МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

МЕХАНІЗМ АНАЛІЗУ ТА ПОШУКУ ВРАЗЛИВОСТЕЙ В БЕЗДРОТОВИХ МЕРЕЖАХ

Виконав: студент групи 2К-21
Спеціальності 123 Комп’ютерна інженерія
Євгеній ШЕВЧЕНКО
Керівник:
Майя ЛЮТА

Черкаси 2025

АНОТАЦІЯ

Кваліфікаційна робота на тему «Механізм аналізу та пошуку вразливостей в бездротових мережах» складається з вступу, основної частини, що містить 3 розділи, висновку та списку використаних джерел. Загальний обсяг роботи – 62 сторінок. У роботі 14 рисунків та 10 таблиць. Перелік використаних ресурсів налічує 19 одиниць.

Метою роботи постає аналіз та дослідження повноцінного функціоналу побудови бездротових мереж на основі класифікації систем, поетапний аналіз типів захисту Wi-Fi мереж та повноцінний механізм їх реалізації.

В першому розділі встановлено класифікацію та характеризацію мереж, розглянуто широко використовувані мережі зловмисниками малого діапазону покриття.

В другому розділі розглянуто основоположення стандартів IEEE 802.11 їх класифікація, та методологія роботи. Проведений аналіз основоположних систем захисту (WEP,WPA,WPA2,WPA3) та типи їх шифрування.

В третьому розділі зіставлена класифікація атак бездротових мереж, згідно наявності вразливостей. Реалізований механізм пошуку DoS атак, та методи їх усунення.

Згідно виявлених класифікацій атак, було встановлено механізм пошуку вразливостей на відмову, проведений аналіз «Периферійних шпигунів», та встановлено методи покращення захисту мережі.

Ключові слова: ЗАХИСТ, ВРАЗЛИВОСТІ, СИСТЕМА АНАЛІЗУ МЕРЕЖІ, ОСНОВОПОЛОЖНІ ТИПИ ЗАХИСТУ, БЕЗПЕКА РОБОЧОГО СЕРЕДОВИЩА.

ABSTRACT

The qualification work on the topic "Mechanism for analyzing and searching for vulnerabilities in wireless networks" consists of an introduction, the main part, which contains 3 sections, a conclusion and a list of sources used. The total volume of the work is 62 pages. The work contains 14 figures and 10 tables. The list of resources used has 19 units.

The purpose of the work is to analyze and study the full functionality of building wireless networks based on the classification of systems, a step-by-step analysis of the types of protection of Wi-Fi networks and a full mechanism for their implementation.

The first section establishes the classification and characterization of networks, considers networks widely used by attackers with a small coverage range.

The second section considers the fundamentals of IEEE 802.11 standards, their classification, and the methodology of work. An analysis of the basic protection systems (WEP, WPA, WPA2, WPA3) and their encryption types is carried out.

The third section compares the classification of attacks on wireless networks, according to the presence of vulnerabilities. A mechanism for searching for DoS attacks and methods for eliminating them are implemented.

According to the identified classifications of attacks, a mechanism for searching for vulnerabilities to denial of service was established, an analysis of "Peripheral Spies" was conducted, and methods for improving network protection were established.

Keywords: PROTECTION, VULNERABILITIES, NETWORK ANALYSIS SYSTEM, BASIC TYPES OF PROTECTION, WORK ENVIRONMENT SECURITY.

ЗМІСТ

ВСТУП

Тема кваліфікаційної роботи зіставлена зі все зростаючою роллю Wi-Fi мереж в забезпеченні ефективної управлінської та організаційної бази, в дійових межах різних типів організацій. При такому обсягу взаємодії робочих компонентів, постає питання в цілісності передачі даних, та поетапному захисту можливих дійових механізмів, повно етапного базису. В цілому спостерігається сукупність низок вразливих місць до несанкціонованого доступу в бездротову мережу, при даній інтенсивності трафіку, кібер-злочинці отримують можливість безперешкодно маніпулювати даними та системами, які мають безпосередній доступ до мережі.

Об'єктом дослідження в кваліфікаційній роботі є механізм захисту даних та протоколи шифрування інформації в бездротових мережах.

Предметом дослідження є механізм пошуку вражливостей Wi-Fi мереж шляхом їх аналізу, та поправки за для налагодження безперервних потоків даних, без порушення безпеки їх передачі.

Метою даної роботи є дослідити повний функціонал побудови бездротових мереж на основі класифікації систем, проаналізувати поетапно систему захисту Wi-Fi мереж та повноцінний механізм її реалізації.

Для досягнення даної мети в кваліфікаційній роботі поставлені та вирішені наступні **завдання:**

1. Проаналізувати поетапно особливості та стандартизації бездротових мереж.

2. Провести ретельний аналіз систем захисту бездротових мереж та пошук вразливостей.

3. Виділити поетапний механізм покращення систем захисту Wi-Fi, та мінімізувати загрози.

Методи дослідження

Теоретичні: систематизація, класифікація, порівняльний аналіз протоколів шифрування бездротових мереж та критичний аналіз технологій Wi-Fi.

Емпіричні: спостереження, прогнозування та перевірка.

Практичне значення одержаних результатів:

1. При проведенні фактичного аналізу мережі, було розширено критерії пошуку вразливостей для оцінки бездротових мереж. Запропоновано ряд критеріїв за для масштабного пошуку та вираження падіння ефективності передачі інформації.

2. Проведення аналізу дестабілізації потоку даних, за для знаходження вразливостей, що до заволодіння інформацією третіми особами. Встановлення головної вразливості при передачі даних.

3. Аналіз комплексних короткотривалих тестів, за для повноцінної перевірки вразливостей та опис дій за для їх усунення.

РОЗДІЛ 1
АНАЛІЗ ТА ЗАГАЛЬНІ ВІДОМОСТІ ПРО СУЧАСНІ ТЕХНОЛОГІЇ БЕЗДРОТОВИХ МЕРЕЖ ТА ЇХ ВРАЗЛИВОСТІ

1.1 Головні основоположення розвитку мережі Wi-Fi

Перший етап розвитку бездротових мережевих систем почався ще в 90-х роках 20-го століття. Типові технології радіо канальної передачі даних використовувались першочергово в локальних мережах масштабних корпорацій гігантів. Початкова варіація даного типу мала велику кількість вад, але водночас могла підтримувати до 30 робочих приладів на кожній з точок доступу. На сьогодні термін Wi-Fi описує більшість технологій працюючих з бездротовими локальними мережами, але первинно даний термін вказував технологію що працює на базисі стандарту IEEE 802.11b з частотою зв'язку 2.4 ГГц та швидкістю обміну даними до 11 Мбіт/с.

З розвитком основних компонентів бездротових мереж, було створено розширений набір стандартів IEEE 802.11 (з класовою системою), які отримали назву Wi-Fi. Даний тип мережі дозволяє передавати данні з допомогою радіохвилей, при передачі даних, швидкість передачі становить близько 100 Мбіт/с. Радіо сигнал, який називається радіочастотою, відходить від точки доступу, яка як правило є роутером, до пристрою, частоту з якою надходить хвиля вимірюється в гігарецах, з чого виходить що 1 гігагерц становить 1 млрд. хвиль на секунду, а 1 герц в свою чергу становить 1 секунда. Джерело доступу в Інтернет в даному випадку – це технологія пакетної передачі даних Ethernet [**Ошибка! Источник ссылки не найден.**]. В будь якому випадку доступ надається тільки при наявності стаціонарного підключенні і роутера чи будь яку точку доступу, яка здатна передавати данні через канали з певною частотою.

Складова точки доступу зіставлена з чотирьох компонентів, головною частиною є інтерфейс підключення мережі також ПЗ для обробки даних,

приймач та передавач. При розгортувані точка доступу створює хвильовий діапазон до 100 метрів безперебійного доступу, також названою Хот-Спот. За канон прийнято вважати, що сучасні роутери працюють на частоті 5 гігагерців на секунду, але більшість з них передають інформацію на невеликі відстані, з великою швидкістю. Саме тому, характеристики бездротових мережі також залежать від встановлених точок доступу, чим більша частота надходження хвиль, тим швидше інформація доходить до користувача, але тим менша робоча область.

В більшості випадків, система містить не менше однієї точки доступу, але підключення в режимі Точка-точка (Ad-hoc) дозволяє підключення двох клієнтів. В даному режимі підключення, користувачі з'єднуються з допомогою мережевих адаптерів безпосередньо напряму (точка доступу не використовується). За допомогою сигнальних пакетів точки доступу надають власний SSID з швидкістю 0.1 Мбіт/с кожні 100 мс, дану швидкість прийнято вважати найменшою швидкістю передачі даних Wi-Fi. Якщо користувач володіє інформацією, що до SSID точки доступу, то він самостійно може перевірити чи має доступ до певної точки. В випадку коли користувач потрапляє в область дії двох різних точок, але котрі мають одинакові SSID, то вибір опирається на рівень сигналу, в даних регаліях стандарт дає самостійний вибір з'єднання.

Класифікація мереж, за способом об'єднання точок доступу:

– автономні (самостійні);
– під управління контролера (централізовані);
– безконтролерні (не автономні).

Безпровідні локальні мережі:

– статичне налаштування радіоканалів;
– динамічне (адаптивне) налаштування радіоканалів;
– багатошаровою структурою радіоканалів.

Не дивлячись на все це, рівень сигналу не стабільний, він може знижуватись та перекриватись в залежності від пристроїв які працюють на

частоті точки доступу. Лише при частоті в 5 гГц можливо подавляти та підтримувати стійку передачу даних, не зважаючи на перешкоди, так як хвиля містить 23 канали, відкриті для передачі. Система передачі даних складається з 3 етапів, створення інформації, перетворення в хвилі та надходження до користувача.

На сьогодні все більше постає питання в необхідності створення власної локальної бездротової мережі, в домашніх умовах і роутери постають найкращим вибором точки доступу, так як вони мають вже встановлений типи захисту та налаштований інтерфейс для взаємодії. При виборі точки доступу, необхідно переглянути підтримку стандартів мережі Wi-Fi, так як деякі з них мають встановлені неіснуючі стандарти.

В основі стандарту також вказана можливість створення мережі одно стільникового варіанту, даний варіант передбачає реалізацію робочої станції яка буде виконувати частково функції точки доступу, але встановлення точки доступу не обов’язкове.

Основні переваги Wi-Fi мереж:

– організація мережі без встановлення кабелю;
– велика кількість можливих підключень до Інтернету;
– наявність фаєрволу, для захисту від зовнішніх загроз;
– простота підключення користувачів;
– зміна місця розміщення користувача в діючому діапазоні, без втрати доступу до ресурсів;
– велика швидкість встановлення мережі;
– мізерна вартість експлуатації;
– мобільність локальної мережі, не зважаючи на умови розташування;
– порівняльна незахищеність даних;
– велика енергозатратливість приладів, що працюють від безпровідних накопичувачів енергії;
– порівняльна слабкість систем захисту.

1.2 Бездротові локальні мережі

Розвиток Інтернету надав нові можливості в створенні та в становленні бездротових мереж. Бездротові мережі дали можливість безперешкодного встановлення мережі, без використання дротів, підключати об’єкти на великих дистанціях та мобільний зв'язок без втрати доступу до ресурсів.

Для спрощеного використання, мережі поділили на 3 типи, за масштабом їх дії (рисунок 1.1):

- глобальну мережу BWA або WWAN (Broadband Wireless Access – мережа широкої дії);
- локальну мережу WLAN (Wireless Local Area Network);
- персональну мережу PAN або WPAN (Wireless Personal Area Network).

WLAN – бездротова локальна мережа, яку використовують як корпоративну мережу як реалізує доступ до групових ресурсів в широкомасштабних приміщеннях, таких як університети, школи, жилі будинки тощо. Даний тип бездротової мережі, як правило заміщує дротові мережі на невеликих підприємствах. Стандарт 802.11 став основоположенням для WLAN.

WPAN – мережа з невеликим радіусом дії, близько 10 метрів. Даний тип мережі використовують для реалізації найпростішого обміну даних, в окремих етапах робочих груп наприклад: в офісу при неможливості прокладання кабельної мережі чи Bluetooth з’єднання мобільних телефонів, принтерів і т.д. з ПК. При підключенні до мережі ми отримуємо відразу доступ до всіх пристроїв в ній, даний тип підключення простіший, ніж отримання доступу шляхом поетапного підключення до кожного елементу мережі окремо. При підключенні система самостійно налаштовує TCP/IP підключення між пристроями.

WWAN – широко масштабний тип мережі, який використовується для надання доступу мобільним користувачам до мережі (Інтернету). Даний тип також класифікують як WMAN, так як він використовує WiMAX, бездротову технологію зв’язку. В сучасному світі, більшість розробників вбудовують

адаптер WWAN в портативні пристрої, що дає змогу отримувати користувачеві безпровідний зв'язок до світових ресурсів в межах дії оператора з будь якої точки. Даний тип зв’язку розповсюджується на платній основі. З точки зору видів комутації в мережах передачі даних мережі WWAN можуть бути побудовані на основі наступних принципів: комутації пакетів (GPRS); комутації каналів (CSD, HSCSD) [**Ошибка! Источник ссылки не найден.**].

Безпека цілісності даних при передачі в межах WWAN, зіставлена типовими типами шифрування і автентифікації, але як і більшість типів, надати повноцінний захист неможливо. На сьогодні відомо 2 із 3 випадки злому ключів шифрування.

Всі пристрої Wi-Fi можливо об’єднати в мережі WLAN, дані мережі являють собою локальні мережі з радіусом дії близько 100 метрів. Для створення мережі даного типу використовують адаптери які являють собою мережеві карти, підключені через слот розширення PCI, PCI-Express або USB та точки доступу, які постають вбудованим в мікропроцесор самостійним модулем та приймально-передавальним пристроєм.

