ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до бакалаврської роботи

на тему: **“ Тенденції розвитку засобів захисту інформації бездротових комунікаційних систем”**

Виконав: студент 5 курсу, групи РТЗ-51

спеціальності

172 Телекомунікації і радіотехніка

(шифр і назва спеціальності)

Боярська К.М.

(прізвище та ініціали)

Керівник

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтроль_____

Київ – 2021

РЕФЕРАТ

Текстова частина бакалаврської роботи: 73 сторінок, 50 рисунків, 4 табл., 27 джерел.

Метою роботи є оцінка ризиків стандарту 802.16, з точки зору визначення його вразливостей, загроз та механізмів захисту стандарту.

Об'єктом роботи є вивчення та аналіз побудови стандарту 802.16.

Предметом роботи є аналіз захищеності пристроїв побудованих по технології WiMax.

Метод дослідження – створення і реалізація системи захисту інформації бездротової мережі та вибору надійних технологій і методів захисту.

Короткий зміст роботи: У роботі було розроблено систему захисту інформації бездротової мережі. Визначено основні та обов'язкові правила при організації і налаштуванні системи захисту інформації бездротової мережі. Реалізовано власне програмне забезпечення для побудованої системи захисту у вигляді програми по аналізу трафіка.

Галузь використання – бездротова мережа зв'язку України.

БЕЗДРОТОВА МЕРЕЖА, ЗАГРОЗА, АТАКА, ВРАЗЛИВІСТЬ, АУТЕНТИФІКАЦІЯ, ПРОТОКОЛ БЕЗПЕКИ, СИСТЕМА ЗАХИСТУ, МЕТОДИ ЗАХИСТУ, ПОЛІТИКА БЕЗПЕКИ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, МОДЕЛЬ ЗАГРОЗ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ARP - Address Resolution Protocol - протокол перетворення адрес;

DMZ - демілітаризована зона;

DOS - Denial of Service - відмова в обслуговуванні;

FDM - Frequency Division Multiplexing - ущільнення з частотним розділенням;

IDS - Intrusion Detection System - системи виявлення вторгнень;

IEEE - Institute of Electrical and Electronics Engineers - Інститут інженерів з електротехніки та електроніки;

IKE - Internet Key Exchange - схеми обміну ключами через Інтернет;

IV - Initialization Vector - вектор ініціалізації;

MIC - Message Intgrity Check – перевірка цілісності повідомлень;

OFDM - Orthogonal Frequency Division Multiplexing - механізм мультиплексування за допомогою ортогональних несучих частот;

OSI - Open Systems Interconnection - мережева модель взаємодії відкритих мереж;

RADIUS - Remote Authentication Dial-In User Service - протокол для реалізації аутентифікації, авторизації та збору відомостей про використані ресурси;

RSN - Robust Security Network - концепція підвищення безпеки;

SOHO - Small Office / Home Office – «малий офіс/домашній офіс»;

TDM - Time Division Multiplexing) - ущільнення з тимчасовим поділом;

TKIP - Temporal Key Integrity Protocol - тимчасовий протокол інтеграції ключа;

VPN - Virtual Private Network - віртуальна приватна мережа;

WDS - Wireless Distributed System - бездротова система розподілу;

БМ – бездротова мережа;

НСД - несанкціонований доступ;

СБЗ - Системи безпроводового зв’язку;

СЗІ – система захисту інформації;

СЗІ БМ – система захисту інформації бездротової мережі;

ВСТУП

Актуальність: Дана робота присвячена розгляду забезпечення захисту безпроводових мереж WiMax, вразливості таких мереж та криптографічні алгоритми захисту даних, що циркулюють у мережі.

Метою роботи є оцінка ризиків стандарту 802.16, з точки зору визначення його вразливостей, загроз та механізмів захисту стандарту.

Об'єктом роботи є вивчення та аналіз побудови стандарту 802.16.

Предметом роботи є аналіз захищеності пристроїв побудованих по технології WiMax.

Метод дослідження – створення і реалізація системи захисту інформації бездротової мережі та вибору надійних технологій і методів захисту.

WiMax (англ. Worldwide Interoperability for Microwave Access) — телекомунікаційна технологія, розроблена з метою надання універсальному безпровідному зв'язку на великих відстанях для широкого спектру пристроїв (від робочих станцій і портативних комп'ютерів до мобільних телефонів). Заснована на стандарті IEEE 802.16, який також називають Wireless MAN. Назва «WiMax» була створена WiMax Forum — організацією, яка була заснована в червні 2001 року з метою просування і розвитку технології WiMax. Форум описує WiMax як «засновану на стандарті технологію, що надає високошвидкісний безпровідний доступ до мережі, альтернативний виділеним лініям і DSL»

При переході до створення систем широкосмугового радіодоступу з інтеграцією послуг стало зрозуміло, що основні принципи, закладені в безпровідникові системи на попередніх етапах, потребують значної корекції. З цією метою в 2004 році був розроблений стандарт IEEE 802.16, що являє собою розраховану на введення в міських бездротових мережах (WirelessMAN) технологію без провідного широкосмугового доступу операторського класу. Часто використовується комерційна назва стандарту WiMax(Worldwide Interoperability for Microwave Access), що походить від назви міжнародної організації WiMax Forum, в яку входять ряд передових комунікаційних і напівпровідникових компаній.

Основне призначення даних мереж - це надання послуг абонентам по високошвидкісній і високоякісний безпровідній передачі даних, голосу і відео на відстані в декілька десятків кілометрів. У жовтні 2007 року International Telecommunication Union (ITU-R) включив технологію WiMax стандарту IEEE 802.16 в сімейство стандартів мобільного зв'язку 3G. У мережах WiMax реалізовані найостанніші досягнення науки і техніки в області радіозв'язку, телекомунікацій і комп'ютерних мереж. Стандарт IEEE 802.16 визначає застосування:

– на фізичному рівні широкосмугового радіосигналу OFDM з множиною піднесучих;

– на канальному рівні використовується сучасний протокол множинного (багатостанційного) доступу Time Divion Multiply Access (TDMA) і Scalable OFDM Access (SOFDMA);

– на мережевому (транспортному) рівні в мережах WiMax застосовується IP-протокол передачі даних, що широко використовуваний в більшості сучасних мережах передачі даних, зокрема, в мережі Інтернет.

В більшості випадків проектування мереж WiMax є досить складним і неоднозначним процесом. Розрахунок покриття відбувається на основі вимірювань рівня завад на місцевості, що потребує значних витрат коштів та часу. В даній роботі пропонується метод оцінки параметрів системи WiMax на основі математичної моделі. Даний математичний апарат, в деякій мірі, може полегшити процес розрахунку покриття.

1. АНАЛІЗ СУЧАСНИХ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ

1.1 Основи бездротових мереж передачі данних

1.1.1 Основні елементи мережі

Для побудови бездротової мережі використовуються Wi-Fi адаптери та точки доступу. Адаптер (рис. 1.1) являє собою пристрій, який підключається через слот розширення PCI, PCMCIA, CompactFlash. Існують також адаптери з підключенням через порт USB 2.0. Wi-Fi адаптер виконує ту ж функцію, що і мережева карта в дротовій мережі. Він служить для підключення комп'ютера користувача до бездротової мережі. Завдяки платформі Centrino всі сучасні ноутбуки мають вбудовані адаптери Wi-Fi, сумісні з багатьма сучасними стандартами. Wi-Fi адаптерами, як правило, забезпечені і КПК (кишенькові персональні комп'ютери), що також дозволяє підключати їх до бездротових мереж. [6]

Для доступу до бездротової мережі адаптер може встановлювати зв'язок безпосередньо з іншими адаптерами. Така мережа називається бездротовою одноранговою мережею або Ad Hoc. Адаптер також може встановлювати зв'язок через спеціальний пристрій - точку доступу. Такий режим називається інфраструктурним. Для вибору способу підключення адаптер повинен бути налаштований на використання або Ad Hoc, або інфраструктурного режиму.

Точка доступу на рис. 1.2 являє собою автономний модуль з вбудованим мікрокомп'ютером і приймально-передавальним пристроєм.

Рис.1.1 Адаптери

Через точку доступу здійснюється взаємодія та обмін інформацією між бездротовими адаптерами, а також зв'язок з проводовим сегментом мережі. Таким чином, точка доступу грає роль комутатора.

Рис. 1.2 Точка доступу

Точка доступу може використовуватися як для підключення до неї клієнтів, так і для взаємодії з іншими точками доступу з метою побудови розподіленої мережі (Wireless Distributed System - WDS). Це режими бездротового мосту "точка-точка" і "точка - багато точок", бездротовий клієнт і повторювач. [2]

Доступ до мережі забезпечується шляхом передачі сигналів через ефір. Приймаюча станція може отримувати сигнали в діапазоні роботи декількох передавальних станцій. Станція-приймач використовує ідентифікатор зони обслуговування (Service Set IDentifier - SSID) для фільтрації одержуваних сигналів і виділення того, який їй потрібен. [6] Зоною обслуговування (Service Set - SS) називаються логічно згруповані пристрої, що забезпечують підключення до бездротової мережі. Базова зона обслуговування (Basic Service Set - BSS) - це група станцій, які зв'язуються одна з одною по бездротовому зв'язку. Технологія BSS припускає наявність особливої станції, яка називається точкою доступу [4].

1.1.2 Методи доступу до середовища в бездротових мережах

Одна з основних проблем побудови бездротових систем - це вирішення завдання доступу багатьох користувачів до обмеженого ресурсу середовища передачі. Існує кілька базових методів доступу, заснованих на поділі між станціями таких параметрів, як простір, час, частота та код. Завдання ущільнення - виділити кожному каналу зв'язку простір, час, частоту і/або код з мінімумом взаємних перешкод і максимальним використанням характеристик середовища передачі [7].

Ущільнення з просторовим поділом

Засноване на поділі сигналів в просторі, коли передавач посилає сигнал, використовуючи код c, час t і частоту f області s_i. Тобто кожний бездротовий пристрій може вести передачу даних тільки в межах певної території, на якій будь-якому іншому пристрою заборонено передавати свої повідомлення [12].

Наприклад, якщо радіостанція веде мовлення на чітко визначеній частоті та на закріпленій за нею території, а будь-яка інша станція в цій же місцевості також почне транслювати на тій же частоті, слухачі радіопередач не зможуть отримати "чистий" сигнал ні від однієї з цих станцій. Інша справа, якщо радіостанції працюють на одній частоті в різних містах. Спотворень сигналів кожної радіостанції не буде у зв'язку з обмеженою дальністю поширення сигналів цих станцій, що виключає їх накладення один на одного. Характерний приклад - системи стільникового телефонного зв'язку.[15]

Ущільнення з частотним розділенням (Frequency Division Multiplexing - FDM)

Кожен пристрій працює на певній частоті, завдяки чому кілька пристроїв можуть вести передачу даних на одній території (рис. 1.3). Це один з найбільш

відомих методів, так чи інакше використовується в самих сучасних системах бездротового зв'язку.

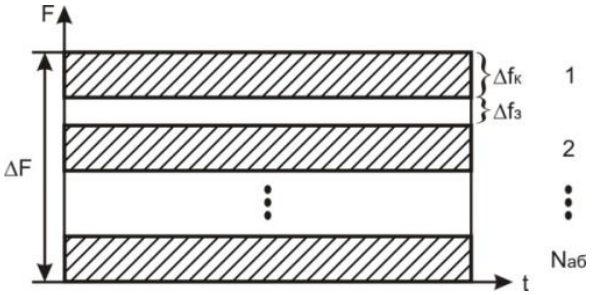

Рис. 1.3 Принцип частотного розділення каналів

Ця схема, хоч і дозволяє використовувати безліч пристроїв на певній території, сама по собі призводить до невиправданого марнотратства зазвичай мізерних частотних ресурсів, оскільки вимагає виділення своєї частоти для кожного бездротового пристрою.

Ущільнення з тимчасовим поділом (Time Division Multiplexing - TDM)

У даній схемі розподіл каналів йде за часом, тобто кожен передавач транслює сигнал на одній і тій же частоті області s, але в різні проміжки часу при суворих вимогах до синхронізації процесу передачі (рис. 1.4). [12]

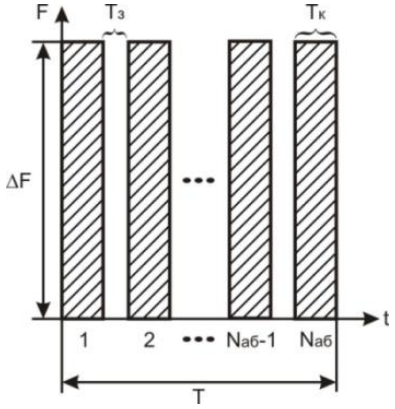

Рис. 1.4 Принцип тимчасового поділу каналів

Подібна схема досить зручна, так як тимчасові інтервали можуть динамічно перерозподілятися між пристроями мережі. Пристроям з великим трафіком призначаються більш тривалі інтервали, ніж пристроїв з меншим обсягом трафіку.

Основний недолік систем з тимчасовим ущільненням - це миттєва втрата інформації при зриві синхронізації в каналі, наприклад через сильні перешкоди, випадкові чи навмисні. Проте успішний досвід експлуатації таких знаменитих TDM-систем, як стільникові телефонні мережі стандарту GSM, свідчить про достатню надійність механізму тимчасового ущільнення. [20]

Ущільнення з кодовим поділом (Code Division Multiplexing - CDM)

У даній схемі всі передавачі транслюють сигнали на одній і тій же частоті f, в області s і за час t, але з різними кодами C_i. Також у схемі CDM кожен передавач

замінює кожен біт вихідного потоку даних на CDM-символ - кодову послідовність довжиною в 11, 16, 32, 64 і т. п. біт (їх називають чіпами). Кодова послідовність унікальна для кожного передавача. Як правило, якщо для заміни "1" у вихідному потоці даних використовують якийсь CDM-код, то для заміни "0" застосовують той самий код, але інвертований. [12]

Приймач знає CDM-код передавача, сигнали якого повинен сприймати. Він постійно бере всі сигнали і оцифровує їх. Потім у спеціальному пристрої (кореляторі) проводиться операція згортки (множення з накопиченням) вхідного оцифрованого сигналу з відомим йому CDM-кодом і його інверсією. У дещо спрощеному вигляді, це виглядає як операція скалярного добутку вектора вхідного сигналу і вектора з CDM-кодом. Якщо сигнал на виході коррелятора перевищує деякий встановлений граничний рівень, приймач вважає, що прийняв 1 або 0. Для збільшення ймовірності прийому передавач може повторювати посилку кожного біта кілька разів. При цьому сигнали інших передавачів з іншими CDM-кодами приймач сприймає як адитивний шум. Більш того, завдяки великій надмірності (кожен біт замінюється десятками чіпів), потужність прийнятого сигналу може бути порівнянна з інтегральною потужністю шуму. Подібності CDM-сигналів з випадковим (гауссових) шумом домагаються, використовуючи CDM-коди, породжені генератором псевдовипадкових послідовностей. Тому даний метод ще називають методом розширення спектру сигналу за допомогою прямої послідовності (DSSS - Direct Sequence Spread Spectrum).[20]

Механізм мультиплексування за допомогою ортогональних несучих частот (Orthogonal Frequency Division Multiplexing - OFDM)

Суть цього механізму: весь доступний частотний діапазон розбивається на досить багато піднесучих (від кількох сотень до тисяч). Одному каналу зв'язку (приймача і передавача) призначають для передачі кілька таких несучих, вибраних з множини за певним законом. Передача ведеться одночасно по всіх піднесучих, тобто в кожному передавачі вихідний потік даних розбивається на N субпотоків, де N - число піднесучих, призначених даним передавачем. Розподіл піднесучих в ході роботи може динамічно змінюватися, що робить даний механізм не менш гнучким, ніж метод тимчасового ущільнення. [15]

Схема OFDM має кілька переваг. По-перше, до селективного завмирання будуть схильні тільки деякі підканали, а не весь сигнал. Якщо потік даних захищений кодом прямого виправлення помилок, то з цим завмиранням легко боротися. По-друге, що більш важливо, OFDM дозволяє подавити міжсимвольну інтерференцію. Міжсимвольна інтерференція надає значний вплив при високих швидкостях передачі даних, так як відстань між бітами (або символами) мала. У схемі OFDM швидкість передачі даних зменшується в N разів, що дозволяє збільшити час передачі символу в N разів. Таким чином, якщо час передачі символу

для вихідного потоку становить T_s, то період сигналу OFDM буде дорівнює NT_s. Це дозволяє істотно знизити вплив міжсимвольних перешкод. При проектуванні системи N вибирається таким чином, щоб величина NTs значно перевищувала середньоквадратичний розкид затримок каналу [15].

1.2 Архітектура IEEE 802.11

Самий популярний стандарт бездротових локальних мереж - IEEE 802.11. Інститут інженерів з електротехніки та електроніки IEEE (Institute of Electrical and Electronics Engineers) сформував робочу групу для бездротових локальних мереж 802.11 в 1990р. Ця група зайнялася розробкою загального стандарту для радіоустаткування і мереж, що працюють на частоті 2,4 Ггц, з швидкостями доступу 1 і 2 Мбіт / с. Роботи зі створення стандарту були завершені через 7 років, і в червні 1997 р.була ратифікована перша специфікація 802.11. Стандарт IEEE 802.11 був першим стандартом продуктів WLAN від незалежної міжнародної організації, що розробляє більшість стандартів для провідних мереж. [14]

Стек протоколів IEEE 802.11

Природно, стек протоколів стандарту IEEE 802.11 відповідає загальній структурі стандартів комітету 802. Як і у всіх технологій сімейства 802, технологія 802.11 визначається двома нижніми рівнями, тобто фізичним рівнем і рівнем MAC, а рівень LLC виконує свої стандартні загальні для всіх технологій LAN функції [27].

На фізичному рівні існує кілька варіантів специфікацій, які відрізняються використовуваним частотним діапазоном, методом кодування і як наслідок - швидкістю передачі даних. Всі варіанти фізичного рівня працюють з одним і тим же алгоритмом рівня MAC, але деякі часові параметри рівня MAC залежать від використовуваного фізичного рівня [14].

