарський А.В. Бездротові мережі Wi-Fi/А.В.Пролетарський,І.В.Баскаков,Д.Н.Чирков.-М.: БИНОМ.Лабораторія знань,2007.-178 с.

7. 802.11 b g n методи перевірки. Способи збільшення швидкості з'єднання бездротової мережі Wi-Fi [Електронний ресурс]. – 2016 – Режим доступу до ресурсу: https://reactor-web.ru/uk/80211-b-g-nverification-methods.html

8. WPA2-Enterprise. Як створити безпечну мережу? [Електронний ресурс]. – 2018. - Режим доступу до ресурсу: https://wifisolutions.ru/zashita-korporativnoy-seti-s-wpa2-enterprise/

9. Mathy Vanhoef and Frank Piessens. Release the kraken: new KRACKs in the 802.11 standard. In Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS). ACM, 2018.

10. Підпалий О.І. АНАЛІЗ ВРАЗЛИВОСТІ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI З НОВИМ ПРОТОКОЛОМ ЗАХИЩЕНОСТІ WPA3. XIV Міжнародна

науково-технічна конференція «Перспективи телекомунікацій»; ПТ2020: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2020. – С. 98-102. ISSN(print) 2663-502X

11. Що таке 802.11ax - огляд нового стандарту WI-FI 6 [Електронний ресурс]. – 2017. – Режим доступу до мережі: https://translate.google.com.ua/?hl=ru&sl=ru&tl=uk&text=%D0%A7%D1%82%D0%BE%20%D1%82%D0%B0%D0%BA%D0%BE%D0%B5%20802.11ax%20%E2%80%93%20%D0%BE%D0%B1%D0%B7%D0%BE%D1%80%20%D0%BD%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0%20WI-FI%206&op=translate

12. FrankBulk The ABCs Of WPA2Wi-Fi Security – NetworkComputing, 2006,February 2.–P.65-69.

13. What are IEEE 802.11 Standards? : 802.11a/b/g/n/ac/ax [Електронний ресурс]. – 2017. – Режим доступу до мережі: https://www.signalboosters.com/blog/ieee-802.11-standards-explained802.11abgnacax/

14. IEEE Standard for Information technology – Telecommunications and informationexchangebetweensystems–Localandmetropolitanareanetworks–Specificrequirements. Part 11: Wireless LAN Medium Access Control (MAC) and PhysicalLayer(PHY)specifications.Amendment6:MediumAccessControl(MAC)SecurityEnhancements.–IEEE 802.11i–2004.

15. IEEE 802.11ax TECHNOLOGY INTRODUCTION. // ROHDE&SCHWARZ. – 2019. – С. 36.

16. РоссД.WI-FI.Бездротова мережа,НТІПрес,2007,400-420стр.

17. C.Hoffman,WhyYouShouldn'tUseMACAddressFilteringOnYourWi-FiRouter, 2014. [Electronic resource]. Access mode: https:// www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-macaddress-filtering-on-your-wi-fi-router/.

18. Kulkarni A, Seetharam A, Ramesh A, Herath JD. DeepChannel: передбачення якості бездротового каналу за допомогою глибокого навчання. Трансакції IEEE щодо транспортних технологій 2020; 69 (1): 443-456. doi: 10.1109/TVT.2019.2949954

19. Georgiadis L, Neely MJ, Tassiulas L. Розподіл ресурсів і міжрівневий контроль у бездротових мережах. Бостон, США: Основи та тенденції в мережі,2006.

20. StewardS.Miller.Wi-fiSecurity/StewardS.Miller.–2003.430-463p.

21. RunfuZ.Securityfor Wireless Network Basedon Fuzzy-AHPwithVariableWeight

/ Z. Runfu, H. Lianfen, X. Mingbo // 2010 Second International Conference onNetworks Security, Wireless Communications and Trusted Computing, 24–25 April2010:proceedings.–Wuhan,Hubei,China: IEEE,2010.Vol.2.– P.490–493.

22. Goel R. Wireless Honeypot: Framework, Architectures and Tools / R. Goel, A.Sardana, R. C. Joshi // International Journal of Network Security, 2013. – Vol. 15,No.5.– P.373–383.

23. Методи та засоби аналізу систем-приманок в процесі зламу / [В. Б. Дудикевич,А. З. Піскозуб, Н. П. Тимошик и др.] // Науково-технічний журнал «Захистінформації».– 2009.– № 1.– С.27–31.

24. Cisco Visual Networking Index: Forecast and Methodology, 2013–2018. – CiscoPublic,2014,June10.

25. 19.802.11WirelessNetworksSecurityandAnalysis.HoltA.,Chi-YuHuang.– Springer,2010

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Кафедра мобільних та відеоінформаційних технологій

Студент групи АРДМ-62
Чирва Богдан Миколайович

# УДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ WI-FI МЕРЕЖ ВІД ЗОВНІШНІХ ЗАГРОЗ

Науковий керівник –
Макаренко Анатолій Олександрович

## Мета роботи

Дослідження  підходів щодо захисту WI-FI мереж, їх діагностика із застосуванням технологій WPA та WPA2.