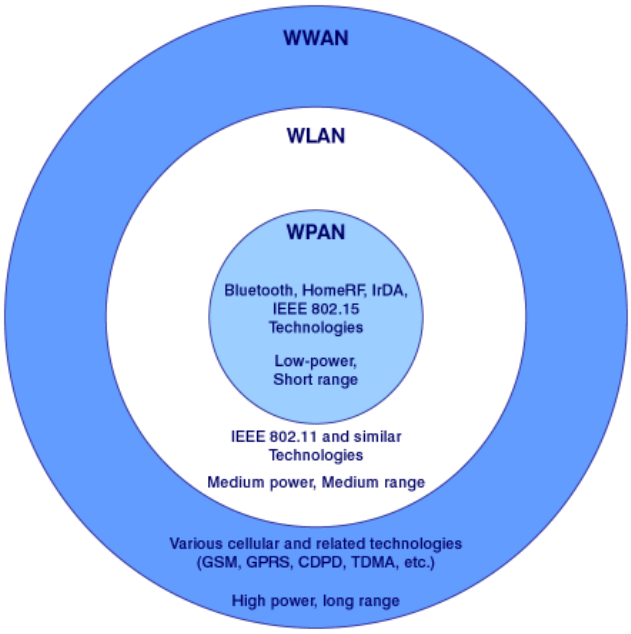

Рисунок 1.1 – Радіус дії бездротових мереж

Для доступу до мережі адаптер може з’єднуватись через точку доступу, даний режим роботи має назву «Інфраструктурним». Через точку доступу

здійснюється взаємодія і обмін інформацією між елементами безпроводової мережі (між безпроводовими адаптерами), а також зв'язок з проводовим сегментом мережі (зображено на рис. 1.2) [**Ошибка! Источник ссылки не найден.**].

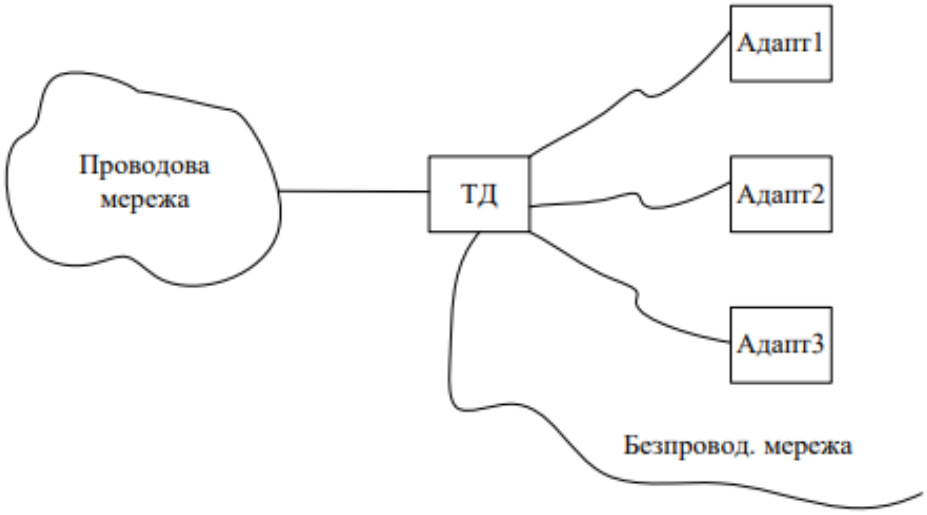

Рисунок 1.2 – Взаємодія між елементами бездротових мереж

Згідно схеми, точка доступу при певному функціоналі постає комутатором, та має в наявності мережевий інтерфейс за для підключення до дротової мережі. Створення бездротових локальних мереж вирішує питання, що до швидкого та стабільного доступу до інформаційних ресурсів, яке використовується в більшості випадках, як Hot spots при проведенні тимчасових заходів.

Діапазон робочих частот WWAN, WPAN та WLAN при побудові мереж та їх технології створення майже не відрізняються. Всі вони працюють в неліцензійних частотах, діапазон який варується від 2,4 до 5 ГГц. Якщо при розсортуванні мережі, в діапазоні працює ще одна мережа також діапазону частот, не дивлячись на це нам не потрібна координація, поправка чи частотне планування що до інших радіомереж.

Wi-Fi і WiMAX є найпоширеніші способи реалізації даної побудови. Дані технології використовують схожі стандарти IEEE 802 (рис. 1.3), мають бездротове підключення і також обидва направленні для підключення до

Інтернету. Не зважаючи на все це, завдання на вирішення яких вони спрямовані різняться. WiMAX, являє собою систему з великою областю дії, яка використовує ліцензовані спектри частот, за для з'єднання провайдера, з користувачем. Wi-Fi, являє собою систему з невеликим радіусом дії до декількох десятків метрів та використанням не ліцензованих частот.

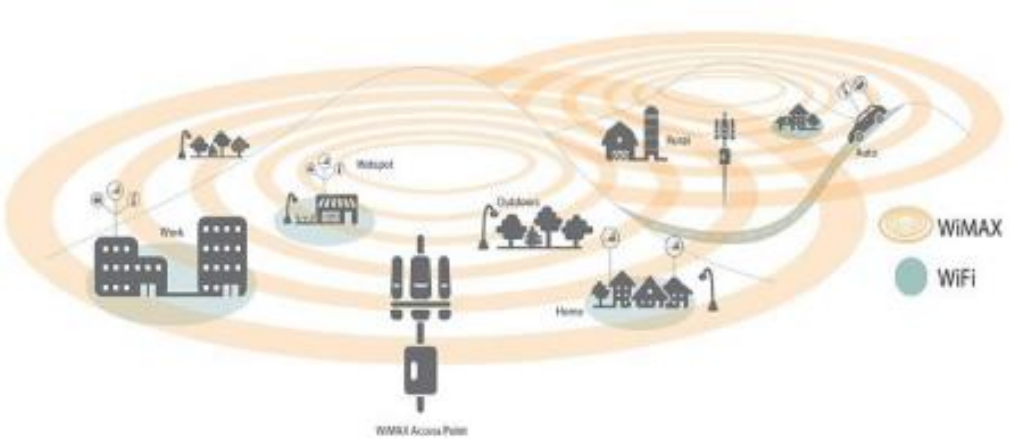

Рисунок 1.3 – Діапазон стандартів безпровідного зв'язку

В порівняльній характеристиці WiMAX можливо вважати як систему мобільного зв'язку, а Wi-Fi більше як стаціонарний бездротовий телефон. Вони мають зовсім різний механізм QoS. WiMAX має певний алгоритм який гарантує значення QoS для будь якого з'єднання. Wi-Fi в свою чергу, використовує механізм з певною пріоритизацією, де кожний пакет отримує різний приорітет. Згідно з простотою реалізації та відносною дешевизною, Wi-Fi частіше використовують при наданні доступу до Інтернету.

1.3 Бездротові мережі малого діапазону покриття

1.3.1 Мережа Bluetooth

Bluetooth (англ. Bluetooth) – вузько масштабна бездротова технологія реалізації зв'язку на базі функціонального інтерфейсу. В 1998 році світ побачив інноваційну розробку групи компаній: Ericsson, IBM, Intel, Nokia, Toshiba, яка отримала назву Bluetooth. Створення даної технології було за для забезпечення

економічного та мобільного типу зв’язку в описових умовах. Умови використання, як і компактність компонентів давала можливість використання Bluetooth в будь яких приладах, порівняльну характеристику зображено в табл. 1.1.

Таблиця 1.1 – Різниця між технологіями IEEE 802.11 та Bluetooth

	IEEE 802.11	Bluetooth
Призначення	Бездротова мережа (Домашня/Офісна)	Компактна бездротова мережа, для заміни дротових з’єднань якщо вони не можливі.
Робоча частота	2.4 ГГц	2.4 ГГц
Швидкість передачі даних	2/11 Мбіт/сек (IEEE 802.11/802.11b)	До 721 Кбіт/с (в залежності від типу)
Діапазон дії	100 м	10/100 м
Кількість вузлів	128 на мережу	8 на піко мережу, максимум 10 піко мереж до 71 приладу на scatternet
Підтримка аудіо каналів	Немає (Встановлення вручну)	3 канали
Ціновий діапазон	До 300 $ за оптимальний безперебійний вузол	До 10 $ за вузол

На відміну від технології інфрачервоного зв'язку IrDA (Infrared Direct Access), що працює за принципом "точка-точка" в зоні прямої видимості, технологія Bluetooth розроблялася для роботи як за принципом "точка-точка", так і в якості багатоточкового радіоканалу, керованого багаторівневим протоколом , схожим на протокол мобільного зв'язку GSM [7]. Конкурентна спроможність Bluetooth набувала великого впливу, що в свою чергу виділило пріоритетні задачі даної технології: об’єднування периферії, створення локальних мереж малої зони, але з великою швидкістю передачі даних тощо. Першочергові етапи розробки даної технології припали на 1994 рік, новоутворена технологія мала узгоджувати потреби FLYWAY системи, тобто при підтримці функціонального інтерфейсу узгоджувати дані між системою та користувачами. З часом Bluetooth технологія стала частиною IEEE 802.15.1 після укладання домовленості між компаніями Bluetooth SIG та IEEE. З того часу будь які компанії, які мали наміри створювати прилади на основі

Bluetooth, могли стати асоціативними членами групи розробників. Навіть після угоди, Bluetooth залишився конкуренто спроможним типовим технологіям як:

– IrDA – технологія об’єднання периферії з ПК, але не налаштована на створення побудову локальної мережі;

– IEEE 802.11;

– HomeRF.

Можливість швидкої передачі даних не була єдиним еквівалентом інформації для передачі, інтерфейс Bluetooth передбачав передачу частотних хвиль певного діапазону чи імітацію звукових сигналів при швидкості 64 Кбіт/с. Для передачі даних використовувались 2 методи: симетричний та асиметричний.

Симетричний метод, має стабільний тип передачі інформації в обох напрямках 432.6 Кбіт/с.

Асиметричний метод, має різнобій швидкості передачі, в одному напрямку 721 Кбіт/с в другому 57.6 Кбіт/с.

Bluetooth, як технологія, була специфічною розробкою, за для досягнення максималізації дешевизни, яка в свою чергу повинна зберігати максимальну безпеку передачі даних, ефективну роботу з різними типами даних та мінімальні розміри передавача. Діапазон розгортуванні мережі складає 10/100 метрів з робочою частотою 2.4 ГГц, обсяги занадто різняться, але це обумовлено тим, що при невеликій дистанції встановлюється передавач компактного розміру, незначної вартості та має зменшене енергоспоживання.

Характеризація технології Bluetooth:

– встановлена інтерфейсна специфіка зниження рівня енергозатрат;

– встановлений тип кодування CVSD (Continuous Variable Slope Delta Modulation), для збільшення робочої області розпізнавання частот та по бітова робота з помилками;

– мінімалізації часу підтвердження доступу;

– спеціалізовані типи пакетів, для реалізації на будь яких додатках.

Реалізація захисту інформації зіставлена типовим шифруванням даних, з встановленням ключа 8-128 біт та варіативним типом автентифікаціїї (Односторонній, Двосторонній). Для додаткової безпеки, встановлення шифрування можливо як на програмному рівні, так і на рівні протоколу.

Принцип дії Bluetooth, постає його частковим захистом. Реалізація зв'язку відбувається за методом FHSS (Frequency Hopping Spread Spectrum), тобто частота сигналу, починає хаотично змінюватись (1600 змін на секунду), робочих частот всього виділяється 79, шириною в 1 Мгц. Послідовність перемикання між частотами для кожного з'єднання є псевдовипадковою і відома тільки передавачу і приймачу, які кожні 625 мкс (один часовий слот) синхронно перебудовуються з однієї частоти, що несе, на іншу [7]. Таким чином прийняти і зрозуміти передані дані, зможе лиш та пара приймач-передавач, яка використовує один шаблон передачі, для інших приладів передача буде не помітною чи відображатиметься як шум.

Для реалізації стандарту Bluetooth, були створені окремі контролери:

– Class 1. Потужність 100 мВт. Радіус дії близько 100 метрів;
– Class 2. Потужність 2,5 мВт. Радіус дії близько 10 метрів;
– Class 3. Потужність 1 мВт. Радіус дії близько 1 метра.

В сучасних регаліях розвитку мереж, лише 2 класи отримали визнання Class 1 та 2.

1.3.2 Технологія UWB

Незважаючи на проривні можливості Bluetooth, технологія мала значимі недоліки, які намагалися виправити інші паралельно створювані стандарти з невеликим робочим діапазоном та порівняльно більшими швидкостями. Головною проблемою постала передача громісткої інформації на невелику дистанцію. Bluetooth, як і Wi-Fi не здатні швидко опрацювати дану інформацію, так як вони не призначені для повноцінної широко смугової передачі, тому

постала необхідність швидкісної передачі даних на невелику відстань, вирішення даної проблеми постала технологія UWB.

UWB – Ultra Wideband «над широка смуга», основоположенням постали широкосмугові високочастотні, низької спектральної потужності імпульси передачі даних, які забезпечують над швидкий зв'язок.

Головним стандартом для широкосмугового зв'язку став IEEE 802.15.4a, на відміну від свої попередників IEEE 802.11b та 802.11a робочий діапазон яких зіставляв 3/10 робочих каналів, підтримка близько 100 робочих каналів стала найкращим вибором. Передача даних за технологією UWB створювалась шляхом генерування хвиль з широким діапазоном частот в встановлені моменти часу, що в свою чергу викликає модуляцію за часом.

Підтримка робочого середовища UWB працюючого в діапазоні нижніх рівнів шуму радіосистем, не потребує значного вкладу, система не потребує особливих типів і характеристик обладнання, на відміну від високочастотних елементних баз, які в свою чергу мають громістку та складну систему, яка потребує значних затрат. Частоти діапазонів від 500 МГц, слугують робочим середовищем при передачі даних та визначають можливу швидкість передачі даних технологією UWB. Використання радіочастотних спектрів глобальної взаємодії мають значні рамки в положенні різних країн, що в свою чергу обмежує діапазон розгортування, але не зменшує швидкість передачі від 480 Мбіт/с до десятків гігабіт в межах мережі.