Рівень доступу до середовища стандарту 802.11

У мережах 802.11 рівень MAC забезпечує два режими доступу до середи:

• розподілений режим DCF (Distributed Coordination Function);

• централізований режим PCF (Point Coordination Function). [13]

1) Розподілений режим доступу DCF

Режим доступу DCF вимагає синхронізації станцій. Це досягається тим, що тимчасові інтервали починають відраховуватися від моменту закінчення передачі чергового кадру (рис. 1.5). Це не вимагає передачі яких-небудь спеціальних синхронизуючих сигналів і не обмежує розмір пакету розміром слота, так як слоти приймаються до уваги тільки при прийнятті рішення про початок передачі кадру. [14]

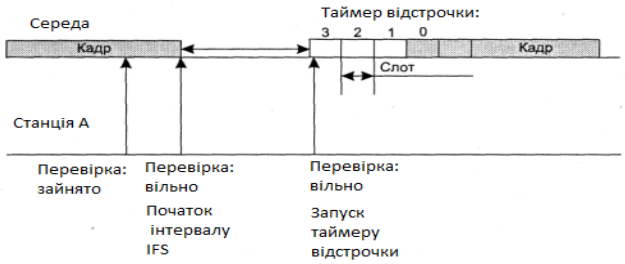

Рис. 1.5 Режим доступу DCF

2) Централізований режим доступу PCF

У тому випадку, коли в мережі є станція, що виконує функції точки доступу, може також застосовуватися централізований режим доступу PCF, який забезпечує пріоритетне обслуговування трафіку. У цьому випадку говорять, що точка доступу грає роль арбітра середовища. Режим доступу PCF в мережах 802.11 співіснує з режимом DCF [5]. Обидва режими координуються за допомогою трьох типів міжкадрових інтервалів.

Після звільнення середовища кожна станція відраховує час простою середовища, порівнюючи його з трьома значеннями:

- короткий міжкадровий інтервал (Short IFS - SIFS);
- міжкадровий інтервал режиму PCF (PIFS);
- міжкадровий інтервал режиму DCF (DIFS). [13]

На керованому інтервалі реалізується централізований метод доступу PCF. Арбітр виконує процедуру опитування, щоб по черзі надати кожній такій станції право на використання середовища, направляючи їй спеціальний кадр [26]. Станція, отримавши такий кадр, може відповісти іншим кадром, який підтверджує прийом спеціального кадру і одночасно передає дані.

Для того щоб якась частка середовища завжди діставалася асинхронному трафіку, тривалість контрольованого періоду обмежена. Після його закінчення арбітр передає відповідний кадр і починається неконтрольований період. Кожна станція може працювати в режимі PCF, для цього вона повинна підписатися на дану послугу за приєднання до мережі. [13]

Кадр MAC-підрівня

На рис. 1.6 зображений формат кадру 802.11, де FC – управління кадром; D/I – ідентифікатор тривалості/з’єднання; SC – управління послідовності. Наведена загальна структура застосовується для всіх інформаційних і керуючих кадрів, хоча не всі поля використовуються у всіх випадках.

FC	D/I	Адреса	Адреса	Адреса	SC	Адреса	Тіло кадру	CRC

Рис. 1.6 Формат кадру MAC IEEE 802.11

Перерахуємо поля загального кадру:

- Управління кадром. Вказується тип кадру і надається управляюча інформація, що управляє (пояснюється нижче).
- Ідентифікатор тривалості/з'єднання. Якщо використовується поле тривалості, вказується час (у мікросекундах), на яке потрібно виділити канал для успішної передачі кадру MAC. У деяких кадрах управління в цьому полі вказується ідентифікатор асоціації або з'єднання.
- Адреси. Число і значення полів адреси залежить від контексту. Можливі наступні типи адреси: джерела, призначення, передавальної або приймаючої станції.
- Управління черговістю. Містить 4-бітове підполе номера фрагмента, що використовується для фрагментації і повторної зборки, і 12-бітовий порядковий номер, який використовується для нумерації кадрів, переданих між приймачем і передавачем.
- Тіло кадру. Містить модуль даних протоколу LLC або керуючу інформацію MAC.
- Контрольна послідовність кадру. 32-бітова перевірка парності з надлишковістю [25].

Версія протоколу	Тип	Підтип	До DS	Від DS	MF	RT	PM	MD	W	0

DS – система розподілу
DS – більше фрагментів
RT – повтор
PM – управління потужністю
MD – більше даних
W – біт захисту дротового еквіваленту
0 - порядок

Рис. 1.7 Поле управління кадром.

Поле управління кадром, показане на рис. 1.7, складається з наступних полів:

- Версія протоколу. Версія 802.11, поточна версія - 0.
- Тип. Визначимо тип кадру: контроль, управління або дані.
- Підтип. Подальша ідентифікація функцій кадру.
- До DS. Координаційна функція MAC присвоює цьому біту значення 1, якщо кадр призначений розподільчій системі.
- Від DS. Координаційна функція MAC присвоює цьому біту значення 0, якщо кадр виходить від розподільної системи.
- Більше фрагментів. 1, якщо за даними фрагментом слідують ще кілька.
- Потім. 1, якщо даний кадр є повторною передачею попереднього.

- Управління потужністю. 1, якщо передавальна станція знаходиться в режимі очікування.
- Більше даних. Вказує, що станція передала не всі дані. Кожен блок даних може передаватися як один кадр або як група фрагментів в декількох кадрах.
- WEP. 1, якщо реалізований алгоритм конфіденційності проводового еквівалента (Wired Equivalent Privacy - WEP).
- Порядок. 1, якщо використовується послуга суворого впорядкування, яка вказує адресату, що кадри повинні оброблятися строго по порядку [14].

1.3 Стандарти IEEE 802.11

Основне призначення фізичних рівнів стандарту 802.11 - забезпечити механізми бездротової передачі для підрівня MAC, а також підтримувати виконання вторинних функцій, таких як оцінка стану бездротового середовища та повідомлення про нього підрівню MAC. Рівні MAC і PHY розроблялися так, щоб вони були незалежними [6].

Кожен з фізичних рівнів стандарту 802.11 має два підрівні:

- Physical Layer Convergence Procedure (PLCP). Процедура визначення стану фізичного рівня.
- Physical Medium Dependent (PMD). Підрівень фізичного рівня, що залежить від середовища передачі. [14]

На рис.1.8 показано, як ці підрівні співвідносяться між собою і з вищезазначеними рівнями в моделі взаємодії відкритих систем (Open System Interconnection - OSI).

Підрівень PLCP по суті є рівнем забезпечення взаємодії, на якому здійснюється переміщення елементів даних протоколу MAC (MAC Protocol Data Units - MPDU) між MAC-станціями з використанням підрівня PMD, на якому реалізується той чи інший метод передачі і прийому даних через бездротову середу. Підрівні PLCP та PMD відрізняються для різних варіантів стандарту 802.11 [13].

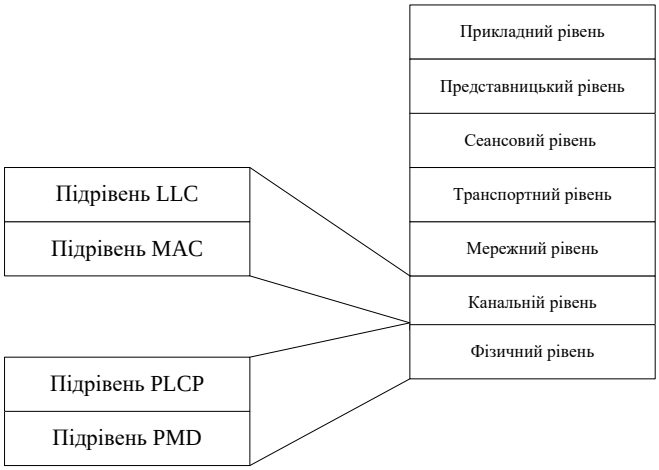

Рис. 1.8 Підрівні рівня PHY

Скремблювання (перестановка елементів) - це метод, за допомогою якого прийняті дані робляться більш схожими на випадкові; досягається це шляхом перестановки бітів послідовності таким чином, щоб перетворити її із структурованої в схожу на випадкову. Цю процедуру іноді називають "відбілюванням потоку даних". Дескремблер приймача потім виконує зворотнє перетворення цієї випадкової послідовності з метою отримання вихідної структурованої послідовності. Більшість способів скремблювання відноситься до числа самосинхронізуючихся; це означає, що дескремблер здатний самостійно синхронізуватися з скремблером [11].

IEEE 802.11

Вихідний стандарт 802.11 визначає три методи передачі на фізичному рівні:

- Передача в діапазоні інфрачервоних хвиль.
- Технологія розширення спектру шляхом стрибкоподібної перебудови частоти (FHSS) у діапазоні 2,4 ГГц.
- Технологія широкосмугової модуляції з розширенням спектру методом прямої послідовності (DSSS) у діапазоні 2,4 ГГц. [6]

Передача в діапазоні інфрачервоних хвиль

Середовищем передачі є інфрачервоні хвилі діапазону 850 нм, які генеруються або напівпровідниковим лазерним діодом, або світлодіодом (LED). Так як інфрачервоні хвилі не проникають через стіни, зона покриття LAN обмежується зоною прямої видимості. Стандарт передбачає три варіанти розповсюдження випромінювання: ненаправлену антену, відбиття від стелі і фокусне направлене випромінювання. У першому випадку вузький промінь розсіюється за допомогою системи лінз. Фокусне направлене випромінювання призначено для організації двохточкового зв'язку, наприклад між двома будівлями. [15]

Бездротові локальні мережі з стрибкоподібної перебудовою частоти (FHSS)

Бездротові локальні мережі FHSS підтримують швидкості передачі 1 і 2 Мбіт / с. Пристрої FHSS ділять призначену для їх роботи смугу частот від 2,402 до 2,480 ГГц на 79 неперекриваючих. Ширина кожного з 79 каналів складає 1 МГц, тому бездротові локальні мережі FHSS використовують відносно високу швидкість передачі символів - 1 МГц - і набагато меншу швидкість перебудови з каналу на канал. Послідовність перебудови частоти повинна мати наступні параметри: частота перескоків не менше 2,5 разів в секунду як мінімум між шістьма (6 МГц) каналами. Щоб мінімізувати число колізій між перекриваючимися зонами покриття, можливі послідовності перескоків повинні бути розбиті на три набори послідовностей [2].

По суті, схема стрибкоподібної перебудови частоти забезпечує неквапливий перехід з одного можливого каналу на інший таким чином, що після кожного стрибка покривається смуга частот, рівна як мінімум 6 МГц, завдяки чому в багатостільникових мережах мінімізується можливість виникнення колізій.

Бездротові локальні мережі, що використовують широкосмугову модуляцію DSSS з розширенням спектру методом прямої послідовності

У специфікації стандарту 802.11 обумовлено використання іншого фізичного рівня - на основі технології широкосмугової модуляції з розширенням спектру методом прямої послідовності (DSSS). Як було зазначено в стандарті 802.11.

Аналогічно підрівню PLCP, використовуваному в технології FHSS, підрівень PLCP технології DSSS стандарту 802.11 додає два поля у фрейм MAC, щоб сформувати PPDU: преамбулу PLCP і заголовок PLCP [15] Формат фрейму представлений на рис. 1.9.

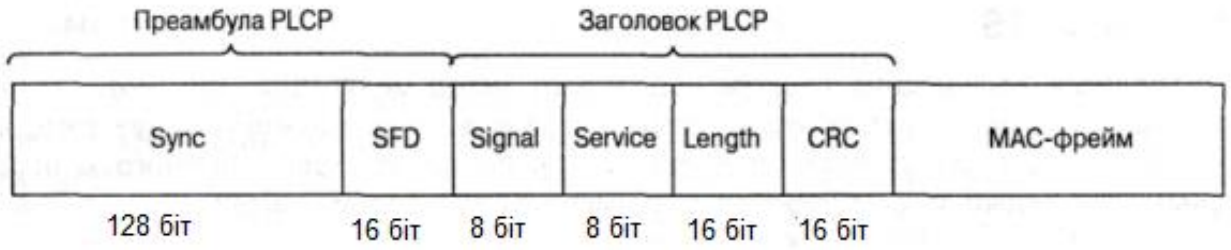

Рис. 1.9 Формат фрейму DSSS підрівня PLCP

Сімейство стандартів IEEE 802.11

IEEE 802.11a

Є найбільш "широкосмуговим" з сімейства стандартів 802.11, передбачаючи швидкість передачі даних до 54 Мбіт/с. На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікаціями 802.11a передбачена робота в діапазоні 5 ГГц. В якості методу модуляції сигналу вибрано ортогональне частотне мультиплексування (OFDM). Найбільш істотна відмінність між цим

методом і радіотехнологиями DSSS і FHSS полягає в тому, що OFDM передбачає паралельну передачу корисного сигналу одночасно на кількох частотах діапазону, в той час як технології розширення спектру передають сигнали послідовно. У результаті підвищується пропускна здатність каналу і якість сигналу. [6]

До недоліків 802.11a відносяться більш висока споживана потужність радіопередавачів для частот 5 ГГц, і ще менший радіус дії (обладнання для 2,4 ГГц може працювати на відстані до 300м, а для 5ГГц - близько 100м). [12]

Підводячи короткий підсумок відзначимо, що дана версія є як би "бічною гілкою" основного стандарту 802.11. Для збільшення пропускної здатності каналу тут використовується діапазон частот передачі 5,5 ГГц. Для передачі в 802.11a використовується метод множини несучих, коли діапазон частот розбивається на підканали з різними несучими частотами, по яких потік передається паралельно, розбитим на частини. Використання методу квадратурної фазової модуляції дозволяє досягти пропускної спроможності каналу 54 Мбіт/сек [5].

IEEE 802.11b

Завдяки високій швидкості передачі даних (до 11 Мбіт/с), практично еквівалентній пропускній здатності звичайних дротових ЛЗ Ethernet, а також орієнтації на "освоєний" діапазон 2,4 ГГц, цей стандарт завоював найбільшу популярність у виробників обладнання для бездротових мереж.

В остаточній редакції стандарт 802.11b, відомий також як Wi-Fi (wireless fidelity), був прийнятий в 1999р. В якості базової радіотехнології в ньому використовується метод DSSS з 8-розрядними послідовностями Уолша. [20]

Оскільки обладнання, яке працює на максимальній швидкості 11 Мбіт / с має менший радіус дії, ніж на більш низьких швидкостях, то стандартом 802.11b передбачене автоматичне зниження швидкості при погіршенні якості сигналу.

Як і у випадку базового стандарту 802.11, чіткі механізми роумінгу специфікаціями 802.11b не визначені. Цей стандарт є найбільш популярним на сьогоднішній день і, власне, сааме він носить ім’я торговельої марки Wi-Fi. Як і в початковому стандарті IEEE 802.11, для передачі в даній версії використовується діапазон 2,4 ГГц. Він не зачіпає канальний рівень і вносить зміни в IEEE 802.11 тільки на фізичному рівні. Для передачі сигналу використовується метод прямої послідовності DSSS, при якому весь діапазон поділяється на 5 перекриваючих один одного піддіапазонів, по кожному з яких передається інформація. Значення кожного біта кодуються послідовністю додаткових кодів (Complementary Code Keying). Пропускна здатність каналу при цьому становить 11 Мбіт/сек. [7]

IEEE 802.11d

Прагнучи розширити географію розповсюдження мереж стандарту 802.11, IEEE розробляє універсальні вимоги до фізичного рівня 802.11 (процедури

формування каналів, псевдовипадкові послідовності частот, додаткові параметри для MIB і т.д.). Відповідний стандарт 802.11d поки перебуває в стадії розробки.[14]

Стандарт визначає вимоги до фізичних параметрів каналів (потужність випромінювання та діапазони частот) і пристроїв бездротових мереж з метою забезпечення їх відповідності законодавчим нормам різних країн.

IEEE 802.11e

Специфікації розроблюваного стандарту 802.11e дозволяють створювати мультисервісні бездротові ЛЗ, орієнтовані на різні категорії користувачів, як корпоративних так й індивідуальних. При збереженні повної сумісності з вже прийнятими стандартами 802.11a і b, він дозволить розширити їх функціональність за рахунок підтримки потокових мультимедіа-даних і гарантованої якості послуг (QoS). Він визначає механізм призначення пріоритетів різним видам трафіку - таким, як аудіо-і відеопріложенія.[14]

IEEE 802.11f

Специфікації 802.11f описують протокол обміну службовою інформацією між точками доступу (Inter-Access Point Protocol, IAPP), що необхідно для побудови розподілених бездротових мереж передачі даних. Дата затвердження цих специфікацій в якості стандарту поки була не визначена. Даний стандарт, пов'язаний з аутентифікацією, визначає механізм взаємодії точок зв'язку між собою при переміщенні клієнта між сегментами мережі. Інша назва стандарту - Inter Access Point Protocol.[13]

IEEE 802.11g

Специфікації 802.11g, яка знаходиться зараз у стадії розгляду, являє собою розвиток стандарту 802.11b і дозволяє підвищити швидкість передачі даних в бездротових ЛЗ до 22 Мбіт/с завдяки використанню більш ефективної модуляції сигналу. З декількох пропозицій щодо базової радіотехнології для стандарту робоча група IEEE нещодавно обрала рішення компанії Intersil, що грунтується на методі OFMD, однак остаточне ухвалення 802.11g очікується тільки до кінця 2002 р. Одним з переваг майбутнього стандарту є зворотна сумісність з 802.11b.

IEEE 802.11h

Робоча група IEEE 802.11h розглядає можливість доповнення існуючих специфікацій 802.11 MAC (рівень доступу до середовища передачі) і 802.11a PHY (фізичний рівень у мережах 802.11a) алгоритмами ефективного вибору частот для офісних і вуличних бездротових мереж, а також засобами управління використанням спектра, контролю за випромінюваної потужністю і генерації відповідних звітів.

Передбачається, що рішення цих завдань буде базуватися на використанні протоколів Dynamic Frequency Selection (DFS) і Transmit Power Control (TPC), запропонованих Європейським інститутом стандартів з телекомунікацій (ETSI).