## Об’єкт дослідження

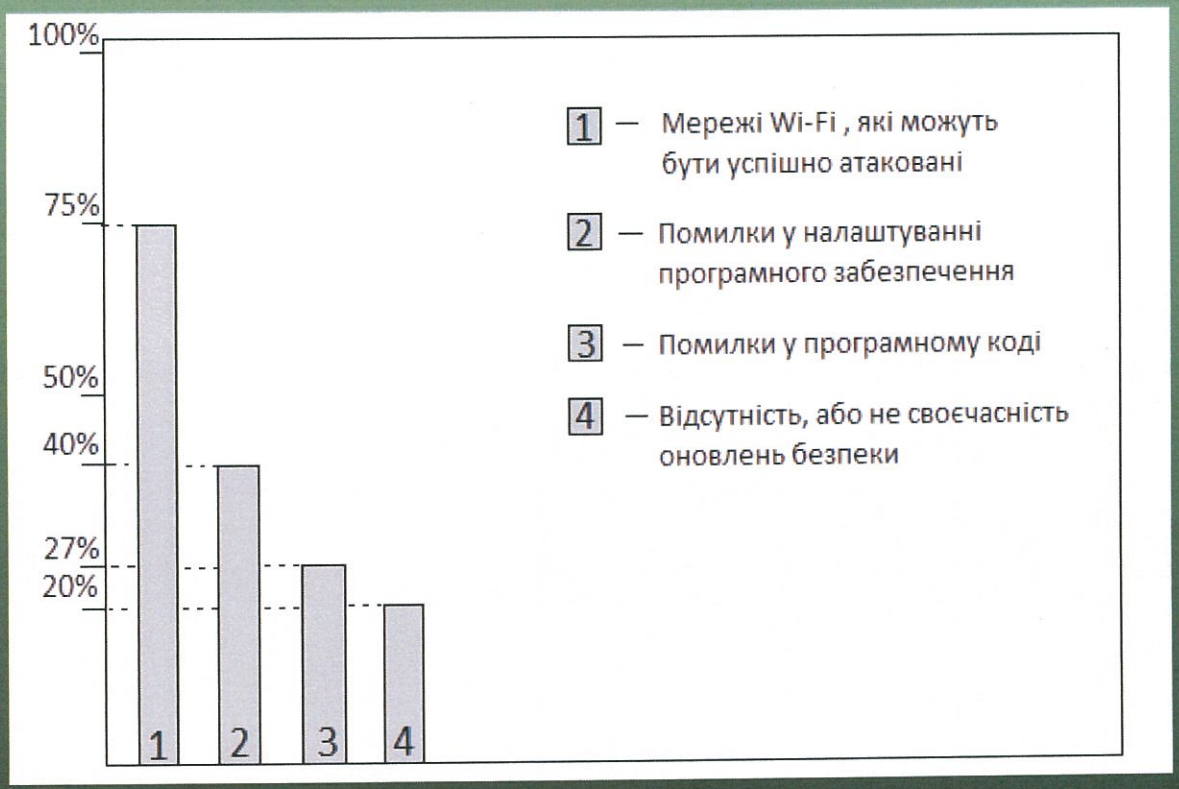
WI-FI мережі та методи їх захисту на основі технологій WPA та WPA2

## Предмет дослідження

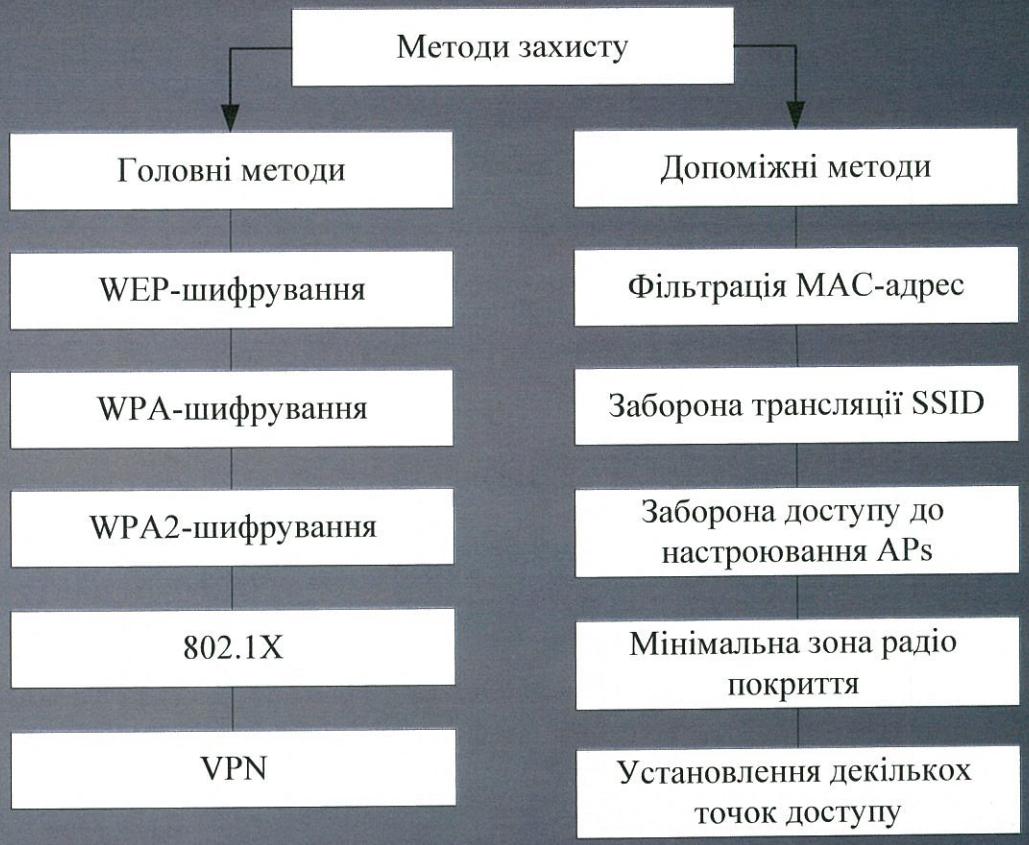
Науково-теоретичні положення і система технічних підходів відносно захисту WI-FI мережі