Використання обладнання для роботи сигналу в діапазоні рівню шуму слугує двоетапнім типом захисту (Захист користувачів при передачі/прийому даних, захист точки доступу від несанкціонованого доступу в безпосередній віддаленості від обладнання). Прийняття сигналу стороннім пристроєм можливе лише в рамкам фізичного підключення до систему, через точку доступу а діапазон змінних частот дає практично неможливим перехоплення даних на відстані.

Головною особливістю даного типу постає можливість безперебійної передачі, навіть поза межами зони безпосередній видимості.

1.3.3 Технологія ZigBee

Створення новітніх стандартів різних типів і можливостей використання, поставило питання, що до створення локальної автономної мережі, яка самостійно створює автоматичне підключення пристроїв і координує робочий процес, вирішенням даного питання зайнялось формування компаній під назвою ZigBee™.

ZigBee – стандарт для набору високорівневих протоколів зв'язку, що використовують невеликі, малопотужні цифрові приймачі, заснований на стандарті IEEE 802.15.4-2006 для бездротових персональних мереж, таких як, наприклад, бездротові навушники, що з'єднані з мобільними телефонами за допомогою радіохвиль короткохвильового діапазону [**Ошибка! Источник ссылки не найден.**]. Структуризація робочих компонентів стандарту ZigBee для сполучення пристроїв, відрізнялася від основних типів бездротових стандартів, основною відмінністю стала топології «Mesh».

Створення робочого середовища поділялося на 3 етапи:

- координатор «ZigBee Coordinator»;
- роутер «ZigBee Router»;
- кінцеві пристрої «ZigBee End Device».

Coordinator слугує головним компонентом мережі, може бути виражений в виді Моста чи Роутера в залежності від необхідного типу передачі даних, тобто пристрій від якого утворюється мережа. Router в даній мережі слугує типовим обладнанням зв’язку між кінцевими пристроями, він приймає потік даних і може вести обмін даними з будь якими Routers і Coordinators в межах мережі (рис. 1.4). End Devices це пристрої призначені тільки для передачі даних як правило гаджети.

Рисунок 1.4 – Топологія ZigBee

Через низьку швидкість передачі інформації та специфікацію утворення мережі, система не набула проривного ефекту як система об’єднання та обміну даними між девайсами чи комп’ютерами, але стала незамінною технологією при створенні охоронних системи чи розумного будинку, які вміщують в себе велику кількість датчиків, пристроїв дистанційного керування тощо**.** Передача інформації по мережі надходить побітово чи побайтово від End Devices в виді сигналів.

Технологія ZigBee має порівняно невелику швидкість передачі даних, згідно інформації наведеної в табл. 1.2, але це не критично, так як використання слугує за для автоматизації систем при порівняно низьким енергозатратам.

Таблиця 1.2 – Різниця між технологіями Bluetooth, Wi-Fi, ZigBee

Технологія	ZigBee	Wi-Fi	Bluetooth
Стандарт зв’язку	IEEE 802.15.4	IEEE 802.11	IEEE 802.15.4
Швидкість обміну даними	250 Кбіт/с	Від 300 Мбіт/с	До 3 Мбіт/с
Енергозатратність	Низька	Висока	Низька
Робоча частота	2.4 Ггц	2.4 Ггц	2.4 Ггц
Підтримка IP	Ні	Так	Ні
Топологія	Зірка, mesh	Зірка, mesh	Зірка, mesh

Особливість мережі ZigBee постає в тому, що якщо в системі знаходиться два Coordinator «Шлюза» які поставлені один після одного то вони

встановлюють контакт між системами і кожна наступна система підхопить мережу першого Шлюза, якщо один з головних Coordinators відключиться то підконтрольні Units можливо переключити на інший Coordinator. Коли декілька Coordinators встановлені в не зони дії друг друга, то вони вважаються незалежними мережами.

На сьогодні головними користувачами технології ZigBee постає компанія Xiaomi, на основі якого створюються системи розумних будинків та мережі охорони державних споруджень.

Висновки до розділу 1

Питання щодо отримання якісної мережі з стабільним типом підключення, постало головним завданням в сучасних реаліях. Систематизація розвитку технологій доступу до мережі охопила також розвиток мережевого обладнання яке постало базисом новітніх стандартів. Новітні стандарти вирішили питання що до розмежування зони покриття без втрати швидкості передачі даних, вирішили питання максимально можливих активних підключень без великих енергозатрат і цінового діапазону та встановили оновлені типи захисту інформації, що в свою чергу створило класифікацію однотипних стандартів за можливістю використання та максимально можливим КПД.

Перші типові технології Wi-Fi і WiMAX стали основоположення сучасного доступу до Інтернету. Технологія WiMAX стала повномасштабним типом передачі інформації на великих відстанях з великою швидкістю, але через громісткість робочого обладнання, складність налаштування та тип розповсюдження, стати заміною для офісних мереж, стандарту не вдалось.

Wi-Fi в свою чергу мала значно меншу швидкість передачі даних, та менший діапазон покриття, але завдяки дешевизні та компактності обладнання, простоті налаштування та малій енергозатратності, Wi-Fi став першочерговим вибором для встановлення мережі.

Як і в багатьох інших областях, у бездротовій передачі даних немає універсальної технології. Під кожні конкретні завдання більше підходить WiMAX або Wi-Fi. Якщо поставлено завдання надати широкосмуговий доступ до мережі, для користувачів, доцільніше використовувати WiMAX, тому що ця технологія була розроблена саме із цією метою. Однак, якщо завдання надати широкосмуговий доступ в обмеженому приміщенні, то технології Wi-Fi і WiMAX однаково добре підходять для вирішення, за умови низького рівня перешкод або їх відсутності. Для впровадження бездротових систем безпеки або відеоспостереження доцільніше скористатися технологією Wi-Fi.

Технології та стандарти перейшли на новий рівень, за останні десять років характеристики та асортимент можливостей виріс в декілька разів, що впровадило локальні мережі майже до будь якого ПК чи пристрою.

РОЗДІЛ 2
ОСНОВОПОЛОЖЕННЯ СТАНДАРТІВ IEEE 802.11 ТА КЛАСИФІКАЦІЯ ТИПІВ ЗАХИСТУ WI-FI

2.1 Основоположення стандартів IEEE 802.11

В кінці 20-го ст. була створена окрема група, Комітетом IEEE 802, для аналізу бездротових мереж, та створення стандартів. В 1997 році світ побачив базисний стандарт IEEE 802.11, що працював з мережею з частотою 2.4 ГГц та швидкістю 1-2 Мбіт/с. Всі стандарти IEEE 802.11 працюють на нижніх двох рівнях моделі ISO / OSI, фізично і канальному, тому будь-який мережевий додаток, мережева операційна система, або протокол (наприклад, TCP / IP), будуть так само добре працювати в мережі 802.11, як і в мережі Ethernet [3]. Фізичний рівень вміщує в собі різноманіття специфікацій, які різнять між собою в залежності від типу кодування, діапазону частот і швидкістю передачі інформації.

Для базового стандарту 802.11 передбачено робочий частотний діапазон від 2400-2483,5 Мгц, розмежований на декілька частотних каналів котрі мають ширину діапазону 83.5 Мгц.

На сьогоднішній день група стандартів IEEE 802.11 набула широкомасштабних оновлень від чого було створена велика кількість апгрейдів.

Стандарт на початку показував гарний результат, ставши першим продуктом WLAN від дочірньої компанії, але на момент релізу зіткнулися з проблемою, недостатністю встановленої швидкості, це спонукало до створення новітнього стандарту до моменту релізу.

Найбільшого практичного використання набули лише декілька типів: 802.11n, 802.11b і 802.11g які в свою чергу були виділені «Інженерним інститутом електротехніки й радіоелектроніки». Для більшої конкретизації

можливостей робочого середовища та їх класифікації на основі характеристик конкретної технології наведено таблицю (табл. 2.1).

Таблиця 2.1 – Суміжність технологій зі стандартами

Назва стандарту	Швидкість передачі	Радіус дії
WWAN		
GSM	9.6 Кб/с	Сота до 35 км
CDMA	14.4 Кб/с	Сота до 20 км
IEEE 802.20 WiMAX	Більше 1 МБ/с	Радіохвилі мобільного зв'язку, залежність від точки доступу
IMT2000	2 МБ/с (для низько мобільних) – 384 Кб/с (для високо мобільних)	Сота від 20-40 км
WPAN		
IEEE 802.15.3	11/22/33/44/55 Мб/с	До 10 м
IEEE 802.15.3a UWB	100 МБ/с-1,3 Гб/с	Від 5-10 м
IEEE 802.15.4 ZigBee	20/40/250 Кб/с	До 10 м
IEEE 802.15.1 Bluetooth	64 Кб/с-1 Мб/с	Від 10-100 м
Home RF	1/2 Мб/с-10/20 Мб/с	До 50 м
WLAN		
IEEE 802.11ac	Більше 1 Гбіт/с	100 м
IEEE 802.11n	Більше 160 Мб/с	100 м
IEEE 802.11g	Від 11-54 Мб/с	100 м
IEEE 802.11b	Від 2/5-11/33 Мб/с	100 м
IEEE 802.11a	6/9/12/18/24/36/48/54 Мб/с	100 м
IEEE 802.11	1-2 Мб/с	300 м
DECT	70 Кб/с	30-70 м (в закритій зоні), 100-400 м (в відкритій зоні)
WMAN		
IEEE 802.11.16 WiMAX	Від 30-40/70 Мб/с	Від 2.5-5 км (мобільні елементи) Від 40-50 км (Сталі елементи)
IEEE 802.11.16e WiMAX	До 15 Мб/с	Від 2-7 км
IEEE 802.11.16f/h WiMAX (широко використовувані)	До 10 Тб/с	Можливість мобільного підключення до 300км/ч

Особливість робочої специфіки стандартів 802.11 полягає в знаходженні та створенні зв'язку між точкою доступу яка слугує двотипним (дротовим/бездротовим) мережевим обладнанням котре має влаштоване ПО для роботи з даними, приймач і дротовий інтерфейс, та клієнтським мережевим обладнанням (як правило слугує мережева карта чи телефонна гарнітура підтримуюча стандарт 802.11). З вище сказаного, маємо, що даний стандарт

встановлює можливість роботи мережі в двох режимах, клієнт-сервер та точка-точка.

В режимі точка-точка, відповідно до рис. 2.1, маємо мережу в яку з’єднання встановлюються напряму між робочими компонентами, при такому з’єднані використання точки доступу можливо уникнути. Найчастіше використання даного типу обумовлене неможливістю встановлення бездротової мережі.

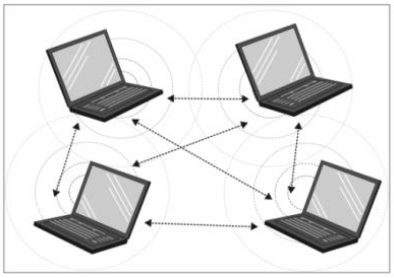

Рисунок 2.1 – Архітектура мережі типу точка-точка

В режимі клієнт-сервер, відповідно до рис. 2.2, першочерговою особливістю є наявність точки доступу підключеної до дротової мережі, яка об’єднана з декількома бездротовими приладами. Даний тип через використання базового набору елементів, отримав назву BSS (Basic Service Set), а декілька об’єднаних BSS отримали назву ESS (Extended Service Set).

Рисунок 2.2 – Архітектура мережі типу клієнт-сервер

Передача даних по протоколу IEEE 802.11 виконується 2 методами, які реалізуються на фізичному рівні:

– FHSS (Frequency Spread Spectrum);

– DSSS (Direct Sequence Spread Spectrum).

При використанні методу FHSS, необхідно першочергово дізнатися максимально можливе переключення каналів в секунду для країни в які використовують метод, так як головний етап постає саме в переключенні каналів, а зі збільшенням часу переключення, зростають затрати на робочий процес. Сам метод схожий на діапазон частотних стрибків від 2.402 до 2.480 ГГц де потік розмежовується на 79 каналів шириною 1 МГц. Данні при передачі надсилаються за раніше встановленою схемою переключення між відправником і отримувачем, потік надходить послідовно до кожного каналу згідно встановленого плану, як правило максимально можлива кількість схем 22. Вірогідність того що 2 передачі даних будуть використовувати одинакові канали низька. Швидкість передачі даних становить близько 2 Мбіт/с, це обумовлено тим, що схема приймача занадто проста але компактна.

Метод DSSS на відміну від FHSS забезпечує більш стійку безпеку передачі даних, але сам процес не стійкий, так як при передачі використовують метод послідовності Баркера через що, сигнал частково втрачається. Незважаючи на втрату сигналу, більшість даних в будь якому випадку надійдуть, так як сигнал буде відновлений. При роботі даний метод розмежовує діапазон в 2.4 ГГц на 14 каналів перекриваючих друг друга, максимально можлива кількість використання каналів в одному місці 3, але для становлення такої кількості каналів, необхідно щоб вони не перекривали один одного, та на 25 МГц відставали один від іншого, щоб не створювати взаємозалежні перешкоди. При передачі даних, кожен біт становиться 11 бітним носієм інформації, такий тип передачі отримав назву «Послідовність Баркера», який захищає дані від сторонніх впливів.

2.1.1 Розширений стандарт IEEE 802.11b

Вирішення проблеми швидкості передачі даних стандарту IEEE 802.11 слугувало необхідністю створення нового підтипу IEEE 802.11b. Вдосконаленій стандарт отримав прискорену передачу інформації близько 11Мбіт/с, однак в дійсності швидкість передачі була значно меншою. Головною проблематикою встала відмова від протоколу CSMA-CA, що встановила лімітовані рамки передачі даних за протоколом UDP та TCP (7.1 Мбіт/с та 5.9 Мбіт/с). Метод передачі даних DSSS постав єдиним вибором для створення умов при яких передача можлива на такій швидкості, що дає можливість синергічної взаємодії систем DSSS 802.11/802.11b. Використання методу FHSS 802.11 як і його взаємодія неможливі, так як даний метод має встановлені обмеження на швидкість передачі даних.