Зазначені протоколи передбачають динамічне реагування клієнтів бездротової мережі на інтерференцію радіосигналів шляхом переходу на інший канал, зниження потужності або обома способами. Розробка даного стандарту пов'язана з проблемами при використанні 802.11a в Європі, де в діапазоні 5 ГГц працюють деякі системи супутникового зв'язку. Для запобігання взаємних перешкод стандарт 802.11h має механізм "квазіінтелектуального" управління потужністю випромінювання і вибором несучої частоти передачі.[14]

IEEE 802.11i

До травня 2001 р. стандартизація засобів інформаційної безпеки для бездротових мереж 802.11 ставилася до ведення робочої групи IEEE 802.11e, але потім ця проблематика була виділена в самостійний підрозділ. Розроблюваний стандарт 802.1X покликаний розширити можливості протоколу 802.11 MAC, передбачивши кошти шифрування переданих даних, а також централізованої аутентифікації користувачів і робочих станцій. У результаті масштаби бездротових локальних мереж можна буде нарощувати до сотень і тисяч робочих станцій.

В основі 802.1X лежить протокол аутентифікації EAP, що базується на PPP. Сама процедура аутентифікації передбачає участь у ній трьох сторін - що викликає (клієнта), викликаємої (точки доступу) і сервера аутентифікації (сервера RADIUS).

Розроблювані засоби захисту даних повинні знайти застосування не тільки в бездротових, але і в інших локальних мережах - Ethernet і Token Ring. Ось чому майбутній стандарт отримав номер IEEE 802.1X, а його розробку група 802.11i веде спільно з комітетом IEEE 802.1. [12]

Метою створення даної специфікації є підвищення рівня безпеки бездротових мереж. Реалізація набору захисних функцій при обміні інформацією через бездротові мережі - зокрема, технологія AES, що підтримує ключі довжиною 128, 192 і 256 біт.

IEEE 802.11j

Специфікація 802.11j - настільки нова, що IEEE ще офіційно не сформував робочу групу для її обговорення на момент публікації. Передбачається, що стандарт буде обумовлювати існування в одній діапазоні мереж стандартів 802.11a і HiperLAN2. Специфікація призначена для Японії і розширює стандарт 802.11a додатковим каналом 4,9 ГГц. [21], [14].

IEEE 802.11n

Інститут IEEE веде роботу над створенням нової специфікації протоколу зв'язку в бездротових локальних мережах (WLAN). 802.11n працює вдвічі швидше, ніж 54-мегабітні "g" і "a": на швидкості від 100 Мбіт/с. Новий стандарт зрівняє дротові і бездротові системи, що дозволить корпоративним клієнтам використовувати бездротові мережі там, де це було неможливо через обмежену швидкості. Визначення швидкісних характеристик для стандарта "n" буде більш

суворим, ніж у "g" або "b". Воно грунтується на фактичній швидкості передачі файлів і потоків, а не на розмірі низькорівневого трафіку, забезпеченого безліччю службових заголовків. Прискорення досягається за рахунок більш оптимального використання частотного діапазону, аналогових радіочіпи, виконаних за поліпшеною CMOS-технології та інтеграції WLAN-адаптера в один чіп [14].

1.4 Бездротова технологія WiMAX

WiMAX - дуже перспективний напрям у розвитку бездротових технологій. Характеристики технології WiMAX багато в чому перевершують стандарт IEEE 802.11.

Цілі і завдання WiMAX

При всьому багатстві вибору мережевих підключень складно одночасно дотриматись три основні вимоги до мережевих з'єднань: висока пропускна здатність, надійність і мобільність. Вирішити таке завдання може наступне покоління бездротових технологій - WiMAX (Worldwide Interoperability for Microwave Access), стандарт IEEE 802.16.

Мета технології WiMAX полягає в тому, щоб надати універсальний бездротовий доступ для широкого спектру пристроїв (робочих станцій, побутової техніки "розумного будинку", портативних пристроїв і мобільних телефонів) і їх логічного об'єднання - локальних мереж. Треба відзначити, що дана технологія має ряд переваг:

1. У порівнянні з дротяними (xDSL або широкосмуговим), бездротовими або супутниковими системами мережі WiMAX повинні дозволити операторам і сервіс-провайдерам економічно ефективно охопити не тільки нових потенційних користувачів, але і розширити спектр інформаційних і комунікаційних технологій для користувачів, що вже мають фіксований (стаціонарний) доступ .
2. Стандарт об'єднує технології рівня оператора зв'язку (для об'єднання багатьох підмереж і надання їм доступу до Internet), а також технології "останньої милі", що створює універсальність і, як наслідок, підвищує надійність системи.
3. Бездротові технології більш гнучкі і, як наслідок, простіше в розгортанні, так як у міру необхідності можуть масштабуватися.
4. Простота установки як фактор зменшення витрат на розгортання мереж у країнах, що розвиваються, малонаселених або віддалених районах.
5. Дальність охоплення є суттєвим показником системи радіозв'язку. На даний момент більшість бездротових технологій широкосмугової передачі даних вимагають наявності прямої видимості між об'єктами мережі. WiMAX завдяки використанню технології OFDM створює зони покриття в умовах відсутності прямої

видимості від клієнтського обладнання до базової станції, при цьому відстані обчислюються кілометрами.

6. Технологія WiMAX містить протокол IP, що дозволяє легко і прозоро інтегрувати її в локальні мережі.

7. Технологія WiMAX підходить для фіксованих, переміщених і рухомих об'єктів мереж на єдиній інфраструктурі. [24]

Принципи роботи

Система WiMAX складається з двох основних частин:

1. Базова станція WiMAX, може розміщуватися на висотному об'єкті - будівлі або вишці.

2. Приймач WiMAX: антена з приймачем (рис. 1.10).

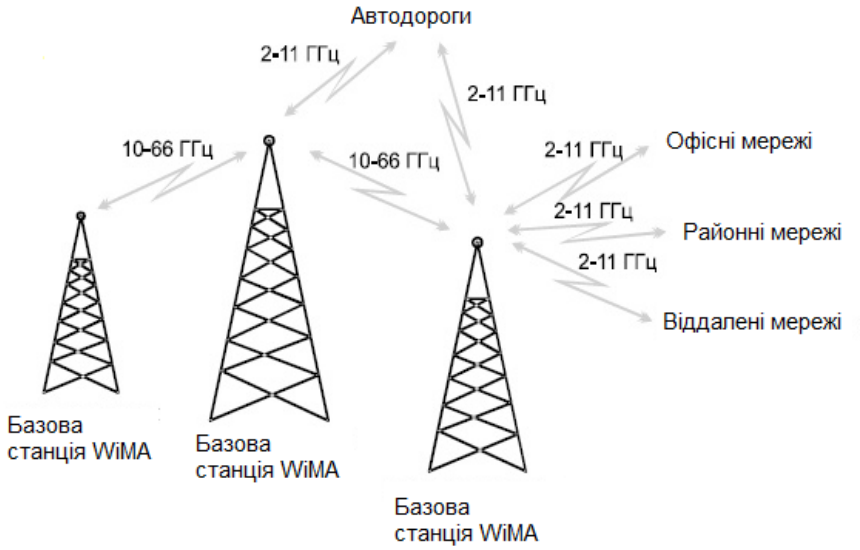

Рис. 1.10 Архітектура WiMAX

З'єднання між базовою станцією і клієнтським приймачем проводиться в НВЧ діапазоні 2-11 ГГц. Дане з'єднання в ідеальних умовах дозволяє передавати дані зі швидкістю до 20 Мбіт/с і не вимагає, щоб станція знаходилася на відстані прямої видимості від користувача. Цей режим роботи базової станції WiMAX близький широко використовуваному стандарту 802.11 (Wi-Fi), що допускає сумісність вже випущених клієнтських пристроїв та WiMAX. Слід пам'ятати, що технологія WiMAX застосовується як на "останній милі" - кінцевій ділянці між провайдером і користувачем, - так і для надання доступу регіональних мережах: офісним, районним.

Між сусідніми базовими станціями встановлюється постійне з'єднання з використанням надвисокої частоти 10-66 ГГц радіозв'язку прямої видимості. Дане з'єднання в ідеальних умовах дозволяє передавати дані зі швидкістю до 120 Мбіт/с. Обмеження за умовою прямої видимості, зрозуміло, не є перевагою, проте воно

накладається тільки на базові станції, які беруть участь в цілісному покритті району, що цілком можливо реалізувати при розміщенні обладнання [6].

Режими роботи

Стандарт 802.16e-2005 увібрав в себе всі версії, що виходили раніше раніше і на даний момент надає наступні режими:

1. Fixed WiMAX - фіксований доступ.
2. Nomadic WiMAX - сеансовий доступ.
3. Portable WiMAX - доступ в режимі переміщення.
4. Mobile WiMAX - мобільний доступ [2].

Fixed WiMAX

Фіксований доступ представляє собою альтернативу широкосмуговим дротовим технологіям (xDSL, T1 і т. п.). Стандарт використовує діапазон частот 10-66 ГГц. Цей частотний діапазон через сильне загасання коротких хвиль вимагає прямої видимості між передавачем і приймачем сигналу.

З іншого боку, цей частотний діапазон дозволяє уникнути однієї з головних проблем радіозв'язку - багатопроменевого розповсюдження сигналу. При цьому ширина каналів зв'язку в цьому частотному діапазоні досить велика (типова - 25 або 28 МГц), що дозволяє досягати швидкостей передачі до 120 Мбіт/с.

Nomadic WiMAX

Сеансовий (мандрівний) доступ додав поняття сесій до вже існуючого Fixed WiMAX. Наявність сесій дозволяє вільно переміщати клієнтське устаткування між сесіями і відновлювати з'єднання вже з допомогою інших вишок WiMAX, ніж ті, що використовувалися під час попередньої сесії. Такий режим розроблений в основному для портативних пристроїв, таких як ноутбуки, КПК. Введення сесій дозволяє також зменшити витрату енергії клієнтського пристрою, що теж важливо для портативних пристроїв.

Portable WiMAX

Для режиму Portable WiMAX додана можливість автоматичного перемикання клієнта від однієї базової станції WiMAX до іншої без втрати з'єднання. Проте для даного режиму все ще обмежена швидкість пересування клієнтського обладнання - 40 км/ч. Втім, вже в такому вигляді можна використовувати клієнтські пристрої в дорозі (в автомобілі при русі по житловим районам міста, де швидкість обмежена, на велосипеді, рухаючись пішки і т. д.).

Введення даного режиму зробило доцільним використання технології WiMAX для смартфонів і КПК. З 2006 року розпочато випуск пристроїв, що працюють в портативному режимі WiMAX [13].

Mobile WiMAX

Цей режим був розроблений в стандарті 802.16e-2005 і дозволив збільшити швидкість переміщення клієнтського обладнання до 120 км/г.

Основні досягнення цього режиму:

1. Стійкість до багатопроменевого поширенню сигналу і власним перешкод.
2. 2.Швидка, пропускна здатність каналу.
3. Технологія Time Division Duplex (TDD), яка дозволяє ефективно обробляти асиметричний трафік і спрощує управління складними системами антен за рахунок естафетної передачі сесії між каналами.
4. Технологія Hybrid-Automatic Repeat Request (H-ARQ), яка дозволяє зберігати стійке з'єднання при різкій зміні напряму руху клієнтського обладнання.
5. Управління енергозбереженням дозволяє оптимізувати витрати енергії на підтримку зв'язків портативних пристроїв у режимі очікування або простою.
6. Технологія Network-Optimized Hard Handoff (HHO), яка дозволяє до 50 мілісекунд і менш скоротити час на перемикання клієнта між каналами.
7. Розмір фрейму в 5 мілісекунд забезпечує компроміс між надійністю передачі даних за рахунок використання малих пакетів і накладними витратами за рахунок збільшення кількості пакетів (і, як наслідок, заголовків).

Висновки до розділу 1

В даному розділі дипломної роботи відбувалось ознайомлення з бездротовими мережами передачі даних. Було проведено аналіз сучасних бездротових технолій. А саме, розглянуто основні елементи бездротової мережі та методи доступу до середовища. Детально описані поняття архітектури стандарту IEEE 802.11 та технології WiMAX.

Також в цьому розділі було проаналізовано режими роботи та особливості їх організації, розкрито організаційні основи планування бездротових мереж.

2 БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ

2.1 Загрози і ризики безпеки бездротових мереж

Головна відмінність між дротовими і бездротовими мережами пов'язано з абсолютно неконтрольованою областю між кінцевими точками мережі. У досить широкому просторі мереж бездротова середа ніяк не контролюється. Сучасні бездротові технології пропонують обмежений набір засобів управління всією областю розгортання мережі. Це дозволяє атакуючим, що знаходяться в безпосередній близькості від бездротових структур, виробляти цілий ряд нападів, які були неможливі в дротовому світі [14].

Підслуховування

Найбільш поширена проблема відкритих і некерованих середовищ, тобто бездротових мереж - можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати дані, як показано на рис. 2.1.

Рис. 2.1 Атака «підслуховування»

Обладнання, що використовується для підслуховування в мережі, може бути не складніша від того, що використовується для звичайного доступу до цієї мережі. Щоб перехопити передачу, зловмисник повинен знаходитися поблизу від передавача. Перехоплення такого типу практично неможливо зареєструвати, і ще важче їм перешкодити. Використання антен і підсилювачів дає зловмисникові можливість перебувати на значній відстані від мети в процесі перехоплення. [10]

Підслуховування ведуть для збору інформації в мережі, яку згодом передбачається атакувати. Первинна мета зловмисника - зрозуміти, хто

використовує мережу, яка інформація в ній доступна, які можливості мережевого устаткування, в які моменти його експлуатують найбільш і найменш інтенсивно і яка територія розгортання мережі. Все це знадобиться для того, щоб організувати атаку на мережу. Багато загальнодоступних мережних протоколів передають таку важливу інформацію, як ім'я користувача та пароль, відкритим текстом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Навіть якщо передана інформація зашифрована, в руках зловмисника з’являється текст, який можна запам'ятати і розкодувати. [10], [11]

Інший спосіб підслуховування - підключитися до бездротової мережі. Активне підслуховування в локальній бездротовій мережі зазвичай грунтується на неправильному використанні протоколу Address Resolution Protocol (ARP). Спочатку ця технологія була створена для "прослуховування" мережі. Насправді ми маємо справу з атакою типу MITM (man in the middle, «людина посередині») на рівні зв'язку даних. Вони можуть приймати різні форми і використовуються для руйнування конфіденційності та цілісності сеансу зв'язку. Атаки MITM більш складні, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Коли жертва атаки ініціює з'єднання, шахрай перехоплює його і потім завершує з'єднання з необхідним ресурсом, а потім пропускає всі з'єднання з цим ресурсом через свою станцію. При цьому, атакуючий може надсилати інформацію, змінювати її або підслуховувати всі переговори і потім розшифровувати їх [2].

Таким чином, бездротова станція може перехоплювати трафік іншого бездротового клієнта (або дротового клієнта в локальній мережі).

Відмова в обслуговуванні (Denial of Service, DOS)

Повне паралізування мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися один з одним (рис. 2.2). Ця атака вимикає всі комунікації в певному районі. Атаку DOS на бездротові мережі важко запобігти або зупинити. Більшість бездротових мережевих технологій використовує неліцензовані частоти - отже, допустима інтерференція від цілого ряду електронних пристроїв. [18]

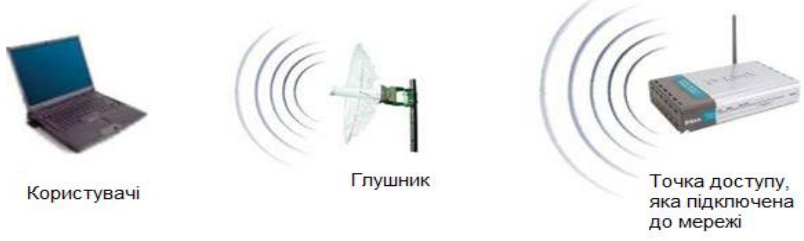

Рис. 2.2 Атака «відмова в обслуговуванні» в бездротових комунікаціях

Глушіння клієнтської станції

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, таким чином, виводячи цей канал з ладу. Атакуючий може використовувати різні способи глушіння [10]. Глушіння клієнтської станції дає можливість шахраєві підставити себе на місце заглушеного клієнта, як показано на рисунку 2.3. Також глушіння можуть використовувати для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.

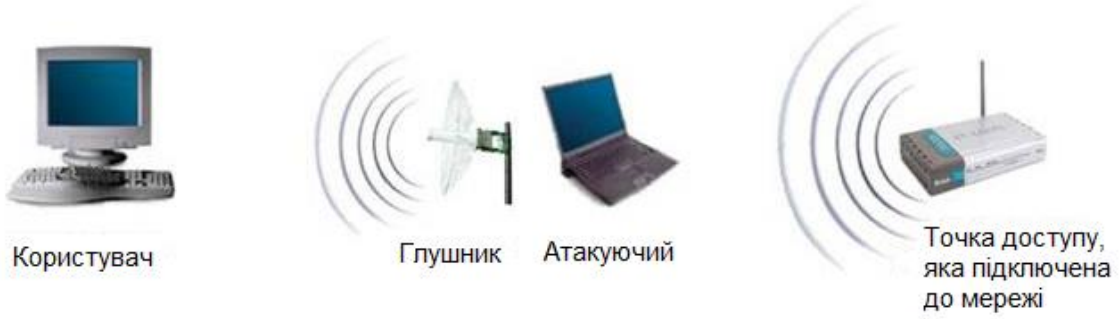

Рис. 2.3 Атака глушіння клієнта для перехоплення з'єднання

Глушіння базової станції

Глушіння базової станції надає можливість підмінити її атакуючої станцією, як показано на рис. 2.4. Таке глушіння позбавляє користувачів доступу до послуг.

Рис. 2.4 Атака глушіння базової станції для перехоплення з'єднання

Як зазначалося вище, більшість бездротових мережевих технологій використовує неліцензовані частоти. Тому багато пристроїв, такі як радіотелефони, системи спостереження і мікрохвильові печі, можуть впливати на роботу бездротових мереж і глушити бездротове з'єднання [14].

Загрози криптозахисту

У бездротових мережах застосовуються криптографічні засоби для забезпечення цілісності та конфіденційності інформації. Однак помилки призводять до порушення комунікацій та зловмисному використанню інформації.

WEP - це криптографічний механізм, створений для забезпечення безпеки мереж стандарту 802.11. Цей механізм розроблений з єдиним статичним ключем, який застосовується всіма користувачами. Керуючий доступ до ключів, часта їх зміна і виявлення порушень практично неможливі. Дослідження WEP-шифрування виявило вразливі місця, через які атакуючий може повністю відновити ключ після захоплення мінімального мережевого трафіку. В Інтернеті є засоби, які дозволяють зловмисникові відновити ключ протягом декількох годин. Тому на WEP не можна покладатися як на засіб аутентифікації та конфіденційності в бездротовій мережі.