# Сутність захисту wi-fi мереж та їх специфіка

На сьогоднішній момент захищеність точок доступу Wi-Fi залишається не достатньою. Частково така ситуація пояснюється використанням застарілого апаратного забезпечення, яке не підтримує WPA шифрування.

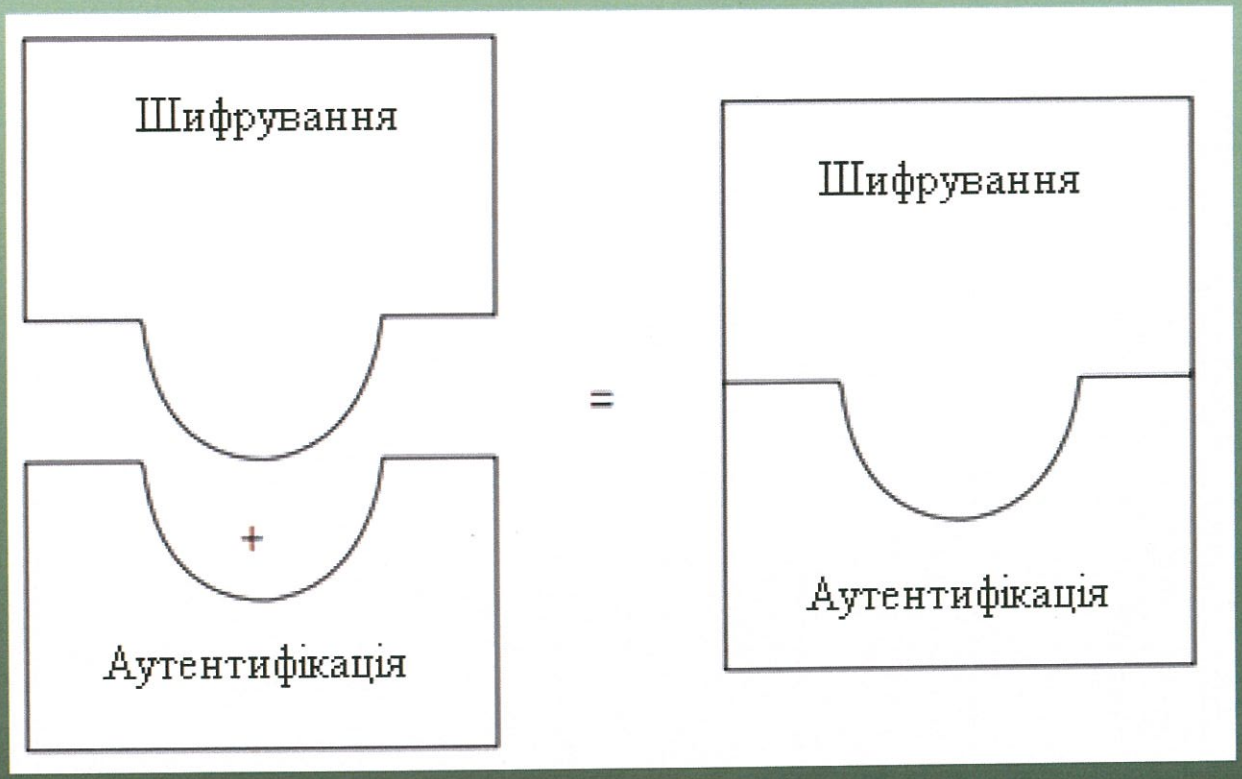


# Класифікація методів захисту WI-FI мереж




Для забезпечення безпеки Wi-Fi мереж використовують різного роду технології обмеження доступу. Найпоширенішими являються фільтрація по MAC-адресах та приховування SSID.