Робочий частотний діапазон стандарту IEEE 802.11b такий же як і в 802.11 становить 2.4 ГГц. Незважаючи на падіння швидкості при використанні певних протоколів, першоетапно передача даних можлива на чотирьох швидкостях (1 чи 2; 5.5; 11).

Використання швидкості 1 чи 2 Мбіт/с обумовлене типом передачі даних при використанні методу DSSS 802.11, головною особливістю якого є використання коду Баркера. Коротко описуючи використання коду Баркера, ми маємо побітовий потік даних, де кожен інформаційний біт стає 11 бітним носієм інформації, такий тип передачі слугує водночас захистом від сторонніх перешкод та захистом від зловмисників. Розглядаючи більш детальніше, то ми маємо біт даних довжиною в 11 інформаційних одиниць (1/0). Кожен біт даних змінюється послідовністю Баркера, де кожна 1 перетворюється на послідовність B1, а кожен нуль на інверсію B1 (B1=10110111000). Після, видозмінений сигнал шифрується шляхом використання BPSK (1 Мбіт/с) чи QPSK (2 Мбіт/с) фазових модуляцій.

Передача даних при 5.5 Мбіт/с та 11 Мбіт/с занадто відрізняється, так як при передачі використовують ССК тип кодування. Даний тип на відміну від 1 Мбіт/с чи 2 Мбіт/с які використовували 11 розрядний код, ССК використовує 8 чіповий код визначений 8 чи 4 біти на символ (табл. 2.2).

Таблиця 2.2 – Послідовність чіпів CCK

B2,B3	C1	C2	C3	C4	C5	C6	C7	C8
00	j	1	j	-1	j	1	-1	1
01	-j	-1	-j	1	j	1	-j	1
10	-j	1	-j	-1	-j	1	j	1
11	J	-1	J	1	-j	1	J	1

При передачі зі швидкістю 5.5 Мбіт/с, потік даних проходить етап групування бітів в символи. Кожен символ перетворюється в 4 біти B0, B1, B2, B3. В першому етапі біти B0, B1 залишаються не змінними, біти B3, B4 згідно таблиці 2 встановлюють послідовність 8 чіпів. Після встановлення послідовностей виконується 2-й етап - біти B0, B1 визначають можливе відхилення фази CCK при кодуванні (табл. 2.3).

Таблиця 2.3 – Відхилення фази CCK

B0,B1	Парні символи	Не парні символи
00	0	π
01	π/2	-π/2
11	π	0
10	-π/2	π/2

Передача даних на швидкості 11 Мбіт/с відбувається за тим же типом що й на швидкості 5.5 Мбіт/с з певними відмінностями:

– Біти групуються в символи по 8 бітів кожен;

– Кінцеві біти з B2-B7 обирають єдину послідовність розширення яка складається з 8 комплексних чіпів.

Система кодування CCK не єдина система яка підтримується стандартом IEEE 802.11b. PBCC (Packet Binary Convolutional Coding) кодування отримало більш розширений тип прихильників, так як на відміну від CCK, він не мав недоліку нестабільного розподілу символів через що при отриманні даних викликало помилки, в додаток за допомогою стиснення коду збільшувалась швидкість передачі даних до 22 Мбіт/с. Даний тип не був стандартизований тому потребував більш ретельного налагоджування.

Головною проблемою стандарту IEEE 802.11b постала передача даних в умовах великої кількості шумів, та передача на велику відстань, що й призвело до створення механізму автоматизованого переключення робочої швидкості.

Першочергово механізм встановлює найбільшу швидкість передачі за максимально можливих умов стабільного зв'язку, але при віддалені від епіцентру доступу чи при виниканню перешкод, система автоматично змінює швидкість передачі даних, за для стабілізації зв'язку.

2.1.2 Оновлений стандарт IEEE 802.11a

Реалізація стандарту IEEE 802.11b призвела до практично одночасного створення стандарту IEEE 802.11a працюючого в більш розширеному діапазоні частот, близько 5 ГГц, та суттєво більшою швидкістю передачі даних до 54 Мбіт/с.

В 1999 році відбулось встановлення нового стандарту, який повинен був вирішити більшість проблем основоположних стандартів, але цього не відбулося і лише в 2001 році стандарт отримав можливість реалізації.

Головною особливістю даного стандарту є можливість одночасних потоків передачі який в свою чергу збільшує швидкість передачі даних, на відміну від послідовної передачі використовуваної методами DSSS чи FHSS. Такий тип можливої передачі обумовлений використання оновленого типу модуляції сигналу OFDM (Orthogonal Frequency Division Multiplexing).

Робота методу мультиплексування по ортогональним частотам зіставлена в необхідності розділення на паралельно задіяні субпотоки, цілісного потоку даних. Кожен з утворених субпотоків має залежно низьку швидкість передачі даних, такий тип утворення допомагає захистити сигнал від перешкод при відносно великій пропускній здатності.

Після утворення виконується модуляція субпотоків з використанням відносно необхідної кількості несучих. Модуляція виконується в залежності від необхідності, 4 типами: BPSK, QPSK, QAM 16, QAM 64.

Стандарт IEEE 802.11a підтримує 8 різновидів швидкості передачі даних, з яких лише 3 обов'язкові. Характеристику різновидів швидкості передачі даних наведено в табл. 2.4 – 2.5.

Таблиця 2.4 – Обов'язкові швидкості передачі даних

Модуляція	Швидкість кодування	Мбіт/с	Кількість канальних біт за символ	Кількість біт за символ OFDM	Біти за символ згідно модуляції
BPSK	1/2	6	48	24	1
QPSK	1/2	12	96	48	2
QAM-16	1/2	24	192	96	4

Таблиця 2.5 – Додаткові швидкості передачі даних

Модуляція	Швидкість кодування	Мбіт/с	Кількість канальних біт за символ	Кількість біт за символ OFDM	Кількість заміни бітів за символ згідно модуляції
BPSK	3/4	9	48	36	1
QPSK	3/4	18	96	72	2
QAM-16	3/4	36	192	144	4
QAM-64	2/3	48	288	192	6
QAM-64	3/4	54	288	216	6

Класифікація робочого середовища стандарту 802.11a залежить від оптимальної потужності передачі. Робочий діапазон був розділений на 3 типи: нижній, середній та верхній діапазони.

Нижній діапазон працює при потужності до 100 мВт при заданій частоті від 5170 до 5330 Мгц.

Середній діапазон працює при потужності до 250 мВт при заданій частоті від 5470 до 5730 МГц.

Верхній діапазон працює при потужності до 1 Вт при заданій частоті від 5715 до 5832 МГц.

Не зважаючи на покращений тип захисту та можливу швидкість передачі даних, стандарт мав суттєві проблеми. Головною проблемою є максимальна робоча область в 100 метрів, яка в 3 рази менша за стандарти які працюють на

частоті 2.4 ГГц, та необхідність відносно великої потужності для елементів працюючих в заданій частоті.

2.1.3 Стандарт об’єднаної модуляції IEEE 802.11g

Стандарти з високим робочим діапазоном частот в 5 ГГц мають значно кращі характеристик на відміну від стандартів працюючих на частоті 2.4 ГГц, але ігнорувати значущі мінуси та збільшений ціновий діапазон неможливо. Незважаючи на все, обидва стандарти використовують в окремо поставлених задачах, але між собою взаємодія даних типів не можлива. Для вирішення даного питання був створений стандарт IEEE 802.11g. Стандарт IEEE 802.11g пропонує перенесення схеми модуляції OFDM із діапазону 5 ГГц в діапазон 2,4 ГГц із одночасним збереженням сумісності пристроїв стандарту 802.11b [2]. Неможливість встановлення зв’язку і отримання інформації першочергово значилась в використанні типу кодування, стандарт 802.11b використовує тип кодування ССК, а тип 802.11a використовує тип кодування OFDM. Якщо намагатися відправити данні на різній робочій частоті і в різних стилях кодування, то при отриманні виникне помилка даних з втратою пакета чи сигнал буде не помітним для приймачів.

Стандарт IEEE 802.11g отримав нову технологію модуляції, яка дозволила працювати в обох типах кодування водночас, та зберегли максимально можливу швидкість передачі до 54 Мбіт/с. Процес направлений на роботу з бітами вказано на рис. 2.3.

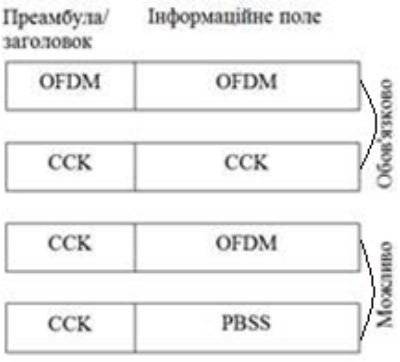

Рисунок 2.3 – Робота з бітами в різних типах кодування

Передача даних з використання даного методу кодування обумовлена взаємодією обох типів, кожний тип кодує окремий інформаційний базис, розбітовані данні кодуються з використанням OFDM методу, в той же час заголовок для ідентифікації пакетів кодується з використання CCK методу.

Такий тип кодування сповільнює процес передачі даних, так як першочергово отримується заголовок пакету даних, в якому вказаний час для передачі пакету, під час чого пристрої 802.11b мовчать, але кросплатформенна передача розширює можливості (табл. 2.6).

Таблиця 2.6 – Швидкість передачі даних при використанні певного типу кодування

Тип кодування		
Обов'язковий тип кодування	Мбіт/с	Додатковий тип кодування
Послідовність Баркера	1	
Послідовність Баркера	2	
CCK	5.5	PBCC
OFDM	6	CCK-OFDM
	9	OFDM/CCK-OFDM
CCK	11	PBCC
OFDM	12	CCK-OFDM
	18	OFDM/CCK-OFDM
	22	PBCC
OFDM	24	CCK-OFDM
	33	PBCC
	36	OFDM/CCK-OFDM
	48	OFDM/CCK-OFDM
	54	OFDM/CCK-OFDM

Окрім стандартних типі кодування, для стандарту 802.11g була ведена підтримка додаткового методу кодування PBCC (Packet Binary Convolutional Coding). Дане кодування широко використовувалось в стандарті IEEE 802.11b, тому для повноцінної роботи зі стандартом IEEE 802.11g, всі пристрої повинні мати 100% сумісність. Максимальна сумісність дасть можливість безперешкодної передачі даних, так як при роботі з різнотипними стандартами, обладнання стандарту 802.11b не може працювати більше чим 11 Мбіт/с, в той

час як обладнанню стандарту 802.11g необхідно працювати на відносно меншій швидкості передачі 11 Мбіт/с.

Швидкість передачі даних критично залежить від можливих перешкод, а максимально можлива швидкість рідкісне явище, досягти яке можливо лише на відкритому просторі без перешкод. Незважаючи на можливі перешкоди, швидкість передачі має діапазон змін, який виконується поступово без різких втрат швидкості.

2.1.4 Стандарт IEEE 802.11n

Розробка стандарту 802.11n почалась з 2002 року, головною задачею якого постала необхідність в максимальній швидкості передачі даних, без втрати пакетів. В 2009 році був представлений оновлений стандарт IEEE 802.11n, який на відміну від своїх попередників працював зі швидкістю передачі даних до 600 Мбіт/с та з можливістю роботи в двох діапазонах частот (2.4 ГГц та 5 ГГц).

Обладнання для можливості роботи з даним стандартом отримали доповнення в виді конфігурації MIMO (Multiple Input Multiple Output). Дана конфігурація визначала можливу кількість передавачів/приймачів (Антени) використовуваних в обладнані. В залежності від кількості антен, визначалась максимальна швидкість передачі даних до 150 Мбіт/с при використанні 1 антени. Мінімальна кількість встановлених антен 1x1, максимальна 4x4. Найбільшого поширення отримало обладнання 2x3 через відносно низьку ціну, гарний діапазон покриття і стабільно високу швидкість передачі даних.

Передача даних виконується по типу віддзеркалення, коли сигнал може прийматись під різним кутом, а під час передавання він відбивається від всіх поверхонь на шляху до кінцевої точки. В кінцеву точку в різні проміжки часу надходить зібрані відголоски сигналу, що дає змогу декодувати їх окремо.

Збільшення швидкості передачі даних призвело до необхідності збільшення ширини каналу з 20 МГц до 40 МГц. Обладнання стандарту 802.11n

може використовувати обидві ширини каналу в заданих частотах. Максимально можливі показники досягаються лише за використання 40 МГц ширини каналу при робочій частоті в 5 ГГц. При роботі на даній ширині каналу при частоті 2.4 ГГц в 19 активних каналів, можуть виникнути труднощі, так як обладнання підтримуючі стандарти 802.11b/g працюючі на тій же частоті, можуть залежно подавляти один одного, створюючи падіння продуктивності.

2.2 Стандартизовані типи захисту Wi-Fi

2.2.1 Основоположний тип захисту WEP

WEP (англ. Wired Equivalent Privacy) – найстаріший стандарт захисту бездротового трафіку, заснований на алгоритмі потокового шифрування RC4 (з використанням загального секретного ключа). Існують варіанти з довжиною ключа 64, 128 і 256 бітів [**Ошибка! Источник ссылки не найден.**]. Найбільш використовуваною були типи шифрування з довжиною ключа 64 та 128 бітів. Спочатку WEP задумувався як тип захисту на рівні дротових мереж, він слугував за для обмеження доступу користувачів та нагляду за трафіком, що давало можливість визначити шлях перехоплення та перегляду даних, але він мав значимі вразливості.

Так як бездротові мережі не мають фізичної структури на відміну від стандартних дротових мереж, а інформація передається через радіохвилі, то вона стає вразливою для зловмисників. Даний стандарт, після отримання інформації робив її не пізнаваною для системи шляхом шифрування, тільки авторизовані в мережі системи, могли безперешкодно зчитувати дані.

WEP надає можливість захисту від зловмисників які прослуховують лінії зв’язку, щоб знайти лінію відкритого доступу, але якщо система зловмисника налаштована на аналіз та пошук секретного ключа вибраної мережі, то далі все залежить від швидкості підбору ключа, та частоти зміни встановлених ключів.