Всі бездротові комунікаційні мережі схильні до атак прослуховування в період контакту. А управління ключем, як правило, викликає додаткові проблеми, коли застосовується при роумінгу і в разі загального користування відкритим середовищем [1].

Анонімність атак

Бездротовий доступ забезпечує повну анонімність атаки. Без відповідного обладнання в мережі, що дозволяє визначати місце розташування, атакуючий може легко зберігати анонімність і ховатися де завгодно на території дії бездротової мережі. У недалекому майбутньому прогнозується погіршення розпізнавання атак в Інтернет через широке поширення анонімних входів по небезпечним точкам доступу. Вже є багато сайтів, де публікуються списки таких точок, які можна використовувати з метою вторгнення. Важливо відзначити, що багато шахраїв вивчають мережі не для атак на їхні внутрішні ресурси, а для отримання безкоштовного анонімного доступу в Інтернет, прикриваючись яким вони атакують інші мережі. Якщо оператори зв'язку не вживають заходів обережності проти таких нападів, то будуть відповідати за шкоду, яку завдають при використанні їх доступу до Інтернет інших мереж. [6]

Фізичний захист

Пристрої бездротового доступу до мережі, самі за своєю природою мають бути маленькими а також точки доступу мають невеликий розмір і компактність. Крадіжка таких пристроїв багато в чому призводить до того, що зловмисник може потрапити в мережу, не використовуючи складних атак, тому що основні механізми аутентифікації в стандарті 802.11 розраховані на реєстрацію саме фізичного апаратного пристрою, а не облікового запису користувача. Отже втрата одного мережевого інтерфейсу і не своєчасне повідомлення адміністратора може призвести до того, що зловмисник отримає доступ до мережі.[6]

2.2 Аутентифікація в бездротових мережах

Основними стандартами аутентифікації в бездротових мережах є стандарти IEEE 802.11, WPA, WPA2 і 802.1x. Розглянемо основи цих стандартів.

Стандарт IEEE 802.11 мережі з традиційною безпекою

Стандарт IEEE 802.11 з традиційною безпекою (Tradition Security Network, TSN) передбачає два механізми аутентифікації бездротових абонентів:

- відкриту аутентифікацію (Open Authentication);
- аутентифікацію за загальним ключем(Shared Key Authentication).[13]

У аутентифікації в бездротових мережах також широко використовуються два інших механізми, що виходять за рамки стандарту 802.11, а саме призначення ідентифікатора бездротової локальної мережі (Service Set Identifier, SSID) і аутентифікація абонента за його MAC-адресою (MAC Address Authentication).

Ідентифікатор бездротової локальної мережі (SSID) представляє собою атрибут бездротової мережі, що дозволяє логічно відрізняти мережі один від одного. У загальному випадку, абонент бездротової мережі повинен поставити у себе відповідний SSID для того, щоб отримати доступ до необхідної бездротової локальної мережі. SSID ні в якій мірі не забезпечує конфіденційність даних, так само як і не аутентифікує абонента по відношенню до точки радіодоступу бездротової локальної мережі. Існують точки доступу, що дозволяють розділити абонентів підключаючихся до точки на кілька сегментів, це досягається тим, що точка доступу може мати не один, а декілька SSID [8].

Принцип аутентифікації абонента в IEEE 802.11

Аутентифікація в стандарті IEEE 802.11 орієнтована на аутентифікацію абонентського пристрою радіодоступу, а не конкретного абонента як користувача мережевих ресурсів. Процес аутентифікації абонента бездротової локальної мережі IEEE 802.11 складається з наступних етапів (рис. 2.5).

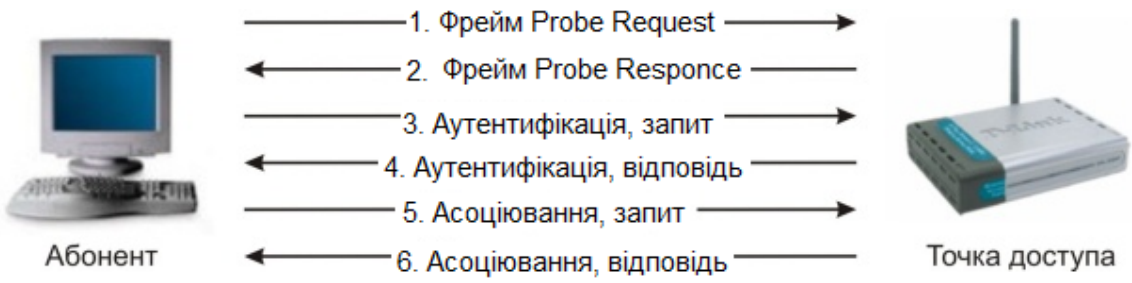

Рис. 2.5 Аутентифікація за стандартом 802.11

1 Абонент (Client) посилає кадр Probe Request у всі радіоканали.

2 Кожна точка радіодоступу (Access Point, AP), в зоні радіовидимості якої знаходиться абонент, посилає у відповідь фрейм Probe Response.

3 Абонент вибирає бажану для нього точку радіодоступу і посилає в обслуговуваємий нею радіоканал запит на аутентифікацію (Authentication Request).

4 Точка радіодоступу посилає підтвердження аутентифікації (Authentication Reply).

5 У разі успішної аутентифікації абонент посилає точці радіо доступу фрейм асоціації (Association Request).

6 Точка радіодоступу посилає у відповідь фрейм підтвердження асоціації (Association Response).

7 Абонент може тепер здійснювати обмін користувальницьким трафіком з точкою радіодоступу та провідною мережею.[16]

При активізації, бездротовий абонент починає пошук точок радіодоступу в своїй зоні радіовидимості за допомогою керуючих фреймів Probe Request. Фрейми Probe Request посилаються в кожен з радіоканалів, підтримуваних абонентським радіоінтерфейсом, в спробі знайти всі точки радіодоступу з необхідними клієнтові ідентифікатором SSID і підтримуваними швидкостями радіообміну. Кожна точка радіодоступу з тих, що знаходяться в зоні радіовидимості абонента і яка задоволяє запитуваними у фреймі Probe Request параметрами відповідає фреймом Probe Response, містячим синхронізуючу інформацію і дані про поточне завантаження точки радіодоступу. Абонент визначає, з якою точкою радіодоступу він буде працювати, шляхом зіставлення підтримуваних ними швидкостей радіообміну і завантаження. Після того, як бажана точка радіодоступу визначена, абонент переходить у фазу аутентифікації [11].

Відкрита аутентифікація

Відкрита аутентифікація, по суті, не є алгоритмом аутентифікації в звичному розумінні. Точка радіодоступу задовольнить будь-який запит відкритої аутентифікації. На перший погляд, використання цього алгоритму може здатися безглуздим, однак слід враховувати, що розроблені в 1997 році методи аутентифікації IEEE 802.11 орієнтовані на швидке логічне підключення до бездротової локальної мережі. Додатково до цього, багато IEEE 802.11-сумісні пристрої являють собою портативні блоки збору інформації (сканери штрих-кодів і т. п.), не мають достатньої процесорної потужності, що вимагається для реалізації складних алгоритмів аутентифікації.

У процесі відкритої аутентифікації відбувається обмін повідомленнями двох типів:

- Запит аутентифікації (Authentication Request);
- Підтвердження аутентифікації (Authentication Response).[14]

Таким чином, при відкритій аутентифікації можливий доступ будь-якого абонента до бездротової локальної мережі. Якщо в бездротовій мережі не використовується шифрування, то будь-який абонент, що знає ідентифікатор SSID точки радіодоступу, отримає доступ до мережі. При використанні точками радіодоступу шифрування WEP самі ключі шифрування стають засобом контролю доступу [2], [4]. Якщо абонент не має коректного WEP-ключа, то навіть у разі успішної аутентифікації він не зможе ні передавати дані через точку радіодоступу, ні розшифровувати дані, передані точкою радіодоступу (рис. 2.6).

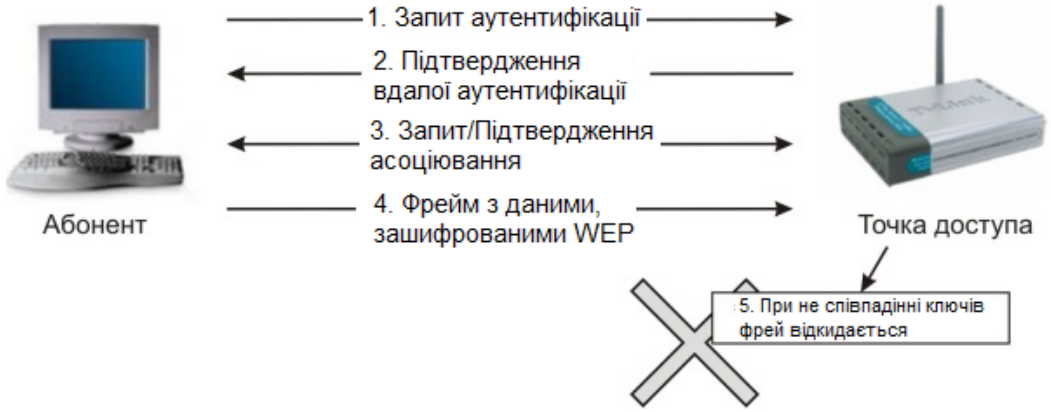

Рис. 2.6 Відкрита аутентифікація

Аутентифікація із загальним ключем

Аутентифікація із загальним ключем є другим методом аутентифікації стандарту IEEE 802.11. Аутентифікація із загальним ключем вимагає налаштування в абонента статичного ключа шифрування WEP. Процес аутентифікації ілюструє рис. 2.7:

1. Абонент надсилає точці радіодоступу запит аутентифікації, вказуючи при цьому необхідність використання режиму аутентифікації з загальним ключем.

2. Точка радіодоступу посилає підтвердження аутентифікації, що містить Challenge Text.

3. Абонент шифрує Challenge Text своїм статичним WEP-ключем, і посилає точці радіодоступу запит аутентифікації.

4. Якщо точка радіодоступу в змозі успішно розшифрувати запит аутентифікації і який міститься в ньому Challenge Text, вона посилає абоненту підтвердження аутентифікації, таким чином надаючи доступ до мережі.[18] Аутентифікація за MAC-адресою

5. Аутентифікація абонента за його MAC-адресою не передбачена стандартом IEEE 802.11, однак підтримується багатьма виробниками обладнання для бездротових мереж. При аутентифікації за MAC-адресою відбувається

порівняння MAC-адреси абонента або з зберігаючимся локально списком дозволених адрес легітимних абонентів, або за допомогою зовнішнього сервера аутентифікації (рис. 2.8). Аутентифікація за MAC-адресою використовується на додаток до відкритої аутентифікації і аутентифікації із загальним ключем стандарту IEEE 802.11 для зменшення ймовірності доступу сторонніх абонентів [10].

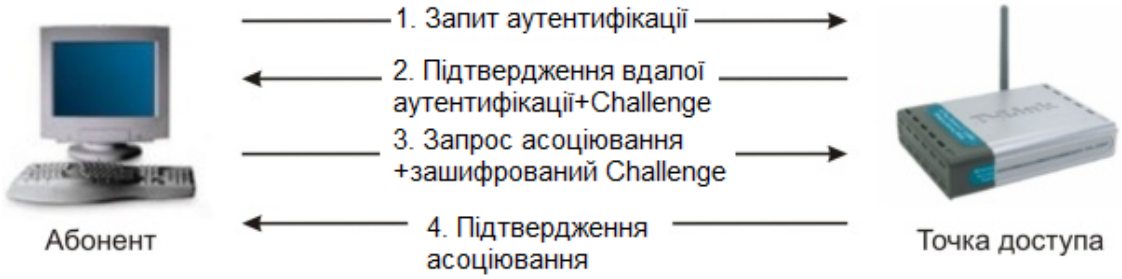

Рис. 2.7 Аутентифікація із загальним ключем

Рис. 2.8 Аутентифікація за допомогою зовнішнього сервера

2.3 Вразливість автентифікації 802.11

Проблеми ідентифікатора бездротової мережі. Ідентифікатор SSID регулярно передається точками радіодоступу у спеціальних фреймах Beacon незважаючи на те, що ці фрейми грають суто інформаційну роль в радіомережі, тобто зовсім «прозорі» для абонента, сторонній спостерігач в стані з легкістю визначити SSID за допомогою аналізатора трафіку протоколу 802.11, наприклад Sniffer Pro Wireless. Деякі точки радіодоступу, у 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. Ідентифікатор SSID не розроблявся для використання в якості механізму забезпечення безпеки. Додатково до цього, відключення широкомовного SSID передачі точками радіодоступу може серйозно відбитися на сумісності обладнання бездротових мереж різних виробників при використанні в одній радіомережі [18].

Вразливість відкритої аутентифікації

Відкрита аутентифікація не дозволяє точці радіодоступу визначити, чи є абонент легітимним чи ні. Це стає серйозною проблемою в системі безпеки в тому випадку, якщо в бездротової локальної мережі не використовується шифрування WEP.

D-Link не рекомендує експлуатацію бездротових мереж без шифрування WEP. У випадках, коли використання шифрування WEP не потрібно або неможливо (наприклад, в бездротових локальних мережах публічного доступу), методи аутентифікації більше високого рівня можуть бути реалізовані за допомогою Інтернет-шлюзів. [11]

Вразливість аутентифікації з загальним ключем

Аутентифікація із загальним ключем вимагає налаштування в абонента статичного WEP-ключа для шифрування Challenge Text, відправленого точкою радіодоступу. Точка радіодоступу аутентифікує абонента за допомогою дешифрування його відповіді на Challenge і порівняння його з відправленим оригіналом. Обмін фреймами, що містять Challenge Text, відбувається з відкритого радіоканалу, а значить, зазнає атак з боку стороннього спостерігача (Man in the middle Attack). Спостерігач може прийняти як нешифровані Challenge Text, так і той же Challenge Text, але вже в зашифрованному вигляді. Шифрування WEP проводиться шляхом виконання побітової операції XOR над текстом повідомлення і ключовий послідовністю, в результаті чого виходить зашифроване повідомлення (Cipher-Text). Важливо розуміти, що виконання побітової операції XOR над зашифрованим повідомленням і ключовий послідовністю має результатом текст вихідного повідомлення. [11],[10] Таким чином, спостерігач може легко обчислити сегмент ключовою послідовності шляхом аналізу фреймів у процесі аутентифікації абонента.

Вразливість аутентифікації за MAC-адресою

Стандарт IEEE 802.11 вимагає передачі MAC-адрес абонента і точки радіодоступу у відкритому вигляді. У результаті цього в бездротовій мережі, що використовує аутентифікацію за MAC-адресою, зловмисник може обійти метод аутентифікації шляхом підміни свого MAC-адреси на легітимний. Підміна MAC-адреси можлива в бездротових адаптерах, що допускають використання локально адміністрованих MAC-адрес. Зловмисник може скористатися аналізатором трафіку протоколу IEEE 802.11 для виявлення MAC-адрес легітимних абонентів [11].

2.4 Технології цілісності і конфіденційності переданих даних

Розгортання бездротових віртуальних мереж

Віртуальна приватна мережа (Virtual Private Network, VPN) - це метод, що дозволяє скористатися телекомунікаційною інфраструктурою загального користування, наприклад мережею Інтернет для надання віддаленим офісам або окремим користувачам безпечного доступу до мережі організації. Оскільки бездротові мережі 802.11 працюють в неліцензованому діапазоні частот і легко доступні для випадкового або зловмисного прослуховування, то саме в них розгортання та обслуговування VPN набуває особливу важливість, якщо необхідно забезпечити високий рівень захисту інформації [3].

Користуватися ж реалізацією стандарту на базі попередньо розділених ключів (PSK) і протоколу 802.1x при наявності високошвидкісного каналу між мережами не найбезпечніший метод. 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 на канальному рівні (Layer Two Tunneling Protocol, L2TP).

VPN відповідає трьом умовам: конфіденційність, цілісність і доступність. Слід зазначити, що ніяка VPN не є стійкою до DoS-або DDoS-атакам і не може гарантувати доступність на фізичному рівні просто в силу своєї віртуальної природи і залежності від попередніх протоколів [15]. Є багато способів класифікації VPN, але основні три види - це мережа-мережа, хост-мережа і хост-хост.

Топологія мережа-мережа

Цим терміном іноді описують VPN-тунель між двома географічно рознесеними приватними мережами (рис. 2.9).

Рис. 2.9 Топологія мережа-мережа

VPN такого типу зазвичай застосовуються, коли потрібно об'єднати локальні мережі за допомогою мережі загального користування так, як ніби вони знаходяться всередині одного приміщення.

Основна перевага такої конфігурації полягає в тому, що мережі виглядають як суміжні, а робота VPN-шлюзів абсолютно прозора для кінцевих користувачів. У цьому випадку важливо також тунелювання, оскільки в приватних мережах звичайно використовуються зарезервовані адреси, які не можуть маршрутизироваться через Інтернет. Тому для успішної взаємодії трафік необхідно інкапсулювати їх в тунель [2].

Топологія хост-мережа

При такій конфігурації віддалені користувачі підключаються до корпоративної мережі через Інтернет.

Спочатку мобільний клієнт встановлює з'єднання з Інтернет, а потім ініціює запит на організацію зашифрованого тунелю з корпоративним VPN-шлюзом. Після успішної аутентифікації створюється тунель поверх мережі загального користування і клієнт стає просто ще однією машиною у внутрішній мережі. Всі більш широке поширення надомної роботи стимулює інтерес до такого застосування VPN.

На відміну від VPN типу мережа-мережа, де число учасників невелике і більш-менш передбачувано, VPN типу хост-мережу легко може вирости до неосяжних розмірів. Тому системний адміністратор повинен заздалегідь продумати масштабований механізм аутентифікації клієнтів і управління ключами.

Топологія хост-хост

Така топологія, мабуть, зустрічається рідше всього. Мова йде про два хости, що обмінюються один з одним шифрованими і нешифрованому даними. У такій конфігурації тунель відбувається між двома хостами і весь трафік між ними інкапсулюється всередині VPN. Як приклад таких мереж можна назвати географічно віддалений сервер резервного зберігання. Обидва хоста підключені до Інтернет, і дані з центрального сервера дзеркально копіюються на резервний. Наприклад, прості мережі VPN типу хост-хост можна використовувати для захисту однорангових (Ad Hoc) мереж [2].