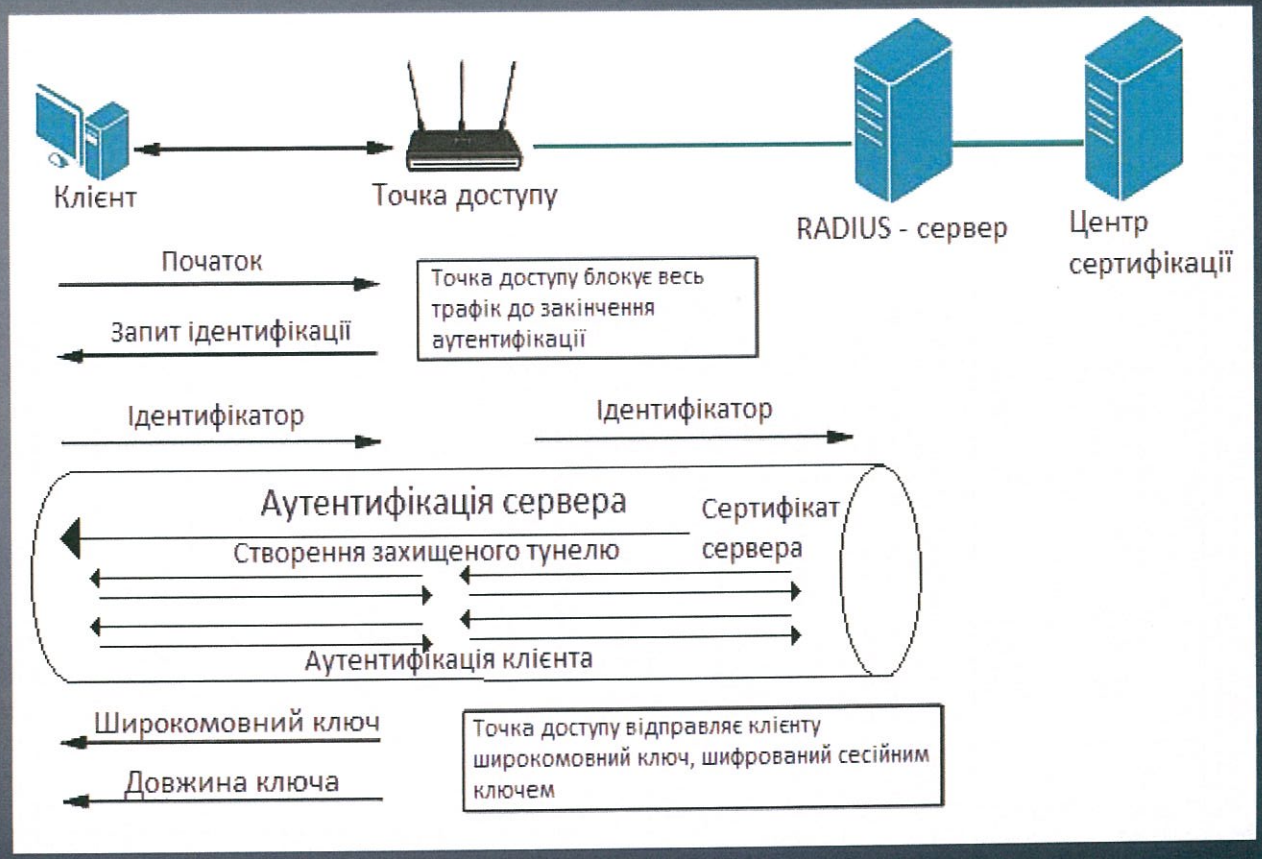
# Характерні риси захисту WI-FI мережі, використовуючи технології WPA та WPA2




Найбільш ефективною є комбінація використання стандарту захисту WPA2 та протоколу шифрування CCMP (який базується на алгоритмі AES) з використанням складного ключа доступу (наприклад 14-и значний набір випадкових цифр та літер).

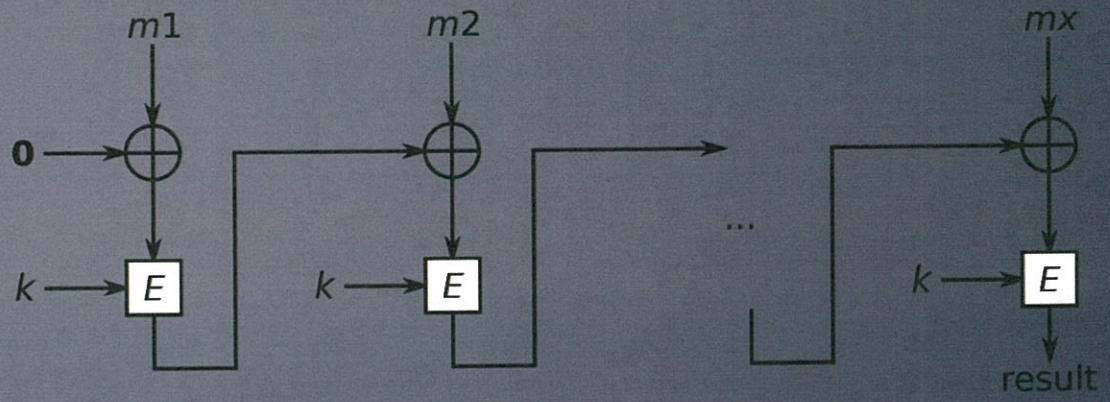
# Механізм захисту WI-FI мережі, із застосуванням технологій WPA та WPA2