Окрім шифрування, даний тип захисту так же забезпечував та перевіряв цілісність даних. Головною проблемою даного типу, стали ключі шифрування,

занадто проста їх реалізації, змусила створити та перейти на новий тип захисту WPA. При передачі даних, першоетапно вони кодуються з використанням секретного ключа і при отриманні даних, використовується один і той же ключ для їх декодування. Ширина ключа встановлюється 64 біта (швидкий тип в реалізації, але менш ефективний) або 128 біт (довший ти в реалізації, але більш ефективний). Ключі шифрування складені з 2 частин:

– Секретний ключ (присвоєний адміністратором);

– Вектор ініціалізації – (IV) Initialization Vector (внутрішня генерація).

Обидва ключі мають стандартно встановлений вектор ініціалізації коду в 24 біти, даний вектор допомагає в створенні різновидів однотипних ключів шифрування для різних пакетів, шляхом рандомної генерації частини ключа, що в свою чергу збільшу можливу варіацію ключів. Секретний ключ присвоюється напряму адміністратором в розмірі 40 та 104 біта, виходячи з цього ми маємо повноцінний розмір ключів (40+24=64/104+24=128). Першочерговою проблемою постала робота обладнання з різною шириною ключів, яка в майбутньому отримала підтримку змішаного кодування, але пакет даних зашифрований 128 бітною схемою був лише односторонньо сумісний з 64 бітною.

Шифрування стандарту WEP розділено на дві частини:

– Реалізація алгоритму CRC-32 (Cyclic Redundancy Check) за для встановлення ICV (Integrity Checksum Value), для можливості відстежування цілісності даних приймаючою стороною;

– Шифрування даних з використанням генератора випадкових чисел.

Шифрування генерує секретний двосторонній ключ на базі шифрування Вернама. Кожному пакету даних формується особистий ключовий потік. Зашифроване повідомлення (рис. 2.4) утворюється в результаті виконання операції XOR над незашифрованим повідомленням з ICV і ключовим потоком. Коли інформація приймається на іншій стороні, проводиться зворотний процес (p = c + b) [6].

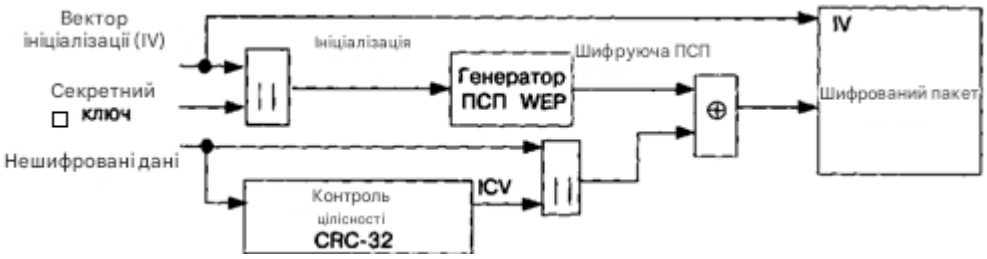

Рисунок 2.4 – Процес шифрування WEP

Шифрування з однотипними встановленими значеннями виконує циклічний процес для інших пакетів даних, тим самим змінюючи значення шифрування лише в вказаному діапазоні ініціалізації. Згідно специфікації шифрування RC4, при циклічному встановлення однакового значення коду та значення IV ми також отримуватимемо однакове значення b. Маючи два пакеті даних зашифровані загальним значенням b, ми зможемо використати виняткову диз'юнкція, тим самим отримавши процес використання виняткової диз'юнкції до нешифрованого тексту. Провівши даний процес, ми отримуємо нешифрований текст.

$$\begin{gathered} c_1 = p_1 + b \\ c_2 = p_2 + b \\ c_1 + c_2 = (p_1 + b) + (p_2 + b) = p_1 + p_2 \end{gathered} \tag{2.1}$$

Приймаючи той факт, що маючи 24 бітний вектор ініціалізації максимальна можливість не повторюваних значень зіставляє лише 16 777 216 (2^{24}). При максимальній кількості передачі даних, можна встановити що даний тип ініціалізації справить до колізії векторів. Час до початку циклу передач можливо визначити знаючи швидкість передачі даних, та середній розмір пакету даних. Знаючи що розмір пакету зіставляє 2000 байт то при швидкості передачі в 11 Мбіт/с ми маємо близько 688 пакетів передачі в секунду, за годину виходить 59 400 000 пакетів даних. Знаючи максимальну кількість варіантів, ми можемо визначити що через 18 хв відбудеться повторення циклу ($\frac{16\ 777\ 216}{59\ 400\ 000}$). Для максимально продуктивного використання даного типу захисту,

необхідно проводити регулярну зміну встановлених кодів шифрування, але є безліч інших типів атак від яких WEP не в змозі захистити.

На відміну від оновлених типів захисту, WEP був лише початковим стандартом шифрування інформації. Створений в 1997 р WEP захищав мережу до 2001 р, до першої позитивної спроби злому.

2.2.2 Покращена версія реалізації захисту WPA

WPA (англ. Wi-Fi Protected Access) – новий тип захисту бездротових мереж, зі встановленою розширеною системою захисту, даний тип змінив WEP в 2004 році. Заснований на TKIP (англ. Temporary Key Integrity Protocol – протокол тимчасової цілісності ключів), який ефективно бореться з проблемою, що лежить в основі вразливості WEP, – повторного використання ключів шифрування [2]. Першочергово, в 2003 році був випущений прототип WPA, який на той час мав якісніший тип шифрування використовувавший 128-бітні ключі, оновлений вектор ініціалізації та просту систему автентицікації.

В подальшому даний тип отримав оновлення в виді:

– WPA-Personal;

– WPA-Enterprise.

Режим WPA-Personal /WPA-PSK (Pre-Shared key) – тип доступу до своєї мережі, за допомогою єдиного ключа/пароля (рис. 2.5). Якщо виникне необхідність в зміні паролю, то доведеться ще раз пройти авторизацію та вводити пароль з кожного пристрою окремо. Даний пароль вказується для всіх користувачів, а після зберігається на кожному пристрої, що дає можливість користувачу самостійно продивитись пароль.

Рисунок 2.5 – Схема роботи PSK

Режим WPA-Enterprise (WPA-802.1x, RADIUS) – першочергово використання даного режиму можливо лише за однієї умови, якщо сервер RADIUS був підключений за для автентифікації пристроїв (рис. 2.6). Даний режим запитує облікові данні, при підключенні користувача до мережі, та генерує для кожного з них окремий пароль автентифікації.

Рисунок 2.6 – Схема роботи WPA-Enterprise

Оновлений тип автентифікації протоколу 802.1x забезпечив роботу на рівні порту, що знизило можливість несанкціонованого доступу. Під час проходження автентифікації, користувач може отримувати і відправляти запити тільки про статус особистого доступу і лише після надання доступу, користувач має право користуватися ресурсами.

Встановлення протоколу TKIP, дало можливість взаємодії з кожним пакетом даних окремо, та перевірку цілісності файлів. TKIP став оновленою версією протоколу RC4, використовуваного в WEP. Даний тип шифрування замість 24 бітної векторної ініціалізації, використовую 48 бітну. Використання оновленої ієрархії генерації коду, збільшила кількість максимально можливих варіантів більше ніж в 100 разів. Кодогенерація тепер реалізується побітово (окремо) і ні в якому разі не співпадає. Після шифрування даних виконується етап перевірки цілісності пакетів. Система MIC (Message Integrity Code) виконує порівняльну характеризацію даних при передачі і отриманні пакету з використанням математичних функцій. Якщо результат не відповідає першоетапній характеристиці, то такий пакет даних вважається заміненим і він скидається з потоку.

Окрім стандартного типу автентифікації, протокол WPA може працювати з протоколом EAP. Не дивлячись на те що протокол слугує автентифікацією в дротових мережах, WPA може працювати в його робочому середовищі. Головною відмінністю від базових типів перевірки, є необхідність в наявності помітки про право доступу у підключених користувачів. Система аналізу доступу встановлюється на RADIUS сервер, в якості БД слугує Active Directory.

Дані покращення вирішили питання, що до несанкціонованого доступу шляхом систем генерації коду, повторних запитів та заміни пакета даних.

2.2.3 Основоположник сучасного захисту WPA2

WPA2 (Wi-Fi Protected Access 2) – став ефективним оновленням, технології WPA. Деякий час WPA слугував як тимчасове рішення, що до підвищення захисту мережі. Використання оновленого типу шифрування порівняно покращило методологію захисту технології WEP, але все ще мало вразливості. В свою чергу після декількох невдач, був створений новий протокол захисту WPA2, який базується на алгоритмі шифрування AES (Advanced Encryption Standard) головного аспекту шифрування, методу CCMP-(CBC-MAC «Cipher block chaining message authentication code») (Counter Mod with CBC-MAC Protocol). Окрім використання AES стандарту шифрування, підтримується взаємодія з протоколом TKIP, для можливості роботи з обладнанням WPA. Використання даного типу не тільки шифрує данні, а також виконує перевірку на цілісність пакету даних.

WPA2 як і його попередник WPA працює в двох режимах:

– WPA2-Personal;

– WPA2-Enterprise.

WPA2-Personal генерує PSK ключ з розрядністю в 256 бітів. Ключ PSK, а також ідентифікатор SSID (Service Set Identifier) і довжина останнього разом утворюють математичний базис для формування головного парного ключа (Pairwise Master Key - PMK), який використовується для ініціалізації

чотиристороннього квітірования зв'язку та генерації тимчасового парного або сеансового ключа (Pairwise Transient Key - PTK), для взаємодії бездротового користувацького пристрою з точкою доступу [**Ошибка! Источник ссылки не найден.**]. Автентифікація встановлюється типово як в WPA-Personal, для всіх клієнтів доступний ключ, вказаний в налаштування AP. Практичне використання такого типу можливе в домашній чи офісній мережі, так як при найменшому витоку інформації, встановлений ключ необхідно змінити, а всім користувачам під'єднаним до AP, знову необхідно проходити автентифікацію.

WPA2 – Enterprise практичне використання типове з WPA – Enterprise (корпоративне). Даний тип вирішує проблеми з використанням статичних ключів, так як автентифікації проходить від AP до серверу RADIUS. Робочим базисом по автентифікації та контролю користувачів в WPA2 – Enterprise, виступає стандарт 802.1X. Кожен прилад який потребує авторизації, проходить перевірку сервером автентифікації (RADIUS). Користувачі які потребують доступу, але які його ще не отримали, можуть лише використовувати протокол EAPOL. Під час встановлення доступу, сервер надає згенерований ключ МК, окремо для даної сесії. Після встановлення автентифікації, користувачі можуть отримувати доступ до сервісів, лише через той порт комутатора до якого під'єднані (порт отримає позначку авторизований), якщо ж доступ не буде наданий порт отримає позначку «не авторизовано» а пропускати пакети можливо буде лише IEEE 802.1X.

Передача даних між декількома точками доступу, з проходження поетапної автентифікації може займати більше часу, чим робота напряму з'єднаного пристрою. Для отримання швидкого доступу WPA2 – Enterprise використовує можливості специфіки стандарту 802.11i:

– Отримання попереднього доступу (дає можливість проходити автентифікації, знаходячись в одній мережі, але до іншої AP);

– Збереження PMK в кеш пам'яті (уникає необхідності що разового проходження доступу 802.1X).

AES шифрування, постало основоположенням захисту стандарту WPA2. Даний стандарт шифрування потребує використанні апаратної підтримки, так як реалізація шифрування в зіставлена великим об'ємом даних. Протокол CBC-MAC (CCMP) реалізований з MIC (CTP) використовується для автентифікації, шифрування та реалізації цілісності пакету (MPDU/частини заголовку MPEU 802.11). Реалізація вектору ініціалізації шириною в 128 біт використовується для встановлення MIC. Після встановлення MIC, використовуючи AES та тимчасовий ключ для проведення етапу шифрування IV (128 біт). До отриманого результату та наступних 128 біт застосовується виняткова диз'юнкція (XOR). Встановлений результат знову піддаємо шифруванню (AES та TK), кінцеву варіацію (та наступних 128 біт) якого, знову реалізуємо з використанням виняткової диз'юнкції (XOR). Даний процесуальний тип має циклічне повторення до вичерпання максимальної корисності навантаження. Кінцеву відповідь якого реалізуємо для становлення значення MIC (використанню потребують лише перші 64 біти).

Другим етапом виконується шифрування встановленого значень MIC. Для шифрування використовується метод лічильника, при якому кожен відділ шифрованих даних отримує окремий лічильник. Як і при шифруванні вектора ініціалізації MIC, виконання цього алгоритму починається з попереднього завантаження 128-розрядного лічильника, де в поле лічильника замість значення, відповідного довжині даних, береться значення лічильника, встановлений на одиницю [10]. Далі використовується виключна диз'юнкція до кінцевого результату, шифрування перших 128 бітів за допомогою (AES і TK), після чого отримаємо зашифрований 128-розрядний блок даних. З використання AES і ключа, починається шифрування встановлених значень лічильника, які інкрементально збільшуються. Операцію «виключна диз'юнкція» застосовують до отриманого результату та наступних 128 бітів. Даний процесуальний тип має циклічне повторення до моменту зашифровки 128 блоків, після чого зарезервовані значення в полі лічильнику стануть нулем.

Знов виконується операція «виключна диз'юнкція» до результату шифрування лічильника та MIC, з використанням методу AES.

При використанні методу CBC-MAC, встановлене значення MIC та дані проходять етап шифрування.

Згідно рисунку 2.7, до вихідної інформації зашифрованих даних додається спереду заголовок 802.11, та нумерація пакета CCMP. В останньому блоці, встановлюється кінцеве значення 802.11.