Поширення тунельних протоколів. Протокол IPSec

IPSec - це найбільш широко визнаний, підтримуваний і стандартизований з всіх протоколів VPN. IPSec лежить в основі відкритих стандартів, в яких описано цілий набір безпечних протоколів, що працюють поверх існуючого стека IP. Він надає служби аутентифікації і шифрування даних на мережевому рівні моделі OSI і може бути реалізований на будь-якому пристрої, який працює по протоколу IP. На відміну від багатьох інших схем шифрування, які захищають конкретний протокол верхнього рівня, IPSec може захистити весь IP-трафік. Він застосовується також у

поєднанні з тунельними протоколами на канальному рівні для шифрування і аутентифікації трафіку, що передається по протоколах, відмінним від IP [2].

Протокол IPSec складається з трьох основних частин:

- Заголовка аутентифікації (Authentication Header, AH);
- Безпечно інкапсульованого корисного навантаження (Encapsulating Security Payload, ESP);
- Схеми обміну ключами через Інтернет (Internet Key Exchange, IKE).

Заголовок AH додається після заголовка IP і забезпечує аутентифікацію на рівні пакету і цілісність даних. Іншими словами, гарантується, що пакет не був змінений на шляху проходження і вступив з очікуваного джерела. ESP забезпечує конфіденційність, аутентифікацію джерела даних, цілісність, опціональну захист від атаки повторного сеансу і до деякої міри скритність механізму управління потоком. Нарешті, IKE забезпечує узгодження настроювань служб безпеки між учасниками

Протокол PPTP

Двоточковий тунельний протокол (Point-to-Point Tunneling Protocol, PPTP) – це запатентована розробка компанії Microsoft, він призначений для організації взаємодії по типу VPN. PPTP забезпечує аутентифікацію користувачів за допомогою таких протоколів, як MS-CHAP, CHAP, SPAP і PAP. Протокол PPTP зазвичай застосовується для створення безпечних каналів зв'язку між багатьма Windows-машинами в мережі Intranet. [2]

Протокол визначає такі типи комунікацій:

- PPTP-з'єднання, за яким клієнт організовує PPP-канал з провайдером;
- Управляє PPTP-з'єднання, яке клієнт організовує з VPN-сервером і по якому узгодить характеристики тунелю;
- PPTP-тунель, по якому клієнт і сервер обмінюються зашифрованими даними.

Протокол L2TP

Цей протокол обіцяє замінити PPTP в якості основного тунельного протоколу. По суті, L2TP (Layer Two Tunneling Protocol) являє собою комбінацію PPTP і створеного Cisco протоколу Layer Two Forwarding (L2F). Протокол L2TP застосовується для тунелювання PPP-трафіку поверх IP-мережі загального користування. Для встановлення з'єднання по комутованій лінії в ньому використовується PPP з аутентифікацією за протоколом PAP або CHAP, але, на відміну від PPTP, L2TP визначає свій власний тунельний протокол [2].

Оскільки L2TP працює на канальному рівні, то через тунель можна пропускати і не IP трафік. Разом з тим L2TP сумісний з будь-яким канальним протоколом, наприклад ATM, Frame Relay або 802.11. Сам по собі протокол не містить засобів шифрування, але може бути використаний в поєднанні з іншими протоколами або механізмами шифрування на прикладному рівні [13].

2.5 Системи виявлення вторгнення в бездротові мережі

Системи виявлення вторгнення (Intrusion Detection System, IDS) - це пристрої за допомогою яких можна виявляти та своєчасно запобігати вторгнення в обчислювальні мережі. Вони діляться на два види: на базі мережі та на базі хоста. Мережеві системи (Network Intrusion Detection Systems, NIDS) аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил (Експертні системи). Виняток з точки зору принципів аналізу становлять системи на базі нейромереж та штучного інтелекту. Підмножиною мережевих систем виявлення вторгнень є системи для спостереження тільки за одним вузлом мережі (Network Node IDS).

NIDS діляться в свою чергу на дві великі категорії: на основі сигнатур і на основі бази знань. Сигнатурні IDS найбільш поширені і простіше реалізуються, але їх легко обійти і вони не здатні розпізнавати нові атаки. У таких системах події, відбуваються в мережі, порівнюються з ознаками відомих атак, які й називаються сигнатурами. Крім того, 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 чи статистичними [4].

Гарна IDS для бездротової мережі повинна бути одночасно сигнатурною і статистичною. Деякі інструменти для проведення атак на бездротові мережі мають чітко виражені сигнатури. Якщо вони виявляються в базі даних, то можна піднімати тривогу. З іншого боку, у багатьох атак очевидних сигнатур немає, проте вони викликають відхилення від нормальної роботи мережі на нижніх рівнях стека протоколів. [20] При розгортанні системи необхідно чітко розуміти, що, як і навіщо ми хочемо аналізувати, і намагатися відповісти на ці питання щоб сконструювати необхідну систему IDS (рис. 2.10).

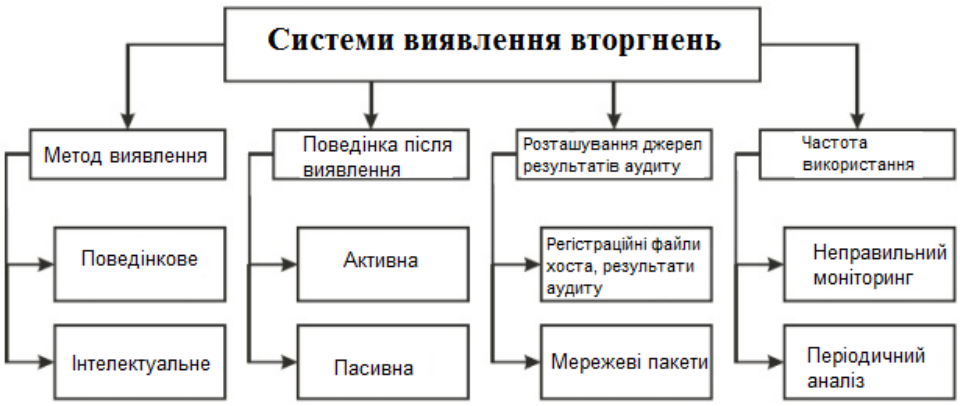

Рис. 2.10 Характеристики систем виявлення вторгнень

2.6 Протоколи безпеки бездротових мереж

Існує безліч технологій безпеки, і всі вони пропонують рішення для найважливіших компонентів політики у сфері захисту даних: аутентифікації, підтримки цілісності даних і активної перевірки. Ми визначаємо аутентифікацію, як аутентифікацію користувача або кінцевого пристрою і його місця розташування з подальшою авторизацією користувачів і кінцевих пристроїв[2].

Цілісність даних включає такі області, як безпека мережевої інфраструктури, безпеку периметра і конфіденційність даних. Активна перевірка допомагає впевнитися в тому, що встановлена політика в галузі безпеки витримується на практиці, і відстежити всі аномальні випадки і спроби несанкціонованого доступу.

Механізм шифрування WEP

Шифрування WEP (Wired Equivalent Privacy) засновано на алгоритмі RC4, що являє собою симетричне потокове шифрування.

Особливості WEP-протоколу:

- Досить стійкий до атак, пов'язаних із простим перебором ключів шифрування, що забезпечується необхідною довжиною ключа і частотою зміни ключів і ініціюючого вектора;
- Самосинхронізація для кожного повідомлення;
- Ефективність: WEP може бути легко реалізований;
- Відкритість;
- Використання WEP-шифрування не є обов'язковим у мережах стандарту
- IEEE 802.11.

Для безперервного шифрування потоку даних використовується потокове і блочне шифрування [1].

Потокове і блочне шифрування використовують метод електронної кодової книги (ECB). Метод ECB характеризується тим, що одне і те ж вихідне повідомлення на вході завжди породжує одне і те ж зашифроване повідомлення на виході. Це являє собою потенційну загрозу в системі безпеки, бо сторонній спостерігач, виявивши повторювані послідовності в зашифрованому повідомленні, може зробити обгрунтовані припущення щодо ідентичності змісту вихідного повідомлення [1].

Для усунення зазначеної проблеми використовують:

1) Вектори ініціалізації (Initialization Vectors, IVs)
2) Зворотній зв'язок (feedback modes)

До початку процесу шифрування 40 - або 104-бітний секретний ключ розподіляється між усіма станціями, що входять в бездротову мережу. До секретного ключа додається вектор ініціалізації (IV).

Вразливості шифрування WEP

Атаки на зашифровані дані за допомогою технології WEP можна підрозділити на два методи: пасивні та активні.

Пасивні мережеві атаки

У серпні 2001 року криптоаналитики Флурер С., Мантинеї І. і Шамір А. встановили, що секретний ключ шифрування WEP може бути обчислено з використанням певних фреймів, пасивно зібраних в бездротової локальної мережі . Причиною уразливості послужила реалізація в WEP методу планування ключів алгоритму потокового шифрування RC4. [6] Деякі вектори ініціалізації дають можливість встановити побайтовий склад секретного ключа, застосовуючи статистичний аналіз.

Дослідниками з AT & T / Rice University та авторами програми AirSnort була продемонстрована можливість визначення секретного ключа довжиною 40 і 104 бітів після аналізу всього лише 4 мільйонів фреймів. Для завантаженої бездротової локальної мережі це еквівалентно приблизно 4 годинам роботи, після чого ключ шифрування стане відомий пасивному спостерігачеві [2].

Подібна вразливість робить шифрування з використанням WEP неефективним, позбавляючи його криптографічної стійкості. Використання динамічних секретних ключів шифрування WEP вирішує проблему лише частково, для повного усунення уразливості потрібно спосіб посилення самого ключа.

Активні мережеві атаки

Індуктивне обчислення секретного ключа шифрування WEP представляє собою процес впливу на бездротову локальну мережу для отримання певної інформації і відноситься до класу активних мережевих атак.

Висока ефективність атаки індуктивного обчислення ключа, що робиться, стороннім спостерігачем в бездротової локальної мережі IEEE 802.11, пояснюється відсутністю дієвих засобів контролю цілісності повідомлень (Message Intgrity Check, MIC). Приймаюча сторона не в змозі розпізнати факт модифікації вмісту фрейма в процесі передачі по загальнодоступному радіоканалу. Більш того, значення ICV (Integrity Check Value), передбачене стандартом для контролю цілісності повідомлень, обчислюється за допомогою функції CRC32 (32-bit Cyclical Redundancy Check), контроль за допомогою циклічного 32-бітного надлишкового коду), яка схильна до атак з маніпуляцією бітами. Таким чином, у відсутності механізмів контролю цілісності повідомлень бездротові локальні мережі схильні активним атакам: повторним використанням вектора ініціалізації (IV Replay) і маніпуляції бітами (Bit-Flipping) [7].

1) Повторне використання вектора ініціалізації (Initialization Vector Replay Attacks) являє собою розроблену теоретично і реалізовану практично активну

мережеву атаку в бездротової локальної мережі, яка існує в декількох різновидах, одна з яких описана нижче і проілюстрована на рис. 2.11.

Рис. 2.11 Повторне використання вектора ініціалізації

В основі атаки лежить знання того, що пара вектора ініціалізації і секретного ключа шифрування, а значить і породжувана ними ключова послідовність, може бути повторно використана для відтворення ключовою послідовності достатньої довжини для порушення конфіденційності в бездротової локальної мережі в умовах використання шифрування WEP. Після того, як ключова послідовність обчислена для фреймів деякої довжини, вона може бути «вирощена» до будь-якого необхідного розміру.

2) Маніпуляція бітами (Bit-Flipping Attacks)

Маніпуляція бітами переслідує ту ж мету, що і повторне використання вектора ініціалізації, і спирається на вразливість вектора контролю цілісності фрейму ICV. Дані користувачів можуть відрізнятися від фрейму до фрейму, в той же самий час більшість службових полів та їх становище всередині фрейму залишаються незмінними.

Хакер маніпулює бітами даних користувача всередині фрейму 2-го (канального) рівня моделі OSI (Open Systems Interconnection) з метою спотворення 3-го (мережного) рівня пакета. Процес маніпуляції проілюстровано на рис. 2.12.

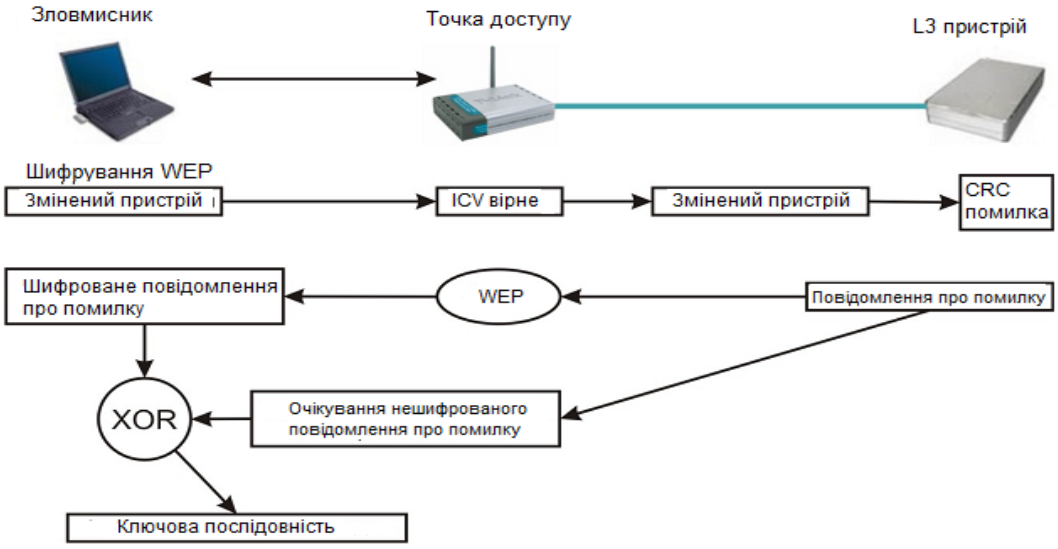

Рис. 2.12 Атака з маніпуляцією бітами

Вектор ICV знаходиться в шифрованого частині фрейму. За допомогою наступної процедури хакер маніпулює бітами шифрованого вектора ICV і таким чином забезпечує коректність самого вектора для нового, модифікованого фрейму. [20]

Проблеми управління статичними WEP ключами

Стандартом IEEE 802.11 не передбачені будь-які механізми управління ключами шифрування. За визначенням, алгоритм WEP підтримує лише статичні ключі, які заздалегідь поширюються тим чи іншим способом між абонентами і точками радіодоступу бездротової локальної мережі. Оскільки IEEE 802.11 аутентифікує фізичний пристрій, а не його користувача, втрата абонентського адаптера, точки радіодоступу чи власне секретного ключа становлять небезпеку для системи безпеки бездротової локальної мережі. У результаті при кожному подібному інциденті адміністратор мережі буде змушений вручну зробити зміну ключів у всіх абонентів і в точках доступу. Для цього у обладнанні відведено чотири поля для введення ключів. І при зміні всіх ключів необхідно тільки поміняти номер використовуваного ключа [6].

Специфікація WPA

Новий стандарт безпеки WPA (Wi-Fi Protected Access) забезпечує рівень безпеки куди більший, ніж може запропонувати WEP. Він перекидає місток між стандартами WEP і 802.11i і має ту перевагу, що мікропрограмне забезпечення більш старого обладнання може бути замінено без внесення апаратних змін. IEEE запропонувала тимчасовий протокол інтеграції ключа TKIP.

Основні удосконалення, внесені протоколом TKIP:

1. Пофреймовое зміна ключів шифрування;

2. Контроль цілісності повідомлення;

3. Вдосконалений механізм управління ключами [6].

Пофреймовое зміна ключів шифрування

Атаки, що застосовуються в WEP, що використовують уразливість слабких IV, таких, які застосовуються в додатку AirSnort, засновані на накопиченні декількох фреймів даних, що містять інформацію, зашифровану з використанням слабких IV. Найпростішим способом стримування таких атак є зміна WEP-ключа, використовуваного при обміні фреймами між клієнтом і точкою доступу, до того як атакуючий встигне накопичити фрейми достатні для виводу бітів ключа.

IEEE адаптувала схему, відому як пофреймовое зміна ключа. Основний принцип, на якому грунтується пофреймовое зміна ключа, полягає в тому, що IV, MAC-адресу передавача і WEP-ключ обробляються разом за допомогою двоступеневої функції перемішування. Результат застосування цієї функції відповідає стандартним 104-розрядному WEP-ключа і 24-розрядному IV.

IEEE запропонувала також збільшити 24-розрядний вектор ініціалізації до 48-разрядного IV. На рис. 2.13 представлений зразок 48-розрядного IV і показано, як цей IV розбивається на частини для використання при пофреймовом зміні ключа.

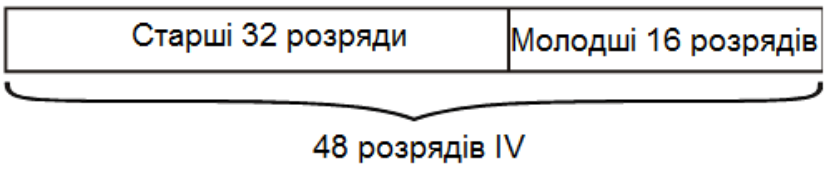

Рис. 2.13 Розбиття 48-і розрядного IV

Процес пофреймової зміни ключа можна представити наступним чином.

Пристрій ініціалізує IV, привласнюючи йому значення 0. У двійковому вигляді це буде значення 00000000000000000000000000000000000000000000000000.

Перші 32 розряди IV (перші 32 нуля) перемішуються з WEP-ключем (наприклад, мають 128-розрядне значення) і MAC-адресою передавача (мають 48-розрядне значення) для отримання значення ключа 1-ї фази (80-розрядне значення).