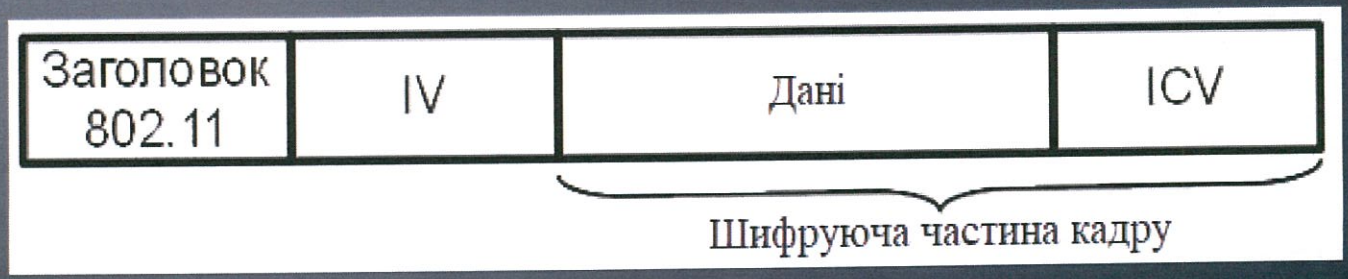
Стандарт IEEE 802.11i (WPA2) розроблений на базі перевірених технологій, однак деякі механізми безпеки були спроектовані з нуля в тісній співпраці з кращими фахівцями з криптографії і вважаються одним з найефективніших рішень проблем захисту бездротових мереж



# Аналіз протоколу шифрування в технологіях WPA та WPA2

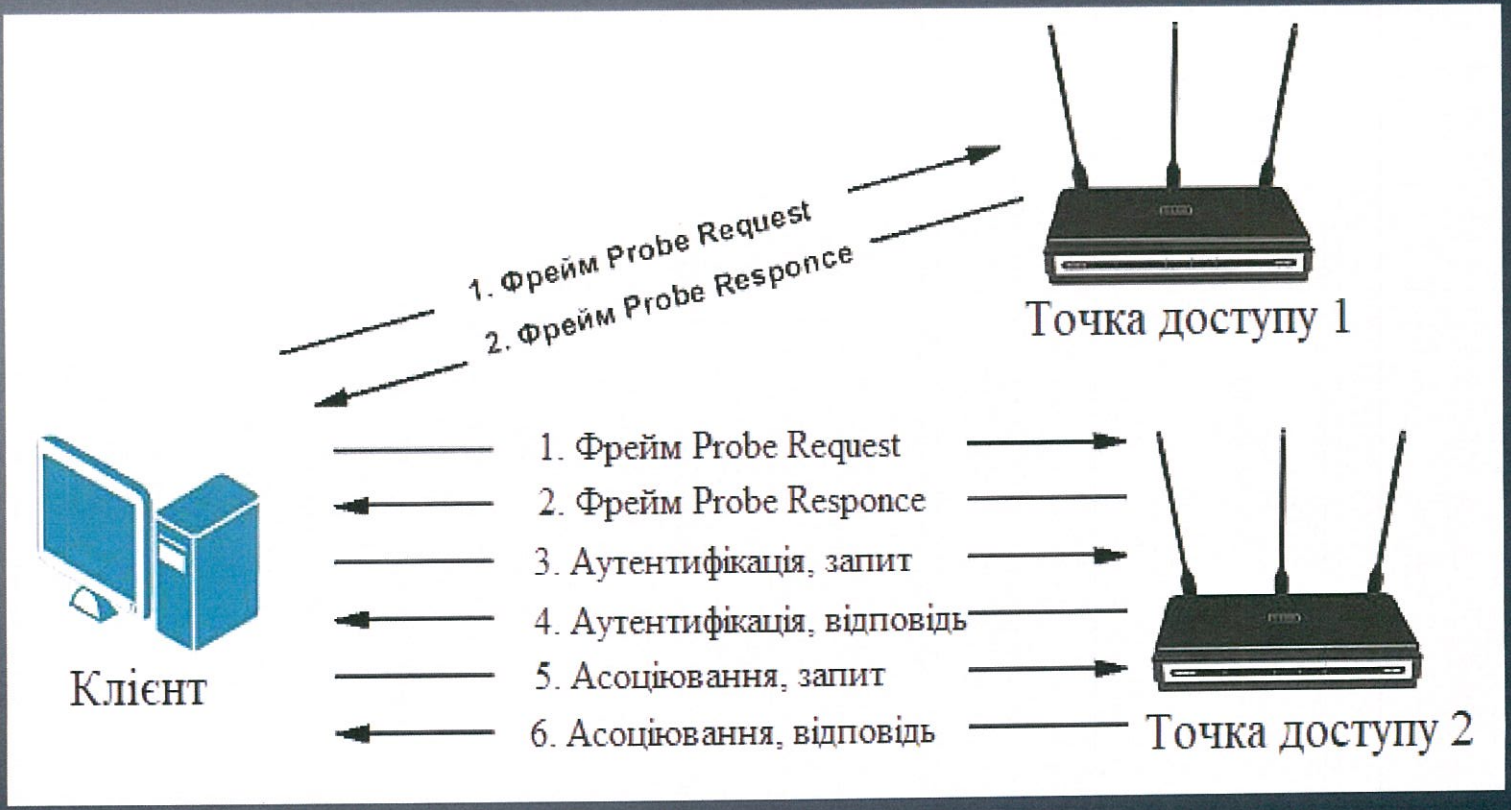
WPA2 використовує протокол CBC-MAC (Cipher Block Chaining Message Authentication Code) для аутентифікації і забезпечення цілісності даних, а для шифрування даних і контрольної суми MIC – режим лічильника (Counter Mode, CTR).