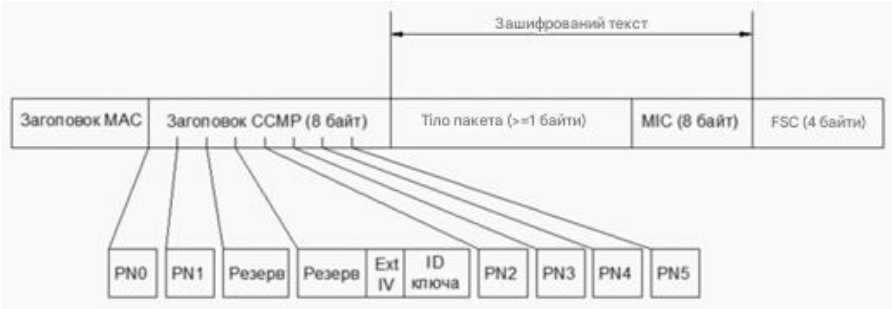

Рисунок 2.7 – CCMP MPDU формат

Процес декодування обернено пропорційний процесу шифрування. При надходженні даних, оберненою операцією встановлюється значення лічильника. Використовується алгоритм дешифровки значень лічильника та корисного навантаження на основі режиму лічильника та ТК. Після дешифрування отримуємо пакет даних, та MIC. За для розшифрування даних, першочергово необхідно підтвердити значення MIC. Використовуючи алгоритм CBC-MAC проводимо процес дешифрування. Отримані результати система звіряє на збіжність, якщо дані не схожі, пакет анулюють, а якщо дані ідентичні, тоді вони надходять до мережевого стеку, і лише потім потрапляють до клієнта.

Кодування та декодування реалізується згідно використовуваного типу захисту, порівняння даних типів наведено в табл. 2.7.

Таблиця 2.7 – Порівняльна характеристика базових стандартів захисту

Характеристика	WEP	WPA	WPA2
Ідентифікація	User-PC, WLAN карта	User-PC	User-PC
Автентифікація	Один ключ для всіх	EAP або один ключ для всіх	EAP або один ключ для всіх

Цілісність	32 бітний ICV	64бітний MIC	CBC-MAC,CRT на базі CCM
Шифрування	Однотипний ключ	PMK	CCMP (AES)
Розподіл ключів	Вручну	Типове PMK	Типове PMK
IV	24 біта	65 біт	48 бітний Номер пакета
Алгоритм	RC4	RC4	AES
Довжина ключів	64/128 біт	128 біт	До 256 біт
Інфраструктура	-	Можлива(RADIUS)	Можлива(RADIUS)

Оновлений тип захисту, давав надію розробникам на неприступність WPA2, однак захистившись від одного типу загроз, протокол став вразливий для інших. Найскладніший тип вразливості був названий KRACK (Key Reinstallation Attack). Головною ціллю для даного типу злому є чотирьох стороннє рукостискання. Рукостискання проводиться в момент коли прилади намагаються підключитись до мережі, а система намагається встановити коректність облікових даних (пароль), перед тим як надати доступ до ресурсів. Даний тип злому, надає можливість кіберзлочинцю встановлювати ключі шифрування, які вже використовувались системою. В момент активного рукостискання, створюється окремі ключі шифрування, для захисту подальшого потоку. Після зміни ключів, два nonces переходять в неактивний стан, що створює щілину в потоці даних. Встановлений ключ шифрування, надає можливість зчитування будь яких даних, той же тип використовується при заміні даних в пакетах чи пересилання.

WPA2 став захистом від більшості типів загроз, але ціле направлені загрози змогли найти шлях для взлому. Wi-Fi Alliance вирішили створи більш надійний та багатофункціональний тип захисту.

2.2.4 Багатофункціональний тип захисту WPA3

Оновлена версія стандарту, WPA3, була представлена в 2018 року компанією Wi-Fi Alliance. WPA3 останній метод безпеки, з оновленим стандартом захисту та стандартом автентифікації в мережі. Робота над

технологіями захисту, змусила Wi-Fi Alliance створити допоміжні протоколи Enhanced Open та Easy Connect, орієнтовані на окремі типи мереж. Кожен з них слугує, як допомога в вирішенні питань загроз окремих класифікацій, для окремих мереж.

Enhanced Open – протокол захисту відкритих мереж від пасивних атак. Більшість бездротових мереж встановлених для загального користування, майже не захищені. Дані які передаються по типовим мережам завжди в відкритому доступу, і будь який зловмисник шляхом банального фільтрування мережі, може збирати будь яку інформацію. Протокол Enhanced Open надає кращий тип захисту, шляхом оновленого гнучкого методу шифрування даних OWE (Opportunistic Wireless Encryption). Нажаль даний метод не надає додатковий тип захисту шляхом автентифікації, так як мережі відкритого типу призначені для відкритого доступу.

Easy Connect – протокол швидкого доступу до мережі. Велика частка мереж в особливості домашніх мереж, мають типові стандарти автентифікації. При необхідності підключення до такого типу мереж, великої кількості приладів, збільшиться час необхідний для отримання доступу до мережі. Рішенням стало використання QR кодів, як аналог введення паролю. Автентифікація виконується типовим обміном ключів і налаштування зв’язку.

WPA3, як і його попередники WPA2 та WPA, вийшов в 2 типах Personal і Enterprise. Personal – це типова мережа як використовує встановлений єдиний пароль для ідентифікації користувачів в мережі. Enterprise – корпоративна мережа, яка використовує типове рукостискання при встановлені автентифікації, але більш ширше шифрування від 192 біт на основі криптографічних протоколів (кривих). Для персональних мереж, можлива підтримка і 128 бітних ключів шифрування. Для підтримки захисту з використанням 192 бітного шифрування, було введення 384 бітний режим роботи з ключами, підтримку та роботу на основі 256 бітного шифрування, та автентифікаційні алгоритми (Elliptic Curve Digital Signature Algorithm та Elliptic Curve Diffie-Hellman exchange). Підвищення можливостей шифрування,

призвело до збільшення об’ємів даних в створенні ключів, та громіздкість робочого процесу, що потребує спеціалізованого обладнання.

WPA3 отримав значний прогрес в захисті мережі, як на етапі автентифікації так і на стадії шифрування. Реалізація KRACK атаки, було усунено при використанні методу автентифікації SAE. KRACK створюючи умову розриву зв’язку, він повторював типове з’єднання, щоб методом аналізу дізнатися пароль. SAE шляхом рівноправних запитів між AP та створення пароля на обох пристроях без подальшого повідомлення, обмежив можливості KRACK. Встановлений 192/256 бітний шифр, обмежує можливість систем підбору ключів, так як реалізувати пошук ключа при значенні в десятки мільйонів, майже неможливо.

WPA2 став першим типом захисту, який переробив максимально автентифікацію, поставивши безпеку доступу на один рівень з шифруванням даних. WPA3 вирішив покращити метод автентифікації PSK, новий тип аналізу доступу до мережі отримав назву «dragonfly handshake».

Одним з основних методів «dragonfly handshake» став новітній метод автентифікації SAE (рис. 2.8). Головною особливістю даного методу стала можливість створення ключа при кожному запиті в доступі та підтвердження доступу паролем PAKE. Даний метод називають рівноправним, так як всі прилади працюють на рівних правах і отримувати доступ та відправляти інформацію може будь який прилад в мережі, за регламентом ключів. Встановлення однорангового з’єднання, мінімізує шанси на заволодіння ключами. Якщо зловмиснику вдалось дізнатися один з ключів, то система все одно захищена, так як тимчасовий ключ не дасть йому можливості для дешифрування даних.

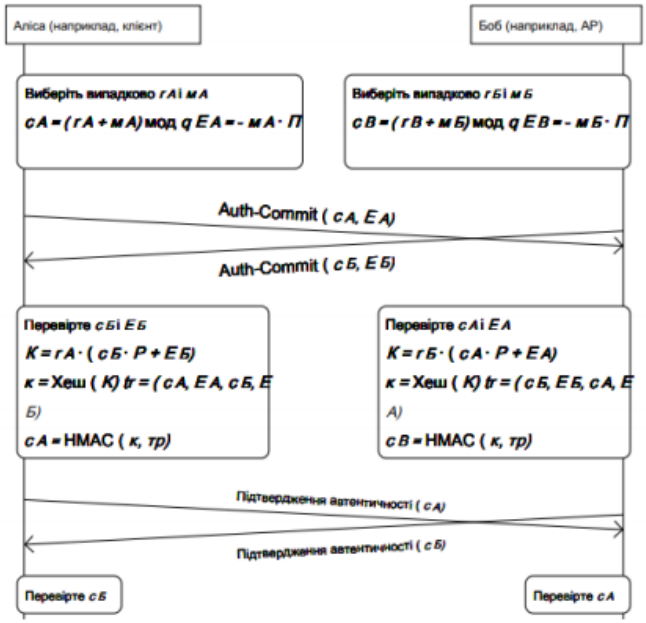

Рисунок 2.8 – Автентифікація SAE

На сьогодні WPA3 не отримав великої популярності, так як необхідність в обладнані підтримуючим WPA3, та реалізація сумісності з іншими типами, доки не можлива. Пройде не один рік, перед тим як WPA3 стане основоположення захисту мереж.

Висновки до розділу 2

В розділі було оглянуто основоположення стандартів 802.11 та типів систем захисту (WEP, WPA, WPA2, WPA3). Частотний розвиток мереж, зіставлений все більшим створенням портативних, повнофункціональних приладів, з підтримкою різновидів стандарт для мобільної роботи, з безперешкодним доступом до ресурсів. Створення стандартів мало цілеспрямований характер, та залежало від питань, на вирішення яких вони налаштовані. Першоетапні стандарти: 802.11, 802.11a, 802.11b створювались за типом покращення один одного.

Стандарт 802.11a збільшив діапазон робочих частот до 5 МГц та швидкість передачі даних до 54 Мбіт/с, але через велику енергозатратність та порівняно невеликий радіус дії, не отримав широкого практичного застосування.

Стандарт 802.11b навпаки, став широко використовуваним стандартом свого часу, працюючи на частоті в 2.4 МГц при швидкості до 11 Мбіт/с, енергозатратність була дуже низькою, а фактичний діапазон дії був в 2 рази більший.

Стандарти широкої робочої межи, такі як: 802.11g, 802.11n, мали можливість взаємодії в декількох діапазонах робочих частот, від використання яких залежала швидкість передачі даних, а також можливість передачі даних між обладнанням котрі підтримують різні стандарти.

Кожен з описаних стандартів отримав практичне застосування в тій чи іншій області, їх використання залежало лише від цілей встановлених при створенні мережі.

Щодо систем захисту, їх оновлення стало поетапною ієрархією один одного. Кожен з вказаних типів захисту вирішував вразливості попередника, та встановлював оновлені системи захисту. WEP використовуючи для автентифікації користувачів в мережі однотипний ключ, водночас для всіх, був занадто вразливий, так як довжина ключа давала можливість встановлення ключа шляхом підбору. WPA2 та WPA3 шляхом використання більш широкого типу ключа, та генерацією його лише при запиту доступу до мережі, мінімізували можливості підбору бібліотеками.

На сьогодні найбільш поширений тип захисту є WPA2, так як більшість обладнання підтримують його реалізацію. Не зважаючи на те, що WPA3 має покращені характеристик автентифікації з багатофункціональним аналізом цілісності даних, та оновленим типом шифрування, не змогла стати заміною. Реалізація WPA3 можлива лише при встановленому режимі WPA3, а так як більшість приладів підтримує тип захисту WPA2, то реалізація більш складного та дорожчого типу захисту, не має сенсу. В додаток WPA3 при роботі з приладами, котрі підтримують WPA2, працює в діапазоні його робочого рівня.

РОЗДІЛ 3
МЕХАНІЗМ РЕАЛІЗАЦІЇ ПОШУКУ ТА АНАЛІЗУ ВРАЗЛИВОСТЕЙ

3.1 Класифікація загроз на основі можливих вразливостей

Wi-Fi мережі сучасності, отримали низьку можливих системних стандартів для стабілізації робочого процесу, та оновлені системи захисту, працюючі в синергії згідно стандартам. При роботі в стандартизованій мережі, головною проблемою до сих пір лишається передача пакетів даних в області між кінцевими точками. Основоположні системи захисту по типу (WEP, WPA, WPA2, WPA3) мінімізували можливості доступу зловмисників до мережі, але систематизовані оновлення мережі зі зростаючою конкуренцією заданих можливостей, задають оновлений темп розширення можливих загроз, та збільшення систематизованих атак, зіставлених на основі бездротових мереж. Систематизовані атаки, мають характерний змістовний тип взаємодій в робочому середовищі, в залежності від вразливостей системи на яку направлена атака. Залежно від даного ефекту роботи, атаки класифікують за чотирма типами:

– авторизація частотних атак для доступа до мережі (DoS - атаки);

– перенаправлення трафіку та встановлення міжмережової точки доступу;

– взаємодія з системи захисту, атака з використання вразливостей шифрування;

– встановлення шумової антени, за для придушення потоку сигналу.

Головною проблемою серед даних типів, виступають DoS – атаки, та атаки перенаправлення трафіку, за допомогою встановлення між мережевої точки доступу. Дані типи загроз базуються на завантаженні мережевого трафіку, та направленні/прослуховуванні систематизованого потоку даних.

DoS атаки, чи атаки типу «відмови в обслуговуванні» націлені на завантаження мережі, що в сою чергу залежить від максимально можливої

пропускної здатності. Чим більша пропускна здатність зловмисника, тим більший діапазон дій та процесуальної загрузки може завдати зловмисник.

Даний тип атаки найбільш вживаний при необхідності несанкціонованого доступу до мережі, якщо системи захисту користувача роблять неможливим атаки інших типів, чи відмова в обслуговувані апаратного забезпечення слугує необхідністю в майбутній атаці. В таких умовах, навіть якщо системи захисту користувача не надали доступу до мережі, апаратне забезпечення як правило виходить з ладу, та потребує заміни чи повно етапного налаштування.

Якщо реалізація DoS – атаки стала причиною заміни апаратного забезпечення то можливість отримання доступу обмежується, так як потік даних припиняється, чи перенаправляється на інше обладнання. Коли системи після атак потребують додаткового налаштування, це дає можливість повторної чи атаки іншого типу.