Ключ 1-ї фази знову перемішується з першими (старшими) 32 розрядами IV і MAC-адресою передавача, щоб отримати 128-розрядний пофреймовий ключ, перші 16 розрядів якого являють собою значення IV (16 нулів). Вектор ініціалізації пофреймового ключа збільшується на 1. Після того як пофреймовие можливостей IV будуть вичерпані, IV 1-ї фази (32 біта) збільшується на 1 (він буде складатися з 31 нуля і однієї одиниці, 00000000000000000000000000000001) і т.д. [4]

Цей алгоритм посилює WEP до такої міри, що майже всі відомі нині можливості атак усуваються без заміни існуючого обладнання. Слід зазначити, що

цей алгоритм (і TKIP в цілому) розроблений з метою прибрати вразливість в системі аутентифікації WEP і стандарту 802.11.

Контроль цілісності повідомлення

Для посилення малоефективного механізму, заснованого на використанні контрольної ознаки цілісності (ICV) стандарту 802.11, буде застосовуватися контроль цілісності повідомлення (MIC). Завдяки MIC можуть бути ліквідовані слабкі місця захисту, що сприяють проведенню атак з використанням підроблених фреймів і маніпуляцією бітами. IEEE запропонувала спеціальний алгоритм, який отримав назву Michael, щоб підсилити роль ICV в шифруванні фреймів даних стандарту 802.11. MIC має унікальний ключ, який відрізняється від ключа, використовуваного для шифруванні фреймів даних. Цей унікальний ключ перемішується з призначеною MAC-адресою і вихідною MAC-адресою фрейму, а також з усією незашифрованою частиною фрейму. [12]

Механізм шифрування TKIP в цілому здійснюється наступним чином:

1) За допомогою алгоритму пофреймового призначення ключів генерується пофреймовий ключ.
2) Алгоритм MIC генерує MIC для фрейму в цілому.
3) Фрейм фрагментується відповідно до настанов MAC щодо фрагментації.
4) Фрагменти фрейму шифруються за допомогою пофреймового ключа.
5) Здійснюється передача зашифрованих фрагментів.

У першому випадку, зберігання бази даних і перевірка автентичності за стандартом 802.1x у великих мережах звичайно здійснюються спеціальним сервером, найчастіше RADIUS (Remote Authentication Dial-In User Service).

У другому випадку мається на увазі застосування WPA всіма категоріями користувачів бездротових мереж, тобто має спрощений режим, який не потребує складних механізмів. Цей режим називається WPA-PSK і передбачає введення одного пароля на кожен вузол бездротової мережі (точку доступу, бездротової маршрутизатор, клієнтський адаптер, міст). До тих пір поки паролі збігаються, клієнту буде дозволений доступ в мережу. Можна помітити, що підхід з використанням пароля робить WPA-PSK уразливим для атаки методом підбору, проте цей режим позбавляє від плутанини з ключами WEP, замінюючи їх цілісною і чіткою системою на основі цифро-літерного пароля [1].

Таким чином, WPA/TKIP - це рішення, що надає більший в порівнянні з WEP рівень безпеки, спрямоване на усунення недоліків попередника і забезпечує сумісність з більш старим обладнанням мереж 802.11 без внесення апаратних змін до пристрою.

Стандарт мережі 802.11I з підвищенням безпеки (WPA2)

Стандарт 802.11i використовує концепцію підвищеної безпеки (Robust Security Network, RSN), яка передбачає, що бездротові пристрої повинні забезпечувати

додаткові можливості. Це вимагатиме внесення змін до апаратної частини та програмного забезпечення, тобто мережа, повністю відповідна RSN, стане несумісною з існуючим обладнанням WEP. У перехідний період буде підтримуватися як обладнання RSN, так і WEP (насправді WPA/TKIP було рішенням, спрямованим на збереження інвестицій в обладнання), але надалі пристрої WEP будуть відмирати.

Одним з найгірших аспектів WEP було управління секретними ключами. Багато адміністратори великих мереж знаходили його незручним. У результаті чого ключі WEP не змінювалися тривалий час (або ніколи), полегшуючи завдання зловмисникам [1].

RSN визначає ієрархію ключів з обмеженим строком дії, схожу з TKIP. У AES / CCMP, щоб вмістити всі ключі, потрібно 512 біт - менше, ніж у TKIP. В обох випадках майстер-ключі використовуються не прямо, а для виводу інших ключів. На щастя, адміністратор повинен забезпечити єдиний майстер-ключ. Повідомлення складаються з 128-бітного блоку даних, зашифрованого секретним ключем такої ж довжини (128 біт). Хоча процес шифрування складний, адміністратор знову-таки не повинен вникати в нюанси обчислень.

Висновки до розділу 2

В даному розділі дипломної роботи детально розглядаються загрози і ризики безпеки бездротових мереж. Адже у досить широкому просторі мереж бездротова середа ніяк не контролюється. Сучасні бездротові технології пропонують обмежений набір засобів управління всією областю розгортання мережі. Це дозволяє атакуючим, що знаходяться в безпосередній близькості від бездротових структур, виробляти цілий ряд нападів, які були неможливі в дротовому світі. А саме:

- підслуховування
- відмова в обслуговуванні (Denial of Service, DOS)
- глушіння клієнтської станції
- глушіння базової станції
- загрози криптозахисту

Також в даному розділі дипломної роботи було проведено аналіз аутентифікації бездротових мереж і виявлено основні проблеми і вразливості, які виникають в стандарті IEEE 802.11.

Детально описані технології цілісності і конфіденційності переданих даних та системи виявлення вторгнень в бездротові мережі.

Значна частина другого розділу дипломної роботи була присвячена висвітленню питання протоколів безпеки бездротових мереж. Такі як: основні механізми шифрування WEP, його вразливості та проблеми управління статичними WEP ключами. Специфікація WPA та стандарт мережі IEEE 802.11 з підвищенням безпеки WPA2.

3. ЗАХИСТ ІНФОРМАЦІЇ БЕЗДРОТОВОЇ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

3.1 Основні принципи політики безпеки

Взагалі в захищеній інформаційній системі, політика безпеки – це документ в якому визначені: мета захисту, ризики системи, основні напрямки захисту інформаційних ресурсів, методи та засоби захисту інформації, властивості захищеності в термінах, що представляють систему захисту інформації з урахуванням встановленої відповідальності за зловмисне порушення визначених вимог.

Опис політики безпеки може включати або враховувати властивості порушника, моделі загроз інформаційній системі та ризики пов'язані з їх реалізацією. [19] Найбільш часто, розглядаються політики безпеки, що пов'язані з поняттям «доступ». Доступ категорія суб'єктно-об'єктної моделі, що описує процес виконання операцій суб'єктів на об'єктами.

Політика безпеки, повинна включати:

- безліч можливих операцій над об'єктами;
- для кожної пари «суб'єкт, об'єкт», безліч дозволених операцій, що є підмножиною всієї безлічі можливих операцій.

Політика безпеки в загальному випадку являє собою нестаціонарний стан захищеності, система, що захищає властивості інформаційних ресурсів, може змінюватися, доповнюватися новими компонентами, тобто бути динамічною.

При розгляді політики безпеки необхідно вирішити чотири класи взаємозалежних завдань представлені на рис.3.1.

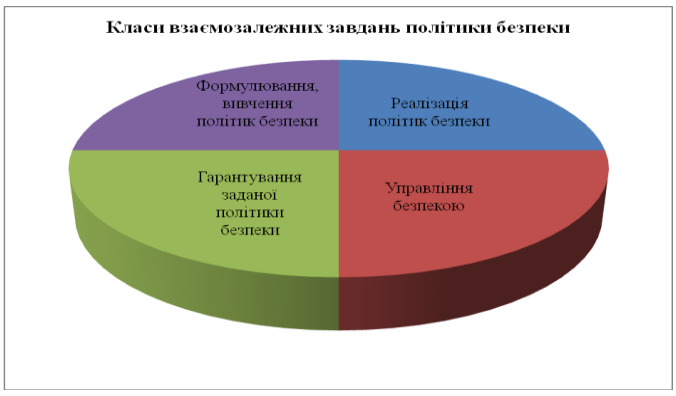

Рис.3.1 Класи взаємозалежних завдань політики безпеки

3.2 Вимоги політики безпеки в бездротових мережах

Політика безпеки - сукупність керівних принципів, правил процедур і практичних прийомів в області безпеки інформації, які регулюють управління, захист і розподіл цінної інформації [12].

Політика безпеки не дозволяє усунути всі загрози мереж стандарту 802.11, але її впровадження істотно знижує їх кількість. Вона встановлює модель захисту для існуючої або розроблюваної мережі. Політика безпеки пропонує набір правил і стандартів для користувачів, адміністраторів та менеджерів бездротової мережі. Для забезпечення функцій захисту мережі політика безпеки передбачає наявність посади начальника служби безпеки.[13]

Для створення політики безпеки необхідне проведення оцінки ризиків в бездротовій мережі. Оцінка ризиків передбачає визначення загроз і вразливостей в системі і також вона обов'язкова при боротьбі з непередбаченими загрозами, витратами і затратами. Керівник служби безпеки повинен використовувати заходи захисту інформації в поєднанні з оцінкою ризику в 802.11 мережах. Оцінка ризику повинна проводитися періодично для забезпечення точного набору потенційних загроз. Заходи політики безпеки повинні передбачати поділ бездротових і загальних мереж, щоб порушення безпеки в одній не впливало на іншу. Сегрегація мережі забезпечує відділення WLAN мереж від дротових, які є менш вразливими для атак. Між загальними і бездротовими мережами необхідно розташовувати фільтруюче пристрій для контролю та моніторингу трафіку [19].

Встановлення автентичності є одним з основних елементів захисту Wi-Fi мереж і повинно бути включено в їхню політику безпеки. Всі користувачі WLAN зобов'язані підтвердити справжність перед отриманням доступу до мережі. Встановлення автентичності необхідно для обмеження доступу до закритих ресурсів.

У політиці безпеки повинна бути визначена форма взаємної аутентифікації. При взаємному встановлення автентичності клієнт і сервер авторизують один одного. Взаємне встановлення справжності, перш за все, підвищує безпеку, встановлюючи справжність сервера, а також зменшує можливості шахрайства в мережі. Іншим фактором при виборі методу аутентифікації повинна бути простота реалізації та адміністрування. Деякі форми встановлення автентичності, такі як PKI, вимагають ретельної розробки та адміністрування. Політика безпеки може вказувати заходи щодо встановлення справжності, а також об'єкти та ресурси, для яких потрібне встановлення автентичності. Політика безпеки може розділити користувачів і рівні доступу по групах.

Засіб для забезпечення конфіденційності в бездротових мережах має бути визначено в політиці безпеки. Шифрування має забезпечити безпечний канал зв'язку, в якому будуть циркулювати закриті дані. Політика безпеки повинна визначити стійкий метод шифрування для забезпечення безпечної передачі даних. Широко застосовується в мережах Wi-Fi метод шифрування WEP забезпечує мінімальний захист і повинен використовуватися, якщо інше шифрування не можливо.

3.3 Основні компоненти політики безпеки в бездротових мережах

Політика безпеки передбачає введення лог файлів та облік діяльності користувачів. Ведення лог файлів передбачається для забезпечення:

• контролю за користувачами;

• спрощення процесу налаштування мережі в разі виникнення несправностей;

• спрощення винесення відповідальності за порушення правил експлуатації мережі.[13]

Лог файли передбачають ідентифікацію та відстеження шляху зловмисника в разі проникнення в мережу. Вони ведуться на бездротових точках доступу (Wireless Access Point, WAP), брандмауерах, які поділяють провідні та Wi-Fi мережі, серверах. У політиці безпеки повинна бути визначена частота перегляду лог файлів.

У політиці безпеки бездротових мереж необхідна регламентація як логічного, так і фізичного захисту WAP. Точки доступу повинні бути розташовані в фізично захищених областях. При зміні конфігурацій точок доступу повинна виконуватися аутентифікація адміністратора. Більшість WAP, після скидання, повертаються до заданого за замовчуванням небезпечному режиму. Більшість WAP дозволяють створювати облікові записи користувачів. Облікові записи необхідно створювати для зменшення ризику несанкціонованого доступу до WAP. Списки користувачів на підключення визначаються політикою безпеки. Бездротові клієнти повинні бути оснащені персональним брандмауером і антивірусним програмним забезпеченням. Через слабкий захист бездротові клієнти стають об'єктом для нападу і потім, одного разу скомпрометовані, вони використовуються як уразливості для подальших нападів. Політика безпеки повинна забороняти прямі (ad-hoc) бездротові з'єднання, минаючи точки доступу, маршрутизуючі трафік.[17]

Політика безпеки повинна передбачати використання брандмауерів для зменшення ризику злому бездротового клієнта. За допомогою брандмауерів слід проводити реєстрацію бездротової діяльності. Політика безпеки повинна вимагати використання антивірусного програмного забезпечення та обов'язкового відновлення антивірусних баз. Політика безпеки повинна передбачати частоту оновлення антивірусної бази [4].

У політиці безпеки визначаються інструменти для виконання бездротового сканування, а також частота їх виконання. Бездротове сканування необхідно для визначення місцезнаходження неправочинних точок доступу. Сканування повинні проводитися не менше ніж один раз на тиждень або, в крайньому випадку, раз на місяць. У політиці безпеки повинно міститися керівництво як для проведення сканування, так і усунення незаконних точок доступу.

Крім того політикою безпеки передбачається:

• статична ARP адресація, що підсилює захист, збільшує адміністрування;

• перевірка MAC адреси;

• статистична IP адресація;

• визначення схеми бездротового мережевого ідентифікатора (SSID).[13]

Політика безпеки може заборонити широкомовну трансляцію SSID, з метою ускладнення ідентифікації точок доступу.

Рекомендується включити в політику безпеки бездротових мереж систему виявлення вторгнення (Intrusion Detection System, IDS). Бездротова IDS необхідна для забезпечення захисту шляхом виявлення незаконної бездротової діяльності (нападу). Для забезпечення безпеки бездротової мережі політика безпеки повинна включати комплекс заходів як апаратної, так і програмного захисту [15].

Як висновок до підбору основних компонентів політики безпеки в бездротових мережіх, можна сказати, що для захисту даних в мережі необхідне точне слідування правилам і вказівкам, викладеним в політиці безпеки. Всі мережеві операції і розробки повинні відповідати встановленим в політиці безпеки правилам. Таким чином, для зменшення загроз безпеки в мережах Wi-Fi, зниження ризиків витоку інформації необхідна розробка і неухильне дотримання політики безпеки.

3.4 Захист конфіденційної інформації в бездротових мережах

Класифікація технологій бездротових мереж

Захисту конфіденційної інформації в бездротових мережах варто надавати особливу увагу. Сьогодні бездротові мережі отримали величезне розповсюдження. Вони використовуються, як у офісах, так і в домашніх умовах. Ці мережі зручні в користуванні і дозволяють незалежно від місця знаходження бути он-лайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в Інтернеті. Бездротова мережа має великий радіус дії, тому зловмисник може перехоплювати інформацію та атакувати мережу, знаходячись на безпечній відстані. Надалі в роботі наведені: класифікація бездротових мереж, класифікації атак, та види захисту конфіденційної інформації від несанкціонованого доступу. [24]

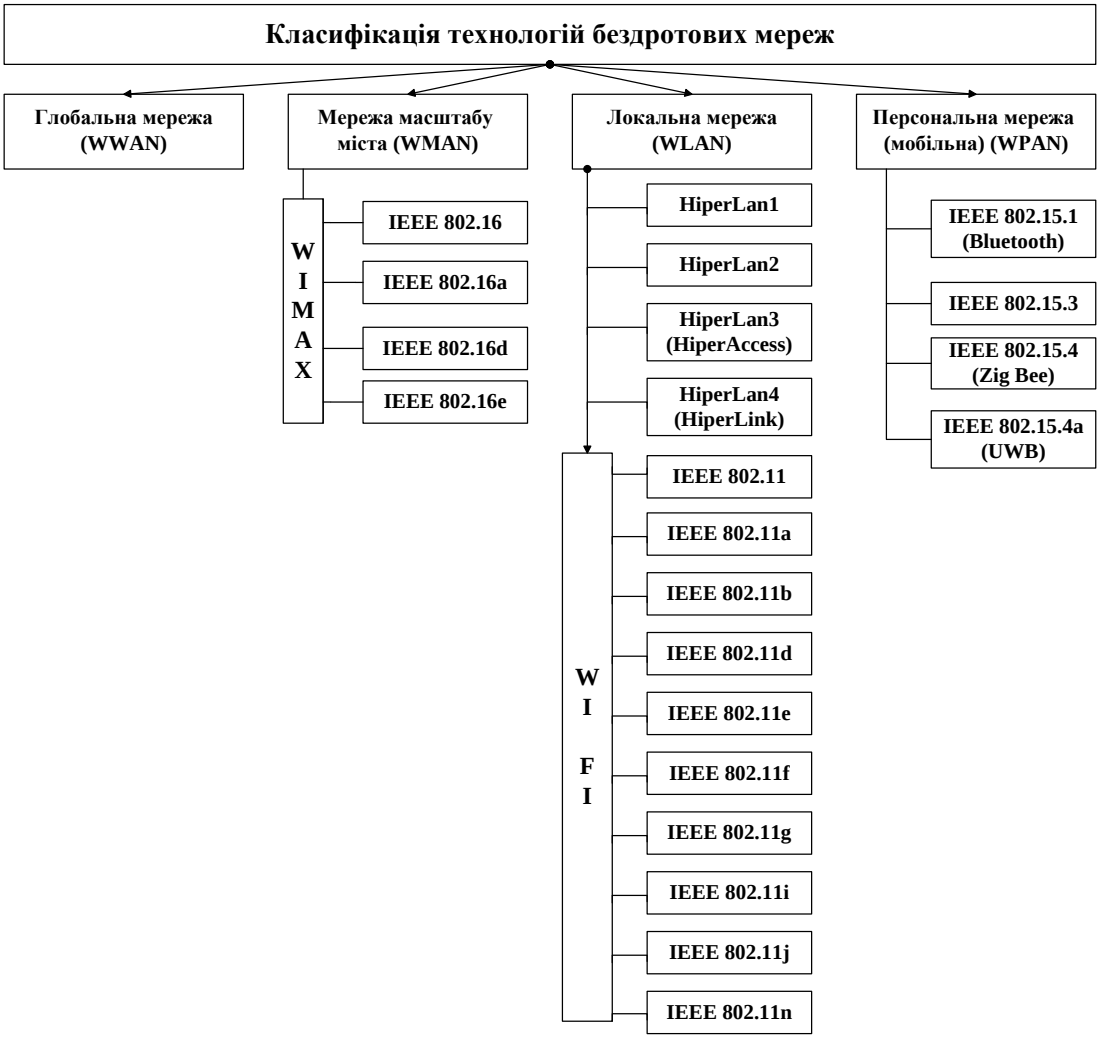

Рис.3.2 Класифікація технологій бездротових мереж

Загальна класифікація атак

Атаки на бездротові мережі. В попередніх розділах дипломної роботи вже приділялась достатня увага атакам на бездротові мережі, згадаємо, що під атакою слід розуміти – запуск зловмисником спеціальних програм для отримання неавторизованого доступу до мережі [6]. Загальна класифікацію атак на бездротові мережі представлена на рис. 3.3.