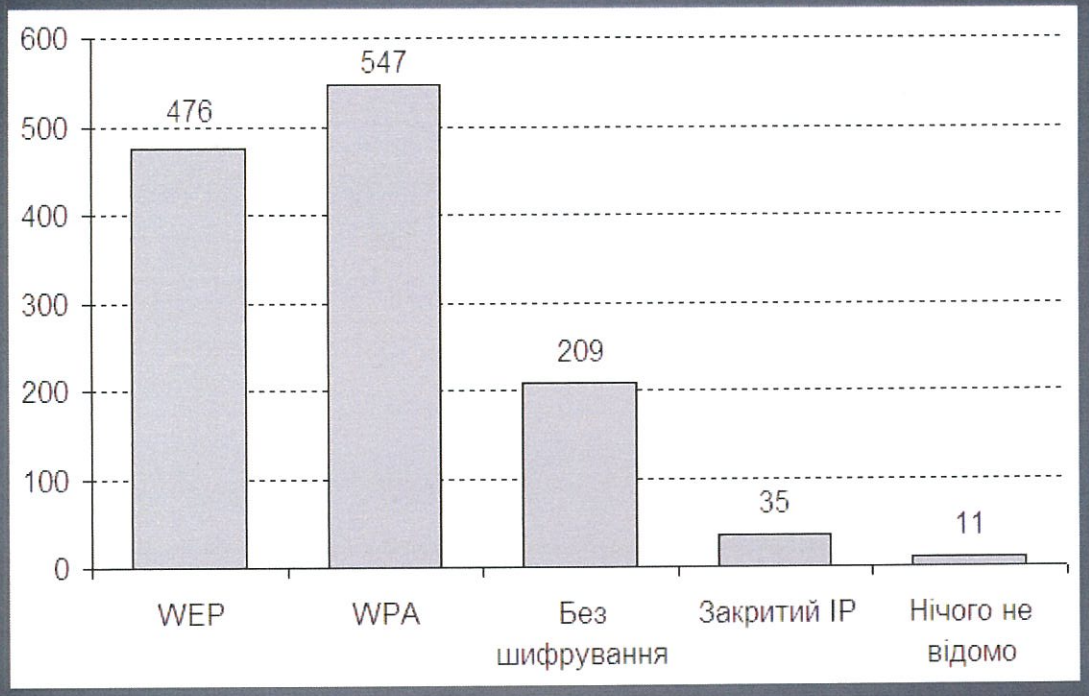



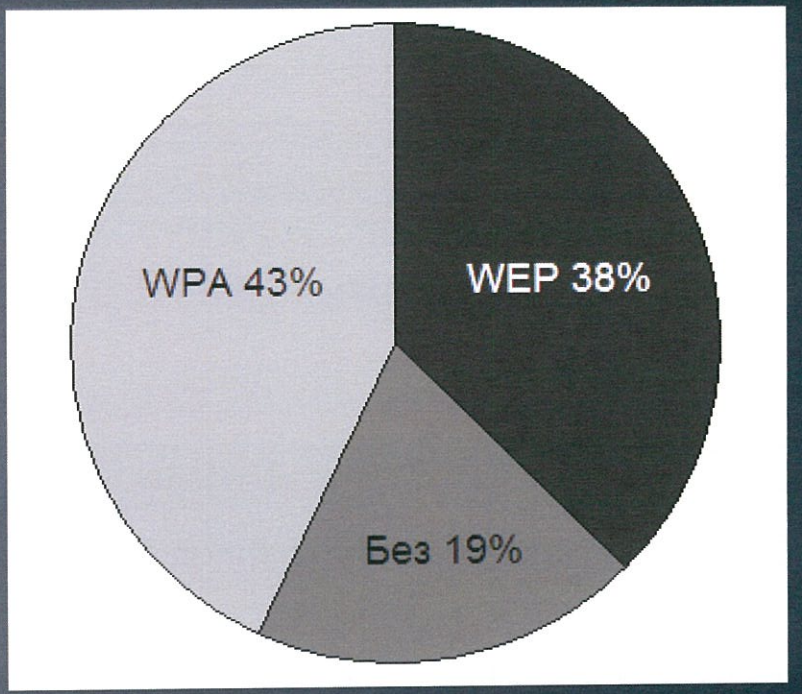
# Оцінка параметрів методу автентифікації WPA та WPA2 для систем і мереж стандарту

WPA2 Personal використовується здебільшого у Small or Home Office (SOHO) мережах. Ключ у механізмі WPA2 Personal є однаковим для всіх користувачів За генерацію пар логін-пароль у WPA2 Enterprise відповідає спеціальний сервер, здебільшого RADIUS.