Налаштування можливе трьома типами:

– налаштування в off-line (даний тип налаштування встановлює рамки для можливих атак, так як стає необхідність в фізичному контакту з обладнанням, для можливості отримання доступу, через те що потік даних припиняється на час обслуговування);

– налаштування з відстрочкою по часу (даний тип налаштування найбільш вразливий, так як навіть при закінченню атаки, система з некоректно налаштованим обладнанням продовжує працювати в стандартному режимі, а налаштування назначають на час найменшої робочої загрузки, згідно з кривими завантаженості трафіку. Налаштування з відстрочкою по часу, має необхідність в створенні файлу зі встановленими робочими командами, які проводять процес налаштування автоматизовано, що в свою чергу дає можливість заміни вказаних критеріїв налаштування, шляхом інших атак);

– налаштування в реальному часі (даний тип налаштування має найбільш поширену методологію використання. Реалізація можлива лише при використанні додаткового «Мобільного ПЗ/АЗ», котре тимчасово замінює процеси аналізу та моніторингу мережі, та встановлюють користувальницьку

систему придушення загроз. «Мобільне ПЗ/АЗ» постає по типу мережевого екрану (firewall), що дає змогу використання повторної DoS – атаки, але до тих пір поки адміністратор керуючий налаштування, не помітить, що пере направлений трафік постає не стандартним навантаженням на апаратне забезпечення, а зовнішнім аспектом завантаження мережі, та не призведе до обриву мережі з вихідного адресу, для типових пакетів даних).

Встановлені можливості реалізації атаки DoS, чи розмежованих атак DoS з різнотипних джерел (DDoS), характеризуються в залежності від типу атаки. Так як для можливості реалізації даних атак, необхідно мати максимально можливу потужність роботи машини (встановленої з одного персонального комп'ютера/використання об'єднаних машин в суцільне робоче середовище), згідно цього дана категорія атаки розподілена на два типи:

– надмірність запитів доступу;

– завантаження робочої пам'яті.

Перший вид атаки зіставлений типовою реалізацією автоматизованих пакетів даних, які намагаються пройти перший етап автентифікації. Велика кількість даних запитів призводить до навантаження системи, та її неможливості реалізувати кожний запит, що в свою чергу дасть можливість пропуску пакетів без перевірки (рис. 3.1).

Другий вид атаки спрямований на роботу з буферами пам'яті. При спробі обробити пакет даних, система виділяє частину фіксованої пам'яті на реалізації даного процесу, та в свою чергу запам'ятати дану дії на майбутнє. Активізація атаки змушує збільшувати можливу кількість робочих процесі, та збільшувати встановленій об'єм пам'яті. З зростанням заповнення пам'яті, система уповільнює роботу, виникає збій в автентифікації даних або відказує сервер, що відкриває доступ до робочого середовища.

На сьогодні широкоротого розповсюдження набули лише три типи даних атак:

– ICMP (даний тип атаки реалізований великою кількістю ICMP пакетів для можливості роботи DDoS загрози);

– UDP (дана атака обумовлена реалізацією великої кількості UDP пакетів, спрямованих на 7-й порт по типу echo запитів);

– HTTP/ping (дані атаки спрямовані на найпростіший доступ до середовища, шляхом збільшення кількості запитів).

Реалізовані загрози в мережі, можуть бути непомітні для деяких систем аналізу, так як вони фактично постають широким спектром обміну даними, для реалізації їх захисту був виділений поетапний механізм пошуку вразливостей, описаний в пункті 3.3.

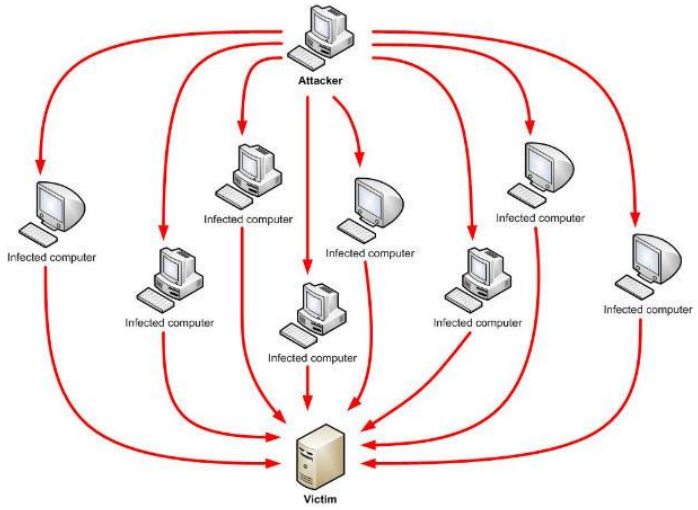

Рисунок 3.1 – Типова схема реалізації DoS/DDoS атак

Найпростіша та найбільш реалізована атака відкритих точок доступу, або домашніх мереж, постає атака пере направлення потоку даних. Відкриті точки доступу, як правило не мають першоетапної автентифікації, та працюють з використанням найпростішого типу шифрування, що в свою чергу дає можливість вільного огляду даних.

Реалізація даної атаки постає в встановленні антени працюючої на частоті приймача, антена встановлюється як підсилювач, в радіусі робочої області необхідної бездротової мережі. Відкрита точка доступу під’єднує зловмисника, навіть на великій дистанції, так як антена збільшує діапазон зв’язку в декілька разів, після чого зловмисник відправляє пакети даних з некоректно налаштованими характеристиками, за для підбору ключа шифрування, після

чого налаштовується на радіо сигнал і може його перехопити, та декодувати пакети.

Даний тип загрози тяжко виявити та прийняти міри до того, як система буде під загрозою. Використання віддаленої точки доступу, дає можливість безпечно проводити атаку, а в випадку спроби виявлення обмежити сигнал чи обірвати зовсім.

Атаки з використанням вразливостей шифрування, зіставлені з особливостями стандартизованих систем захисту (WEP, WPA, WPA2, WPA3) та більш детальніше розглянуті в розділі 2.

Загрози направленні на приглушення сигналу, та встановлення пере направлення потоку даних, зіставлене використанням прихованої точки доступу. В робочій області точки доступу, встановлюється антена працююча в певному діапазоні частот (встановлення даного діапазону можливе прослуховуванням та аналізом мережі).

Встановлена точка доступу генерує шум, який створює перебій в потоці даних, в цей же час активується прихована точка доступу, яка має назву та характеристики вже існуючої. В даній атаці система швидкісного підключення користувачів, яку обирають більшість людей при встановленні точки доступу, слугує головною проблемою, так як без запиту користувачів, прилади автоматично роблять підключення до відкритої точки доступу, з гарним сигналом. Після відновлення доступу, користувачам буде показано стандартизований інтерфейс який вони бачили при першому етапі підключення, до справжньої мережі, а далі надійде запит на повторне введення паролю. Вважаючи що точка доступу одна й таж, користувачі вводять пароль, а при отримані доступу паролю до справжньої мережі, налаштовується доступ через приховану точку доступу, до справжньої. Після чого зловмисник може прослуховувати та проглядати мережу перед відправкою і перед надходженням даних.

3.2 Системи пошуку та аналізу загроз

AirTight – найпростіша система аналізу мережі. Яка не потребує додаткового налаштування та реалізується в встановленій мережі.

Головною особливістю даної системи є постійний аналіз мережі на продуктивність. Система проводить моніторинг мережі, на наявність різнотипних видів загроз (DoS атаки, несанкціоноване з'єднання, встановлення точки доступу тощо). Якщо система підтвердила находження загрози, вона автоматично проводить процес блокування. Система реалізовує використання сенсорів AirTight C-75/60/55/50, навіть в вимкнутому режимі. Сенсори можуть використовуватись в режимі AP, при підтримці 1/2 радіоканалів. Підтримка стандарту 802.11ac.

Додаткові процеси системи:

– захист мобільних пристроїв;

– аналіз на рівні радіочастотного зашумлення, та виявлення перешкод;

– можливість сумісної роботи з платформами (McAfee ePo, Checkpoint, ArcSight тощо);

– встановлення місцезнаходження джерела перешкод;

– управління через фізичне підключення (VS чи Хмара);

– звіти про відповідність стандартам SOX, HIPAA, PCI DSS, DoD Directive 8100.2.

AirMagnet Enterprise – система аналізу мережі, в основі якої лежить функція тріангуляціїї. Система має підтримку стандарту 802.11ac. Використання покращеного методу пошуку вторгнень, збільшило діапазон захисту. Встановлений аналізатор радіочастот, шляхом прослуховування певних частот, виявляє перекриті канали 802.11 та усуває перешкоди. Складова системи зіставлена з консолі управління, сервера та сенсорів. Локалізація зловмисника методом тріангуляції, дає можливість знаходження встановлених бездротових приладів. Для реалізації даного методу, необхідно в систему

завантажити план поверху, на якому буде вказана інформація про встановлені сенсори та AP. Чим більше бездротовий прилад генерує трафіку, тим точніше буде встановлено місцеположення, при встановлених як мінімум 3 сенсорів. Тріангуляція окрім встановлення місцеположення, дозволяє обмежити з'єднання з корпоративною мережею. Система має гнучку побудову звітів, яка може складатися за різними стандартами.

AirMagnet Enterprise направлена на реалізацію виявлення трьох складніших в виявленні загроз:

– помилковий DHCP сервер;

– використання захищених утиліт злому;

– підроблені точки доступи, які виступають під видом корпоративних.

Waidps – консольна Python утиліта аналізу мережі та знаходження атак, на базі використання wireshark та пакету aircrack-ng. Waidps працює за типом знаходження аномалій в потоці, використання можливе й в домашніх умовах. Утиліта працює з типовою базою даних, в якій зберігається повно масштабно інформація з робочого середовища. Дану утиліту використовують, за для випередження можливого наступу WEP, WPA, WPS. Waidps визначає масову деаутентифікацію, так як це може слугувати атакою, з метою перехоплення хендшейку (рис. 3.2).

Рисунок 3.2 – Реалізація Waidps

На відміну від інших утиліті аналізу мережі, Waidps має автоматичне прослуховування ефіру, та підйому інтерфейсів за необхідністю.

Не зважаючи на широкий спектр вибору систем аналізу мереж, кожна з даних систем має власні типи захисту. Характеристика згідно оціночної продуктивності та загального використання, наведено в табл. 3.1.

Таблиця 3.1 – Порівняльна характеристика систем аналізу мережі

Назва	Система аналізу	Відповідність стандартам	Ціновий діапазон	Захист та пошук загроз	Просто реалізації системи	Сумарна кількість балів
AirTight	5	5	4	5	4	23
AirMagnet	4	7	2	6	3	22
Waidps	3	0	5	3	6	17

3.3 Поетапний аналіз захисту від атак на відмову

В основоположенні будь якої системи захисту, встановлено 4 задачі при ініціалізації загрози. Кожна з можливих загроз, обернено пропорційна встановленим задачам при проходженні етапів атаки, за для реалізації несанкціонованого доступу. Перша з встановлених задач при реалізації загрози постає «Попередження атаки». Кожна система, прилад в мережі чи обслуговуюче обладнання повинно бути готовим ідентифікувати загрозу ще до стадії встановлення зв’язку. Якщо система не виявила першочергову загрозу і зловмисник став частиною мережі, то нам необхідно дізнатися класифікацію реалізованого нападу, та на що він орієнтований. В залежності від встановлення типу загрози, будуть використовуватись ті чи інші типи захисту. Після того, як система ідентифікувала загрозу, проводиться етап пошуку джерела атаки. Даний етап найскладніший в реалізації, так як частіше за все, злочинці шифрують канали зв’язку, чи віддзеркалюють трафік по декільком АР. Кінцева задача постає в протидії загрозам.

Попередження атаки, постає в запобіганні надходження до системи можливої загрози. В загалом, ідентифікація загроз на даному етапі, як правило

виражена типовим прослуховування мережі, та аналізу трафіку. Частіше за все, при атаці можливо спостерігати заміну пакету даних, та встановлення іншої адреси джерела. Такий тип пасивної атаки виконується в двох випадках:

– прослуховування мережі, за для отримання доступу до конкретного пакету даних;

– реалізація масштабного навантаження мережі, шляхом циклічного надсилання запиту до мережі.

Наступною нашою дією, постає необхідність «Виявлення атаки». Головною характеризацію систем захисту є, максимальна можливість ідентифікації та усунення загроз, тому даний етап потребує уваги. Встановлення типу атак, надає можливість зрозуміти чи зможе існуючий метод захисту протистояти певній загрозі, чи потрібно ручне налаштування захисту. Реалізація даного типу загроз, супроводжується використанням підроблених пакетів даних, що при великій завантаженості трафіку, створює похибку в аналізі пакету, та система помилково може прийняти даний пакет. Такий тип атаки потребує багато часу для встановлення доступу, що дає Адміністратору можливість скинути весь трафік, до того як система відкаже, щоб розгрузити лінію та почати заздалегідь роботу по ідентифікації джерел. Так як система на даному етапі має можливість похибки, то для більш точного аналізу пакетів використовується трьох етапний механізм роботи с пакетами. Перший етап заснований на аналізу перенавантаженого потоку, так як система може бути перенавантажена великою кількістю пакетів даних, а не тільки фальшивими пакетами. Якщо завантажений трафік досягає певної величини, то система вважає що це атака. Другий тип, це виявлення особливостей, тобто пошук характеристик які не встановлюються для звичайного трафіку. Кінцевий варіант «Виявлення аномалій», даний тип створює макет коректного робочого середовища, та проводить асоціативний аналіз.

Ідентифікація джерела атаки надає можливість визначення вектору атаки. В даному типі загрози, при атаці на мережу, адреси джерел пакетів даних автоматично замінюються, що робить неможливим ідентифікувати їх.

Ідентифікувати джерела через АР неможливо, так як використання динамічної маршрутизації, вказує лише наступний шлях передачі. Використання спеціалізованих утиліт дадуть можливість ідентифікації джерел.