Класифікація загроз інформаційним ресурсам БМ

Загальна класифікація загроз повністю відповідає бездротовим системам і мережам, як загальна для любого виду інформаційно-комунікаційних систем. Однак, присутні певні відмінності, згідно впроваджених методів та засобів передачі інформаційних потоків в бездротових мережах.

Загрози інформаційним ресурсам БСМ, пов’язані загальними проблемами зв’язку, згідно рівнів моделі ISO/OSI:

- втрата зв’язку (навмисна або ненавмисна);

- раптовий сплеск навантаження на мережу з умови обробки великих обсягів даних;
- раптове зменшення пропускної спроможності мережі;
- збільшення затримок в каналі передачі даних;
- підвищений рівень фрагментації пакетів;
- часті повторні передачі або запити;
- наявність додаткових передавачів в зоні дії мережі;
- використання відкритих каналів зв'язку при умові обміну конфіденційними даними;
- присутність ефекту перекриття каналів зв'язку;

Рис.3.3 Загальна класифікація атак

- непередбачена зміна робочого каналу передачі даних при встановлених процесах аналізу трафіку та спостереження;
- погіршення якості переданого сигналу або високий рівень шуму в каналі передачі даних;
- помилки, допущені при конфігурації мережі, тощо.

Загрози інформаційним ресурсам БСМ, пов'язані системою управління доступом:

- підвищена частота («затоплення трафіку») появи деяких типів фреймів;
- присутність в мережі фреймів нестандартних розмірів у відповідності до типів визначених протоколів;
- присутність в мережі фреймів, що не підлягають класифікації;

- обробка неповних, зіпсованих або неправильно сформованих фреймів;
- постійне дублювання («Затоплення трафіку») або повтор пакетів фреймів, що мають запити на від'єднання і припинення (з'єднання або поновлення) сеансу обміну даними;
- присутність в мережі послідовності фреймів з неправильними порядковими номерами;
- частота появи пробних фреймів Probe Request;
- присутність в мережі інформаційного потоку даних, ідентифікатор мережі якого відрізняється від SSID даної мережі;
- присутність в мережі потоку фреймів з широкомовним SSID;
- присутність в мережі потоку фреймів, що часто змінюються або мають випадкові ідентифікатори мережі SSID;
- присутність в мережі потоку фреймів з значеннями (масками або сигнатурами) в полі ідентифікатора мережі SSID або інших полях, типовими для визначених класів атак або НСД;
- присутність в мережі потоку фреймів з MAC-адресами користувачів, що відсутні в списку контролю доступу;
- присутність в мережі потоку дублюючих фреймів з MAC-адресами визначених користувачів;
- присутність в мережі потоку фреймів, що часто змінюються або мають випадкові MAC-адреси;
- постійне багатократне дублювання фреймів запиту і відповіді процедури аутентифікації або начала та кінцівки сеансу користувача;
- присутність в мережі потоку фреймів, що прийшли від невідомих аутентифікаторів (фальшива точка доступу);
- присутність в мережі управляючого потоку фреймів, що прийшли від не аутентифікованих адміністраторів мережі (сторонній адміністративний трафік визначеної точки доступу);
- незавершена процедура аутентифікації згідно визначених протоколів, тощо.

Загрози інформаційним ресурсам БСМ, пов'язані з використанням криптографічних протоколів***:***

- наявність незашифрованого інформаційного потоку даних у бездротовому каналі зв'язку;
- наявність зашифрованого інформаційного потоку даних у бездротовому каналі зв'язку, при умові використання невідомих ключів;
- наявність зашифрованого інформаційного потоку даних у бездротовому каналі зв'язку, при умові використання не стандартних ключів або ключів не стандартної довжини;

- несанкціонована зміна стандартних крипто-протоколів шифрування на невідомі або не стандартні;

- несанкціоноване зниження рівня захисту інформаційних ресурсів БСМ з урахуванням заміни стандартних крипто-протоколів шифрування на менш стійкі;

- присутність помилок при наданні крипто-ключів;

- не можливість зміни або оновлення крипто-ключів;

- неможливість по фреймової зміни ключів шифрування з умови забезпечення швидкої зміни для кожного послідуючого фрейма;

- неможливість контролю цілісності повідомлення (повинен забезпечуватись ефективний контроль цілісності фреймів даних з метою запобігання прихованим маніпуляціям з фреймами);

- відсутність вдосконаленого механізму управління ключами;

- зміна порядку потоку фреймів ключів.

Способи несанкціонованого доступу до бездротових мереж

Існують різні способи несанкціонованого доступу на бездротові мережі на рис.3.4 представлена класифікація видів атак на бездротові мережі.

Рис. 3.4 Способи несанкціонованого доступу до бездротових мереж

Механізми реалізації несанкціонованого доступу

Несанкціонований доступ представляє собою спробу порушника отримати доступ до мережних ресурсів без відповідного дозволу. Несанкціонований доступ дозволяє: неавторизовану маніпуляцію даними (читання, модифікацію, копіювання або переміщення файлів, підробку мережних адрес, переключення з'єднань, зміну маршрутів); доступ до системи (реєстрація зі «стороннім» обліковим записом — імітація, маскування, встановлення та розсилка зловмисного програмного забезпечення для здійснення подальших атак, несанкціоноване встановлення й використання мережних з'єднань, несанкціоноване використання комунікаційних протоколів, використання комунікаційних з'єднань для атак, використання хибних налагоджень, використання внутрішніх помилок, відторгнення комунікаційних відношень); підвищення прав доступу (отримання інформації або виконання процедур, що не є доступними при встановленому для користувача рівні доступу).[25]

Одним із типів НСД, щзо використовує недостатню стійкість відповідних механізмів ідентифікації та автентифікації є імітація, маскування довіреного об'єкта або суб'єкта. Імітація має на увазі фальсифікацію (порушення цілісності) IP-адреси, повторне відтворення повідомлень (порушення доступності) з метою захоплення сеансу зв'язку, зміну параметрів маршрутизації й змісту інформації, що передається. Згадана вище недостатня ідентифікація й автентифікація віддалених один від одного об'єктів полягає, перш за все, у труднощах здійснення однозначної ідентифікації повідомлень, переданих між суб'єктами й об'єктами взаємодії. Для надійної ідентифікації й автентифікації повідомлень, у принципі, можна використати, по-перше, геш-функції, які обчислюються за допомогою, наприклад, відкритого ключа, динамічно виробленого при встановленні каналу, й, по-друге, випадкові багатобітні лічильники пакетів і мережні адреси станцій. Однак на практиці, наприклад, у протоколі TCP для ідентифікації використаються лише два 32-бітних лічильники. [25]

Наступним механізмом ***несанкціонованого доступу є зміна параметрів маршрутизації***. Це пов'язано з тією особливістю, що сучасні глобальні мережі представляють собою сукупність сегментів мережі, пов'язаних між собою через мережні вузли. Для забезпечення ефективної й оптимальної маршрутизації в розподілених обчислювальних системах застосовуються спеціальні керуючі протоколи, що дозволяють маршрутизаторам обмінюватись інформацією один з одним, повідомляти хости про новий маршрут, віддалено управляти маршрутизаторами. При цьому абсолютно очевидно, що маршрутизація в глобальних мережах відіграє найважливішу роль і, як наслідок цього, може піддаватися атаці. Основна мета атаки, пов'язаної з нав'язуванням хибного маршруту, полягає в тому, щоб змінити (*порушити цілісність*, модифікувати) вихідну маршрутизацію на об'єкті розподіленої обчислювальної системи так, щоб

новий маршрут проходив через хибний об’єкт — хост атакуючого. Реалізація даної типової віддаленої атаки складається в несанкціонованому використанні протоколів керування мережею для зміни вихідних таблиць маршрутизації. [25]

Класифікація методів захист у бездротових мережах

Існують різні причини, що спонукають хакерів займатися атаками [1]. Одна з причин: заради цікавості. Такі люди займаються зламуванням задля розваги та самоствердження. Вони можуть навіть зробити послугу суспільству, публічно сповістити про виявленні небезпечні місця мереж, що примусить звернути увагу на існуючі проблеми. [24]

Інша причина атак криється в застосуванні чужої мережі, тобто в крадіжці інтернет-трафіку.

Третя, найважливіша причина – це викрадення конфіденційної інформації. Ці зловмисники є найнебезпечнішими. Стандартні заходи безпеки можуть лише затримати такого супротивника на декілька годин. Якщо безпеці мережі не приділити належної уваги, то атака неминуче виявиться успішною.

Здатність хакерів відстежувати трафік, отримувати неавторизований доступ до ресурсів і викликати відмову в обслуговуванні бездротовою мережею її користувачів - ось ті проблеми, які доведеться вирішувати. Використовуючи ефективні механізми аутентифікації і шифрування, можна істотно знизити небезпеку. Проте слід мати на увазі, що необхідний рівень безпеки залежить від пропонованих до мережі вимог. На рис. 3.5 наведена класифікація різних методів захисту бездротових мереж.

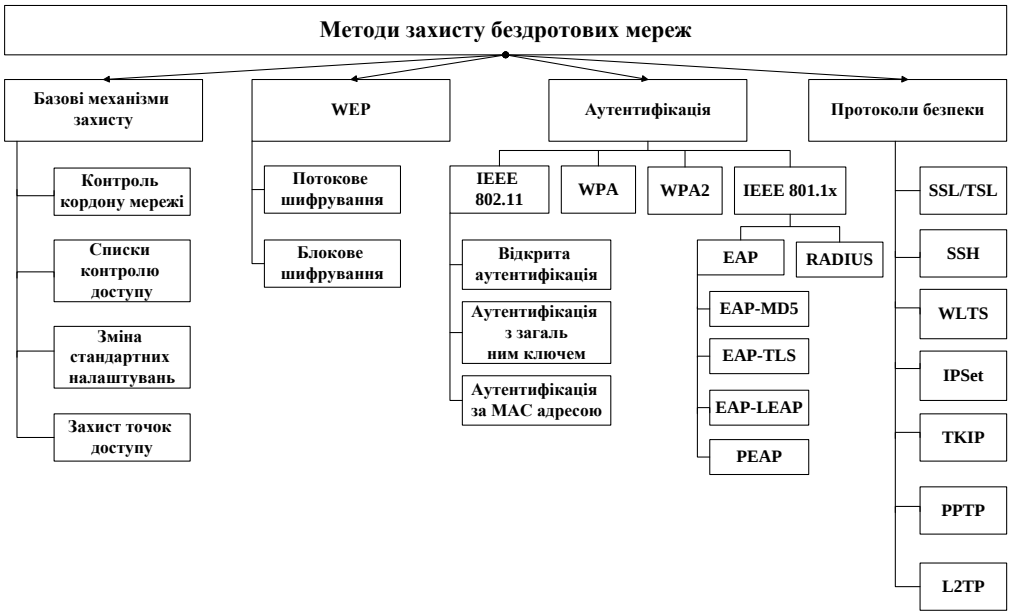

Рис.3.5 Класифікація методів захист у бездротових мережах

Розглянувши усі доступні на сьогоднішній день методи захисту, можна виділити головні: WEP, WPA, WPA2, 802.1X. Який саме метод слід вибрати залежить від мети, яку переслідує користувач, та від існуючого обладнання. WPA2 та 802.1X – більш нові методи захисту, вони потребують потужного обладнання для криптографічних обчислень. Якщо пристрої спроможні підтримувати ці методи, то краще вибрати саме їх. Якщо ні, то можна зупинити свій вибір на WPA, якщо і цей стандарт обладнанням не підтримується, то хоча б на WEP. Також не треба зневажати допоміжними засобами [20]. Але необхідно розуміти, що будь-який захист можна обійти, це просто питання часу.

Захист інформаційних ресурсів є – базовим чинником процесу проектування будь-яких інформаційних систем не залежно від виду комунікацій (дротові або бездротові мережі).[24].

Висновки до розділу 3

Третій розділ дипломної роботи був присвячений захисту інформації бездротової мережі від несанкціонованого доступу. Були представлені основні принципи побудування політики безпеки бездротових мереж, описані відповідні вимоги політики безпеки та її головні компоненти.

Для наглядного висвітлення теми несанкціонованого доступу до бездротових мереж було розроблено такі графічні матеріали:

- ✓ Класифікація технологійй бездротових мереж;
- ✓ Загальна класифікація атак;
- ✓ Способи несанкціонованого доступу до бездротових мереж;
- ✓ Методи захист у бездротових мереж.

Також в розділі представлена детальна класифікація загроз інформаційним ресурсам бездротової мережі пов’яза ним з:

- ➢ Загальними проблемами зв’язку;
- ➢ Системою управління доступом;
- ➢ Використанням криптографічних протоколів.

Розглянуті механізми реалізації несанкціонованого доступу в бездротових мережах.

4 СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ БЕЗДРОТОВОЇ МЕРЕЖІ

4.1 Визначення та аналіз загроз

Модель загроз системи безпроводового зв'язку

Системи безпроводового зв'язку (СБЗ) є найбільш вразливою складовою в телекомунікаційній мережі. Для забезпечення захищеності інформації, що передається СБЗ, необхідно оцінити і мінімізувати ризики, які виникають в результаті реалізації атак противником.[21] Але перед усім необхідно оцінити загрози захищеності СБЗ.

Синтезована модель загроз СБЗ представлена на рис. 4.1. При побудові приведеної моделі загроз СБЗ враховувались лише нижні два рівні моделі взаємодії відкритих систем. Це обумовлюється тим, що захисту інформації на вищих рівнях приділяється достатньо уваги, і переважно вони технічно не реалізовані в більшості СБЗ, особливо спеціального призначення. [21]Структурно в складі СБЗ окремо виділені такі складові, як система управління(СУ) та система захисту (СЗ). Вказані загрози носять як штучний так і природній характер.

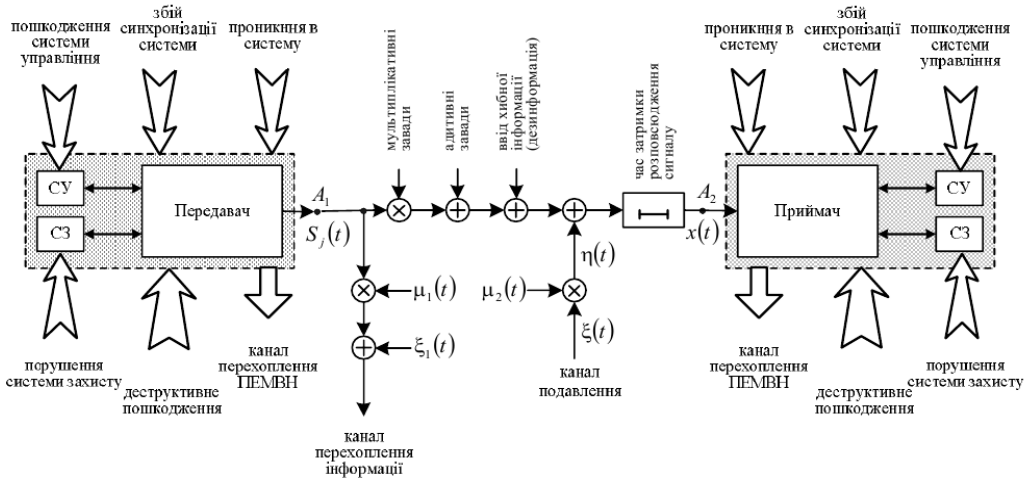

Рис. 4.1 Узагальнена модель загроз бездротової мережі

Загрози інформації діляться по критеріях безпеки на загрози конфіденційності, цілісності та доступності інформації. Приведена загальна модель загроз для СБЗ дозволить виділити та оцінити порушників, які створюють ці загрози, оцінити ризики, розрахувати захищеність СБЗ та застосувати необхідні механізми захисту СБЗ, розроблена модель загроз представлена в таблиці 4.1.

Таблиця 4.1.

Модель загроз бездротових мереж

№ з/п	Вид загроз	Механізми реалізації	Властивості інформаціних об'єктів		
			К	Ц	Д
1	Моніторинг, аналіз трафіку, розвідка	Перехоплення інформації, що переси лається, у незашифрованому вигляді в широкомовному середовищі передачі даних	+	+	+
2	Підміна довіреного об'єкта мережі із підробкою мережних адрес	Фальсифікація (підробка мережних адрес IP-адреси, повторне відтворення повідомлень при відсутності віртуального каналу, недостатні ідентифікації та аутентифікації при наявності віртуального каналу	+	+	+
3	Зміна маршрутизації	Зміна параметрів маршрутизації й змісту інформації, що передається, внаслідок відсутності контролю за маршрутом повідомлень чи відсутності фільтрації пакетів із невірною адресою	+	+	+
4	Відбір інформації та збереження її шляхом впровадження хибних об'єктів (атаки типу «люди на посередині»)	Використання недоліків алгоритмів віддаленого пошуку	+	+	+
5	Подолання систем адміністрування доступом до робочих станцій, локальних і бездротових мереж, заснованих на атрибутах управління доступом і маршрутизації	Використання недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.). Недостатні ідентифікації та автентифікації об'єктів РОМ, зокрема, адреси відправника	+	+	+
6	Подолання криптографічної захищеності ІО, що перехоплені	Використання витоків технічними каналами, вилучення із мережі специфічних вірусних атак шляхом впровадження програм-шпигунів (spyware) із розкриттям ключових наборів	+		
7	Подолання криптографічної захищеності інформаційних об'єктів робочих станцій	Несанкціонований доступ до інформаційних об'єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.) із розкриттям ключових наборів	+		
8	Модифікація переданих даних, даних чи програмного коду, що зберігаються в мережі	Модифікація чи підміна інформаційних об'єктів (програмних кодів) чи їхніх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності		+	+
9	Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні)	Використання атак типу «спрямований шторм» (Syn Flood), передачі на об'єкт, що атакується, некоректних, спеціально підібраних запитів Використання анонімних (чи із модифікованими адресами) запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу			+

4.2 Розроблення системи захисту інформації бездротової мережі

Загальна схема системи захисту бездротової мережі

Головними напрямками захисту будь-яких мереж, у тому числі і бездротових є суттєві з позиції безпеки властивості інформації: конфіденційність, цілісність та доступність, які в свою чергу і уособлюють значення безпеки, графічне зображення даного факту представлене на рис.4.2.