# Проблеми та напрямки їх вирішення у бездротових локальних мережах WI-FI

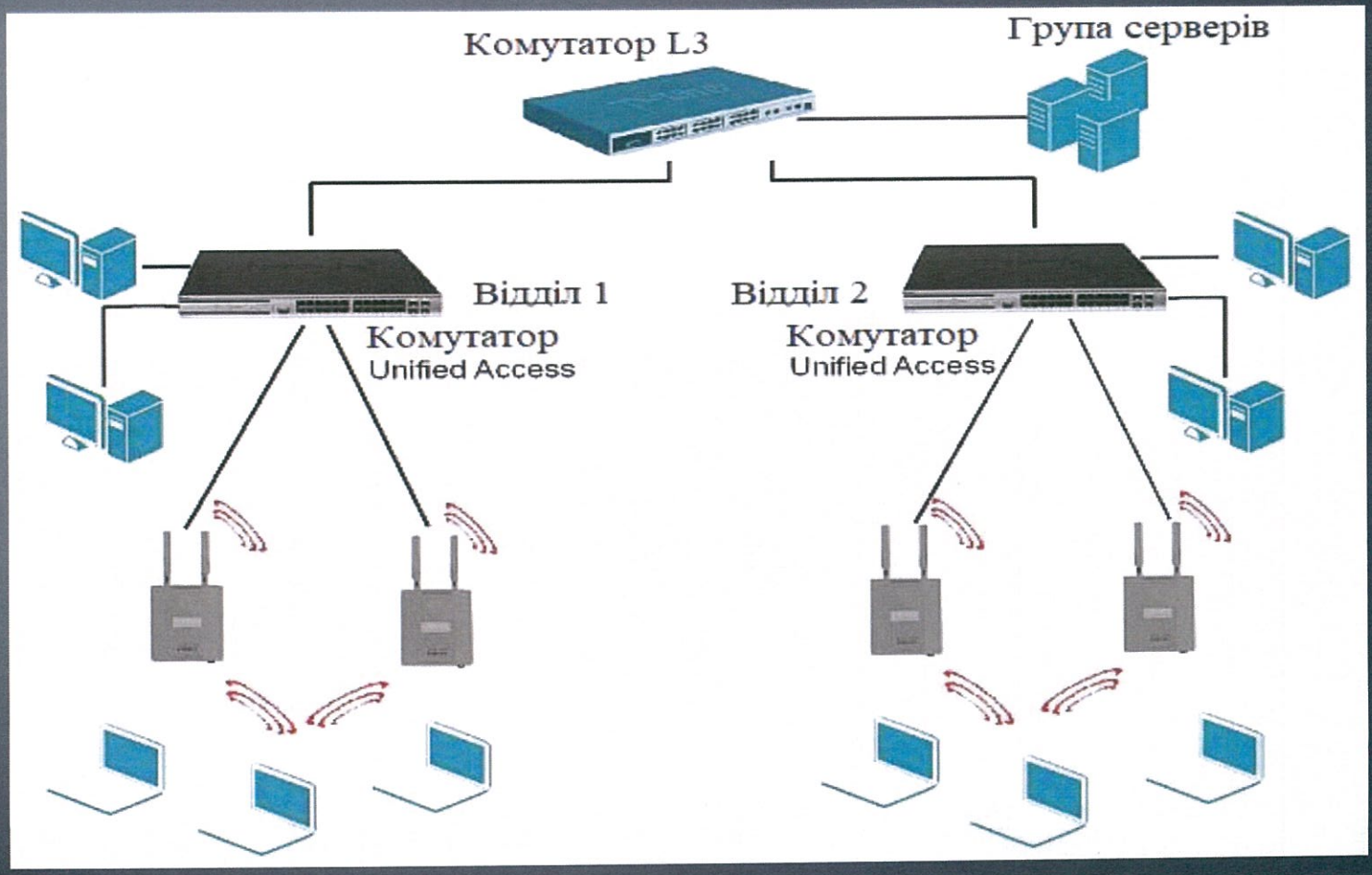


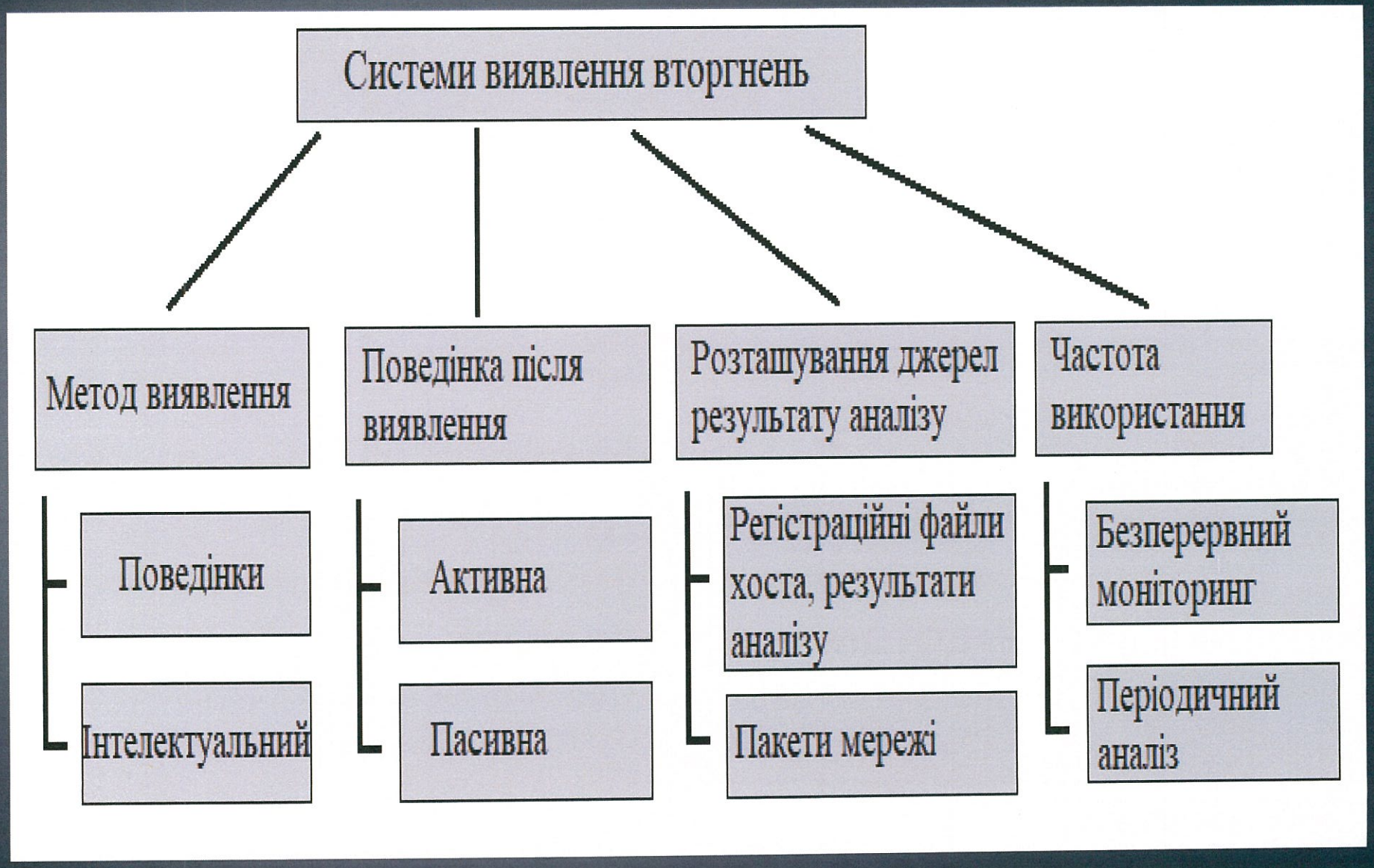

Тільки комбінуванням різних методів і підходів можна забезпечити захист від несанкціонованого доступу.

# Сучасні альтернативні методи захисту

Користувачі WPA3-Personal отримують більш надійну парольну аутентифікацію і захист від брутфорсу навіть в тих випадках, якщо вибирають занадто короткий або простий пароль.



# Сучасні альтернативні методи захисту



# Висновки

Проведено аналіз наявних методів і способів захисту точок бездротового доступу які відносяться до стандарту IEEE 802.11 (Wi-Fi).

Виокремлено вимоги до налаштувань бездротових мереж стандарту IEEE 802.11, які потрібні для створення комплекса протидії зловмисникам.

Для забезпечення високого рівня безпеки бездротових мереж було запропоновано комплекс заходів. На даний момент, більш безпечними можна вважати мережі стандарту 802.11, які захищені за допомогою стандарту WPA2 при умові використання протоколів EAP різних типів з підтримкою тунелювання і двосторонньої аутентикації обох кінців тунелю.

**Протокол аналізу звіту подібності науковим керівником**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Богдан ЧИРВА

**Назва:** Удосконалення методів захисту WI-FI-мереж від зовнішніх загроз

**Координатор:** Анатолій МАКАРЕНКО

**Підрозділ:** ННІТ

**Коефіцієнт подібності 1**:6.5

**Коефіцієнт подібності 2**:3.2

**Тривога:** 27

**Після аналізу Звіту подібності констатую наступне:**

☑ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

*Дата* *Підпис Наукового керівника*