Для мінімізації пошкоджень роботи мережі, система захисту згідно класифікації атакуючого трафіку, застосовує одну з чотирьох основоположних методологій захисту мережі від DoS атак:

– перший етап, полягає в встановлені серверу з особливістю кешування даних (запитів). Як правило встановлення сервера повинно бути обумовлене швидким розгортуванням, та простотою в використанні, тому підтримка Nginx серверів з класовою ієрархією проксі-серверів стає найкращим вибором. Таким чином використання даного серверу, зможе мінімізувати кількість однотипних записів, та регулювати велику кількість пакетів;

– другий етап полягає в вирішенні питанні exo запитів. Систематизовані exo запити використовують UDP пакети для реалізації атаки, таким чином при обмеженні можливих з'єднань на сервері, та відкидання UDP сервісів, мінімізує будь яку можливість надходження пакетів даного типу;

– третій тип використовується при виявленні exo запитів ICMP пакетів. Такий тип атаки ускладнює роботу мережі, якщо вона має велику комп'ютерну базу, так як запити налаштовують на автоматизоване копіювання та цілenаправлене розсилання. При відключенні обробки та відповіді ICMP exo запитів в системі, автоматично система почне ігнорувати запити даного типу, що в свою чергу розвантажить мережу, та надасть можливі швидкого вирішення наслідків першочергових атак;

– четвертий етап заснований на усунення SYN загрози, направленої на роботу з протоколом TPC. Дана загроза заснована на відмові або збільшенні кількості очікуваних SYN+ACK (Synchronize + Acknowledge) підключень. Коли зловмисник подає запит на сервер для встановлення з'єднання, система відправляє запит на який повинен отримати відповідь, але відповідь не надходить, а запит на підключення деякий час залишається в пам'ятці. Таким чином система при збільшенні запитів, не дає можливість іншим користувача

отримати доступ до робочого середовища. Рішення постає в необхідності обмеження, а то й відключенні черги на очікування запиту «напіввідкритих з'єднань», що дає можливість системам аналізу мережі автоматично відхиляти дані пакети без перевірки.

DoS атаки несуть в собі громіздкий характер реалізації загрози, та швидкодіючу та значущу шкоду, безпосередньо для апаратної складової. Так як і серверні мережі, так і домашні мережі не завжди здатні забезпечити захист згідно чотирьох етапної класифікації, тому для цього постають додаткові можливості захисту:

– головним етапом є покращення системного приладдя та максимально можливих споживчих ресурсів, так як дані атаки мають велику залежність від пропускної здатності;

– використання систем аналізу мережі вказаних в пункті 3.2, та можливість використання «Мобільного ПЗ/АЗ»;

– кінцевий тип захисту має найменший показник надійності, але його використання є невід'ємною частиною захисту, налаштувати брандмауер.

3.4 Firewall (міжмережеві екрани) та методи покращення захисту мережі

Firewall (міжмережевий екран) також названий фільтром – це сукупність програмних/апаратних засобів, встановлений для контролю та фільтрування пакетів даних, які надходять. Пакети даних які надходять до між мережевого екрану, проходять етап фільтрування, який зрівнює їх з вже заданими даними в конфігурації, якщо пакет має відмінності, то його не пропускають. Такий тип фільтрування забезпечує мережу від несанкціонованого доступу. Firewalls не мають строгого розділення по класам, але їх класифікують залежно від реалізації за моделлю OSI:

– шлюзи сенсорного рівня;

– пакетні фільтри;

– посередники прикладного рівня;

– інспектори стану.

Проблемою Firewalls постає неможливість вплинути на внутрішній захист, реалізація фільтрування використовується тільки для пакетів ззовні. Єдиною можливістю встановлення захисту, це не дати зовнішнім порушникам отримати внутрішні данні, але на внутрішню передачу пакетів, вплинути неможливо.

Останнє покоління Firewalls (NGFW – Next Generation Firewall), надало можливість реалізації додаткових типів захисту, аналізу, перевірки цілісності пакетів, аналізу трафіку на рівні додатків, за для уникнення несанкціонованого доступу. Багатофункціональний тип Firewalls NGFW, надав можливості повномасштабного захисту мереж, але завантаженість великою кількістю процесів привело до неузгодження процесів між собою, створення затримок в процесах захисту та складному налаштуванню.

Типові міжмережеві екрани здатні захищати мережу від зовнішніх загроз, але можливості реалізації атак, також можуть надходити з середини. Сьогодні більшість периферійних пристрої оснащені додатковими схемами, та власною пам’яттю, які можуть слугувати носіями вірусних програм. Активізація пам’яті, та реалізація загрози відбувається при спробі налаштування периферії, до цього система не вважає периферійні пристрої за носії інформації. Такий тип загрози називають периферійними шпигунами. Системи аналізу та знаходження загроз працюють по типу антивірусів, що ускладнює можливість виявлення периферійних шпигунів, так як периферія починає працювати як внутрішній пристрій, та потребує специфікаційних утиліт для повного функціоналу роботи, що може встановлювати чи передавати загрозу в обхід систем аналізу. Також периферія може містити всередині запрограмовані дії, спеціалізовані на різнотипні випадки, системи аналізу при знаходженні такого процесу, може вважати його вірусом, так як дані дії не продиктований системою, а керуємі пристроєм. Саме через такі типи загроз широко використання набули не системні утиліти, а окремі методи та алгоритми сканування.

Головним типом швидкісного та ефективнішого методу пошуку даних шпигунів постає «Евристичні алгоритми». Робота даного алгоритму зіставлена типовим аналізом та пінгуванням прямих дій периферії, таким чином будь яка дія периферії аналізується методом та зіставляється з можливими діями. Незважаючи на корисність даних методів, вони занадто не точно, так як більшість виділених методом ризиків постає лише додатковими запрограмованими діями, які не є вірусами. Головною програмою яка використовує даний метод пошуку та аналізу загроз постає PuntoSwitcher, та програми на базі словника аналізу дій Lingvo.

Зокрема робочого середовища периферії, є окремо виділені типи функцій, які можуть бути запрограмованими діями, а також виступати як вірусна атака. Функції по типу WindowsHook або Get…State, вони являються головною ціллю периферійних загроз, але так як і методологія евристичних алгоритмів, робочий базис по заданим функціям може бути встановлений системою і їх виклик, помилково може вважатися вірусною атакою.

Систематизовані атаки на мережу, з кожним днем стають все більш простими в реалізації, що в свою чергу дає безперешкодну можливість простим користувачам реалізовувати загрози. Кожен з користувачів при створенні власної мережі, чи приєднанні до іншої не задумується про можливість загрози, так як вважає що захист надає мережеве обладнання, стандартний пароль та основоположні типи шифрування, але це не так. Реалізація захисту в більшості випадків залежить від приладу та підтримуючого типу захисту, але це не дає вам 100% захисту, так як більшість місцевих точок доступу являються відкритого типу, а домашні мережі містять занадто слабке шифрування. Для реалізації більш щільного типу захисту власних мереж необхідно:

1. Першочергово мережа повинна бути скритою, так як більшість пристроїв налаштовані на автоматичне підключення до мережі і навіть при наявності паролю, система на етапі проходження автентифікації може запустити стандартизований список підбору ключів, що дасть зловмиснику доступ до мережі. Якщо мережа відкритого типу, то нажаль дане становлення

захисту неможливе.

2. Більш реалізованим типом захисту, постає надання особистого доступу користувачів, тобто налаштування MAC адреси. Налаштування MAC адреси дає можливість обмежування доступу до робочого середовища, шляхом вказування MAC адрес пристроїв, яким дозволений доступ до мережі, але при необхідності збільшення списку, потрібно буде вказати нові MAC адреси пристроїв в реєстр.

3. Кінцевим типом захисту постає вибір мережевого обладнання, та підтримувані ним стандарти та типи захисту. Найпоширенішими на сьогодні виступають точки доступу (Wi-Fi Router) з підтримкою WPA2 та WPA3 типів шифрування. Оновлені та збільшені ключі шифрування даних в мережі, ускладнюють процес реалізації перехоплення пакетів даних. WPA3 постає кращим вибором, завдяки новішому типу шифрування та підтримці роботи з різними середовищами, але він мало використовуваний та дорогий. WAP2 найбільш вживаний тип захисту в сучасних точках доступу, він працює на порівняльно високих швидкостях передачі даних, та має розширені ключі шифрування що забезпечує достойний захист.

Реалізація будь якого типу захисту, не дає сто відсоткового забезпечення від загроз, так як існує безліч новітніх атак, які на даний момент не стали популяризованими, та й не внесені в списки систем аналізу мереж.

Висновки до розділу 3

В даному розділу було оглянуто класифікації мережевих загроз, та атак. Розглянуто повноцінно схему реалізації, аналізу та механізм уникнення розповсюдженого типу атак на відмову (DoS). Встановлено чотирьох етапну систему передбачення загрози DoS. Розглянули типові системи аналізу мережі, AirTight та AirMagnet, створили порівняльну характеристику, на основі таблиці оцінювання. Провели огляд автоматизованої консольної утиліти Waidps на базі

wireshark. Робочий процес даної утиліти направлений на пошук та аналіз аномалій в потоці.

Розглянули роботу фільтру (мережевого екрану/firewall), перевірку даних фаєрвол реалізує лише при надходженні пакету, а на внутрішній обмін даними, він впливати не може. Новітній стандарт фаєрволу NGFW, надав широку можливість в захисті та аналізу мережі, але через значні мінуси, широкого використання він не набув.

Класифікації типів загроз залежать напряму від об’єкту на який направлена атака. Більшість систем аналізу та пошуку уразливостей, працюють та усувають максимально можливу кількість загроз. Деякі з типів захисту, можуть встановлювати локалізації АР зловмисника.

Подальші дослідження новітніх типів атак, оновлять характеристики захисту мережі, та нададуть системи з більш широкою можливістю ідентифікації загроз.

ВИСНОВКИ

В кваліфікаційній роботі були оновлені методи захисту домашньої мережі, та встановлені структуровані дії для адміністратора. Встановлено класифікацію можливих загроз, згідно вразливостей на які вони направлені. Було оглянуто базові класифікації мереж. Охарактеризовано можливості тих, чи інших мереж, виходячи з робочого середовища в якому вони використані. Відокремлено та розібрано головні типи стандартів IEEE 802.11a/b/n тощо. Відокремлено та пропрацьовано кожну вразливість та особливість, різних типів стандартів. Охарактеризовано кожний тип стандарту IEEE 802.11, згідно їх робочої діяльності.

Розглянуто класову характеризацію різних типів захисту (WEP, WPA, WPA2, WPA3). Проведено аналіз різновидів ключів шифрування, присутніх в кожному з класів захисту мережі. Розглянуто робочий процес шифрування пакетів даних, з використання ключів різної ширини.

Встановлена класифікація можливих атак на мережу, згідно вразливостей, на які направлені атаки. Розглянуто системи прослуховування та аналізу мережевого трафіку, для пошуку популярних загроз. Оглянуто механізм чотирьох етапного пошуку, та передбачення загроз направлених на відмову мережі. Встановлено етапи усунення загрози DoS/DDos атак.

Розглянуто процес взаємодії між мережевого екрану (Firewall), та реалізація його новітньої версії NGFW. Встановлено методи покращення захисту домашньої мережі, та методи усунення «Периферійних загроз».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що ж таке Wi-Fi і як працює ця бездротова мережа, де використовується Вай Фай, його стандарти і режими безпеки | Поширені запитання. URL: http://ipkey.com.ua/uk/faq/463-what-is-wi-fi.html (дата звернення: 30.05.2025);
2. WEP. Вікіпедія. URL: https://uk.wikipedia.org/wiki/WEP (дата звернення: 30.05.2025);
3. Wi-Fi Protected Access. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Wi-Fi_Protected_Access (дата звернення: 30.05.2025);
4. WWAN. Вікіпедія. URL: https://uk.wikipedia.org/wiki/WWAN (дата звернення: 30.05.2025);
5. Стандарт локальних мереж IEEE 802.11 Wi Fi. URL: https://beloshop.ru/uk/ethernet-standard-ieee-80211-wi-fi/ (дата звернення: 30.05.2025);
6. Технології Bluetooth. URL: https://wiki.cuspu.edu.ua/index.php/Технологія_Bluetooth (дата звернення: 30.05.2025);
7. ZigBee. Вікіпедія. URL: https://uk.wikipedia.org/wiki/ZigBee (дата звернення: 30.05.2025);
8. Market Guide for Intrusion Detection and Prevention Systems. URL: https://www.gartner.com/en/documents/3945589 (дата звернення: 30.05.2025);
9. WLAN (Wireless Local Area Network) Definition. URL: https://techterms.com/definition/wlan (дата звернення: 30.05.2025);
10. Практичні аспекти проведення тесту на проникнення. URL: http://www.osp.ru/text/233652/5908864/
11. Аналіз засобів захисту при використанні обладнання стандарту IEEE 802.11. Дніпровська Політехніка. 2018. №10. С. 41.
12. 802.11-2016 - IEEE Standard for Information technology-

Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications | IEEE Standard | IEEE Xplore. URL: https://ieeexplore.ieee.org/document/7786995/ (дата звернення: 30.05.2025);

13. Intrusion Detection System - IDS. URL: http://www2.icmm.ru/~masich/win/lexion/ids/ids.html (дата звернення: 30.05.2025);

14. Олейніков А. Н. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів. Харків: НТМТ, 2014. 298 с.

15. Mathy Vanhoef and Frank Piessens. Predicting, decrypting, and abusing wpa2/802.11 group keys. In 25th USENIX Security Symposium, USENIX Security 16, 2016. 673 c.

16. Georgia Weidman. Penetration testing A Hands-On Introduction to Hacking / Georgia Weidman // No Starch Press, 2014. С. 179 – 339.

17. DSSS - Direct Sequence Spread Spectrum - Telecom ABC. URL: http://www.telecomabc.com/d/dsss.html (дата звернення: 30.05.2025);

18. Стефінко Я.Я., Піскозуб А.З. Використання відкритих операційних систем для тестування на проникнення в навчальних цілях. Вісник Національного університету «Львівська політехніка» Комп’ютерні системи та мережі. 2014. № 806. С. 258-263.

19. Joseph Muniz. Web Penetration Testing with Kali Linux / Joseph Muniz, Aamir Lakhani // Packt Publishing, 2013. С. 114 – 234.