Рис. 4.2 Головні напрямки безпеки бездротової мережі

Безпека мережі представляється наступними вимогами:

Конфіденційність особистих та інших важливих даних;

Цілісність і точність інформації, що зберігається і програм, які її обробляють;

Доступність систем, даних і служб для тих, хто має право доступу. [16]

Загрози безпеці бездротових мереж стосовно основних властивостей інформації:

- загроза усім 3 цілям безпеки ➔ Вторгнення
- загроза конфіденційності ➔ Викрадення інформації
- загроза цілісності ➔ Модифікація даних
- загроза доступності ➔ Відмова в обслуговуванні

Для підтримки даних властивостей в бездротовій мережі застосовуються особливі засоби безпеки представлені на рис.4.3.

Детальніше опишемо основні компоненти побудованої схеми захисту.

Конфіденційність

Заборона трансляції в ефір ідентифікатора SSID; використання цифрових ключів шифрування потоків даних за допомогою функцій WEP, WPA, WPA-2 та VPN вже були детально розглянуті в попередніх розділах дипломної роботи. Зупинимось на засобах, опис яких є новим та необхідним для роботи.

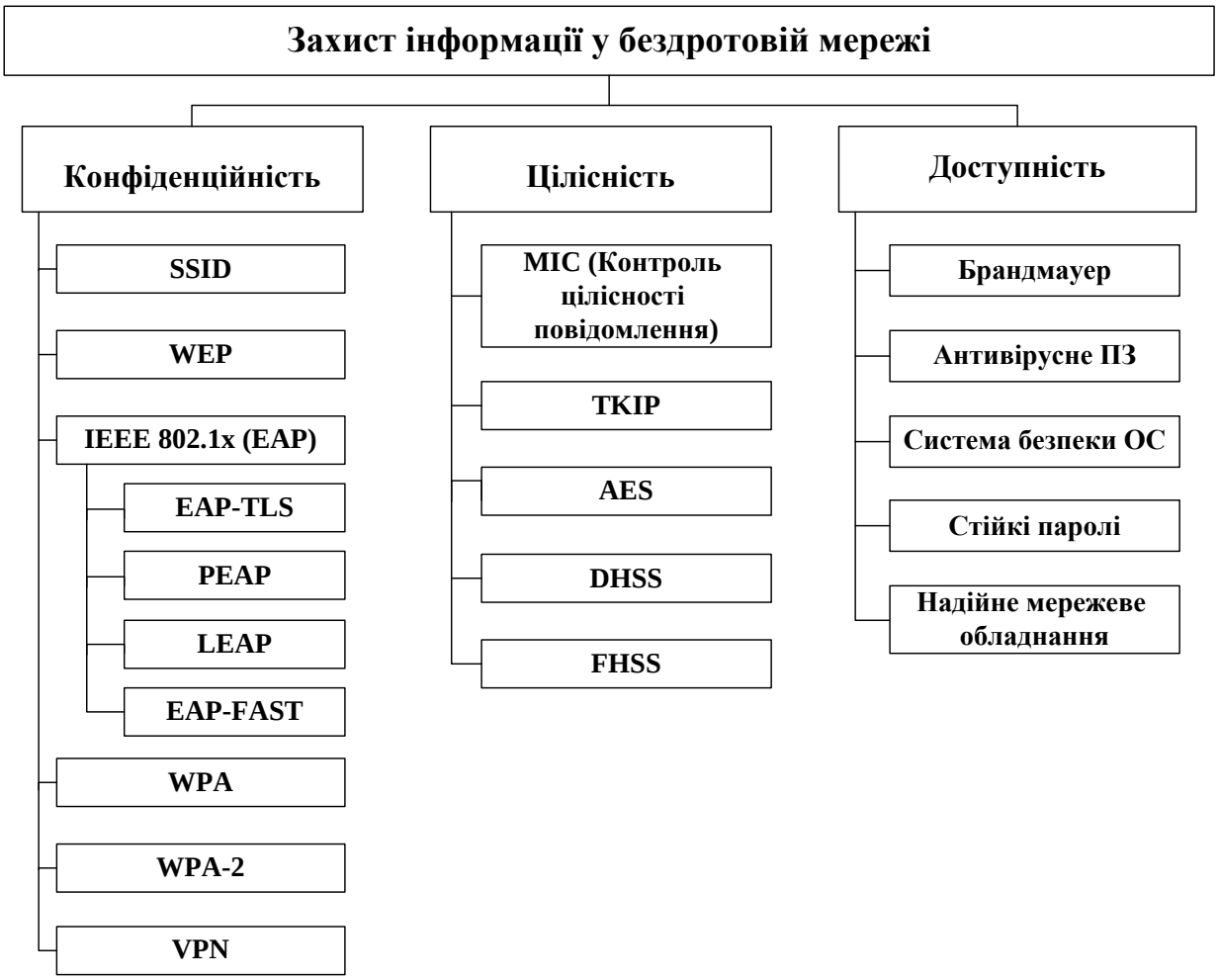

Рис. 4.3 Загальна схема засобів безпеки у бездротових мережах

Спосіб аутентифікації стандарту 802.1x. Принципова відмінність його від колишніх способів аутентифікації полягає в наступному: поки не буде проведена взаємна перевірка користувач не може ні приймати, ми передавати ніяких даних.[11]

• EAP-TLS - стандарт IETF, що забезпечує автентичність шляхом двостороннього обміну цифровими сертифікатами;

• PEAP - покищо попередній стандарт (draft) IETF, який передбачає обмін цифровими сертифікатами та додаткову перевірку імені та пароля по спеціально створеному шифрованому тунелю;

• LEAP-фірмовий протокол Cisco Systems, що представляє собою "легкий" протокол взаємної аутентифікації, схожий на двосторонній Challenge Authentification Protokol (CHAP). Використовує розділяємий ключ, тому вимагає продуманої політики генерації паролів;

• EAP-FAST - розроблений на підставі попереднього стандарту (draft) IETF для захисту від атак за словником і має високу надійність. Принцип роботи схожий з LEAP, але аутентифікація проводиться по захищеному тунелю.

Цілісність

На підставі рекомендацій 802.11i для захисту бездротових мереж реалізований протокол TKIP (Temporal Integrity Protocol), що забезпечує зміну ключа шифрування PPK (Per Packet Keying) [16]в кожному пакеті і контроль цілісності повідомлень MIC (Message Integrity Check).

Забезпечення цілісності покладено на компонент MIC. Забезпечується ефективний контроль цілісності фреймів даних з метою запобігання проведення таємних маніпуляцій з фреймами і відтворення фреймів.

Інший перспективний протокол шифрування та забезпечення цілісності, вже зарекомендував себе в дротяних рішеннях, - AES. Він має кращу криптостійкості порівняно DES, і як уже зазначалося, він забезпечує і шифрацию, і цілісність. Також слід відмітити, що у бездротовому устаткуванні стандарту IEEE 802.11 передбачені спеціальні заходи захисту від порушення цілісності мережі: розширення спектру сигналу у варіанті DSSS або FHSS. [11]

Доступність

Найбільш дієвим захистом від DoS-атак є розробка і дотримання таких правил безпеки:

- встановлення та оновлення брандмауерів;
- постійне оновлення антивірусних програмних засобів;
- встановлення останніх «латок» (оновлень);
- використання довгих паролів;
- від'єднання мережевих пристроїв, які не використовуються.

Також забезпечити захист безпровідної мережі від атак типу «відмова в обслуговуванні» можна за допомогою зменшення проникнення радіосигналів ззовні в будівлю.

Універсального способу протидії DoS-атакам всіх типів не існує. Тому, якщо в результаті атаки безпровідна мережа все ж таки вийшла з ладу, слід забезпечити перехід до пакетного опрацювання даних за допомогою провідникової мережі.

Побудова системи захисту інформації бездротової мережі.

Вибір компонентів та засобів захисту СЗІ. Модель об'єкту захисту.

Модель об'єкту захисту бездротової мережі запропонована на основі представленої на рис 4.4. системи захисту інформації БМ, детальніше розглянемо компоненти побудованої ситеми, та обґрунтування їх вибору, таблиця 4.2.

Обгрунтування необхідністі обраних заходів для СЗІ БМ

Брандмауер. Базове завдання брандмауера – фільтрація інформаційного потоку даних трафіку, що пов'язана з вибірковим пропусканням даних через екранувальний фільтр. Фільтрація здійснюється на основі низки правил. Що

завантажується в екран мережі, а також згідно встановлених мережних аспектів, які є вираженням принятої політики безпеки.[54]

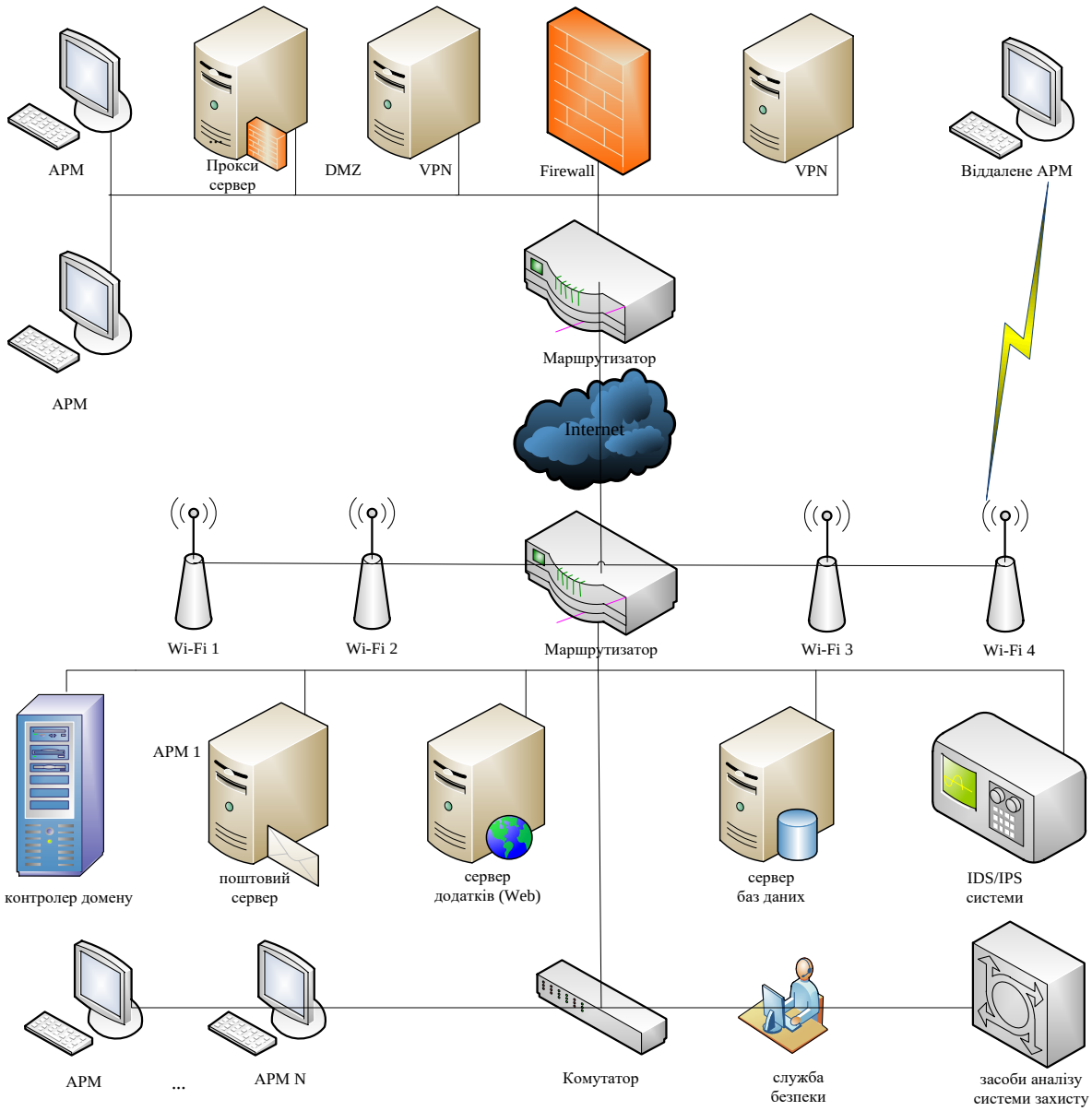

Рис. 4.4 Система захисту інформації бездротової мережі

DMZ (демілітаризована зона). DMZ організує розподіл інформаційних ресурсів й мережних послуг на базі серверних технологій та забезпечує захист інформації від зовнішніх втручань з глобальної інформаційної мережі на основі роботи між мережних екранів і фільтруючих маршрутизаторів. Головна перевага використання DMZ, полягає в тому, що при атаці на загальнодоступний ризик компрометації внутрішніх серверів знижується, оскільки загальнодоступні й внутрішні сервери віддалені один від одного.

Таблиця 4.2

Модель обэкту захисту

№	Компонент системи	Опис
1	Про́ксі-се́рвер	служба в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережевих служб. Також проксі-сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак і допомагає зберігати анонімність клієнта.
2	Фаєрво́л, файрво́л	пристрій або набір пристроїв, сконфігурованих щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв.
3	VPN (Віртуальна приватна мережа)	це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.
4	ДМЗ (демілітаризована зона, DMZ)	технологія забезпечення захисту інформаційного периметра, при якій сервери, що відповідають на запити з зовнішньої мережі, знаходяться в особливому сегменті мережі (який і називається ДМЗ) і обмежені в доступі до основних сегментах мережі за допомогою брандмауера (файрвола), з метою мінімізувати збиток, при зломі одного із загальнодоступних сервісів знаходяться в ДМЗ.
5	Інтерне́т	всесвітня система взаємосполучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів.
6	Маршрутиза́тор	електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.
7	Контролер домену	сервер, який контролює область комп’ютерної мережі (домен).
8	Поштовий сервер, сервер електронної пошти	в системі пересилки електронної пошти так зазвичай називають агент пересилання повідомлень. Це комп'ютерна програма, яка передає повідомлення від одного комп'ютера до іншого..
9	Веб-се́рвер	це сервер, що приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними.
10	Сервер БД	обслуговує базу даних і відповідає за цілісність і збереження даних, а також забезпечує операції вводу-виводу при доступі клієнта до інформації.
11	Intrusion Detection System (IDS)	Система виявлення вторгнень (СВВ) - програмне або апаратне засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет.
12	Мере́жний комута́тор	пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора комутатор передає дані тільки безпосередньо отримувачу.
13	Засоби аналізу системи захисту	призначені для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації.
14	Служба безпеки	підрозділ організації, який створюється з метою забезпечення безпеки шляхом реалізації політики безпеки.

Переваги застосування DMZ

1. Забезпечується можливість виявлення вторгнень, фільтрації й моніторингу змісту на рівні додатків. У такий спосіб забезпечується захист інформаційних ресурсів внутрішньої мережі від зовнішніх та внутрішніх зловмисників.
2. Організація DMZ забезпечує додатковий рівень захисту від атак на загальнодоступні сервери через відкриті порти.
3. Організація DMZ дозволяє контролювати вихідний трафік на предмет поширення модифікованої або спотвореної інформації чи даних.
4. Організація DMZ дозволяє обмежити доступ до адміністративних служб.
5. Технологія організації DMZ дозволяє виявити та захистити серверні платформи від спотворення інформації типу підміни адрес (spoofing) з використанням протоколу ARP (Adress Resolution Protocol).

ВИСНОВКИ

Бакалаврська робота присвячена темі захисту інформації у бездротовій мережі та вирішенню питань підвищення ефективності функціонування, захищеності та активного реагування на спроби порушення безпеки бездротової мережі створення і реалізації системи захисту інформації бездротової мережі та вибору надійних технологій і методів захисту

В роботі відбулось ознайомлення з бездротовими мережами передачі даних. Розглянуто основні елементи бездротової мережі, методи доступу до середовища, загрози і ризики безпеки бездротових мереж. Детально описані поняття архітектури, стандарт IEEE 802.11 та технологія WiMAX.

Також було проведено аналіз аутентифікації бездротових мереж і виявлено основні проблеми і вразливості, які виникають в системі захисту інформації бездротових мереж.

В роботі наводиться загальна структурна схема системи виявлення вторгнень в бездротові мережі, в якій описані її основні характеристики. А також описані технології цілісності і конфіденційності переданих даних.

В роботі особлива увага приділялась основним механізмам шифрування WEP і WPA та їхнім вразливостям.

Розкрите поняття захисту інформації бездротової мережі від несанкціонованого доступу. Розглянуті механізми реалізації несанкціонованого доступу в бездротових мережах.

Також представлена детальна класифікація загроз інформаційним ресурсам бездротової мережі.

На практиці було створено та реалізовано систему захисту інформації бездротової мережі, попередньо побудувавши модель загроз бездротової мережі.

Також для ще більш надійного захисту передаваних даних можна створити зовнішню захисну оболонку бездротової мережі, використовуючи технологію **VPN** понад WPA, що додасть другий рівень шифрування трафіку.

І, нарешті, для отримання достатньо серйозного рівня безпеки необхідно скористатися рядом правил при організації і налаштуванні бездрортової мережі.

Тому розроблені в дипломній роботі необхідні і додаткові методи захисту бездротових мереж та рекомендації для підвищення ефективності функціонування, захищеності та активного реагування на спроби порушення безпеки бездротової мережі є універсальними та прийнятими до застування в багатьох бездротових мережах.

Звичайно, стопроцентної гарантії безпеки бездротових мереж не може надати ніхто, але запропоновані засоби захисту є перевіреними і надійними, тому використання їх для захисту інформації у мережі утворює стійку до атак систему.

Необхідно наголосити, що дана дипломна робота може використовуватися як методичні рекомендації або ряд правил, які треба дотримуватись при створенні системи захисту інформації бездротової мережі або для організації і налаштування приватної Wi-Fi мережі.