МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК* (ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-ПРОФЕСІЙНОГО СТУПЕНЯ ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Створення безпровідної мережі з підтримкою WPA3 з конфігурацією безпеки*

Група: *3-012* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти (підпис) *Кирило НЕВІНЧАНИЙ* (ім'я, ПРІЗВИЩЕ)

Керівник роботи (підпис) *Олександр МИТРОФАНОВ* (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки (підпис) *Оксана ОСАДЧА* (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітньо-професійний ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК* (ім'я, ПРІЗВИЩЕ)
« 10 » 03 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

НЕВІНЧАНОГО Кирила Віталійовича
(прізвище, ім'я, по батькові)

1.Тема роботи *Створення безпровідної мережі з підтримкою WPA3 з конфігурацією безпеки*

Керівник роботи *Митрофанов Олександр Вячеславович, доктор філософії*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* « *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з *01.03.2025* по *15.06.2025*

3. Вихідні дані до роботи *Мережа безпровідної передачі інформації Wi-Fi, технології IEEE 802.11, протоколи мережі WEP,WPA,WPA2, WPA3, атаки типу: підроблена точка доступу, атака KRACK*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Проаналізувати стандарти мереж бездротового доступу Wi-Fi. Розглянути принципи роботи Wi-Fi мережі. Провести аналіз на вразливість протоколу інформаційної безпеки WPA3-Enterprise. Проаналізувати можливі типи загроз і протоколи інформаційної безпеки, що борються з ними в мережах Wi-Fi.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Презентація Microsoft PowerPoint

6. Консультанти розділів роботи (проекту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання з керівником дипломної роботи*	*01.03.2025*	*виконано*
2	*Підбір та вивчення науково-технічної літератури за темою дипломної роботи*	*15.03.2025*	*виконано*
3	*Виконання 1 розділу аналіз сучасного стану безпроводових мереж та стандартів безпеки*	*28.04.2025*	*виконано*
4	*Виконання 2 розділу проектування безпровідної мережі*	*14.05.2025*	*виконано*
5	*Виконання 3 реалізація та конфігурація безпровідної мережі з підтримкою wpa3*	*26.05.2025*	*виконано*
6	*Підготовка матеріалів до презентації*	*30.05.2025*	*виконано*
7	*Написання та оформлення пояснювальної записки*	*06.06.2025*	*виконано*
8	*Захист дипломної роботи*		

Здобувач освіти _____ *Кирило НЕВІНЧАНИЙ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Олександр МИТРОФАНОВ*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 5/27/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Ukrainian national aviation university
Заголовок
Невінчаний Кваліфікаційна робота
Автор Науковий керівник / Експерт
НевінчанийКлименко С
підрозділ
Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

3.29% 3.29% КП 1

0.38% 0.38% КЦ

25
Довжина фрази для коефіцієнта подібності 2

9809
Кількість слів

73989
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		31
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		20

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Політика безпеки для промислового Інтернету речей та оцінка її дієвості [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	41 0.42 %
2	Система захисту бездротових мереж із використанням багатофакторної автентифікації [redacted] 12/12/2024 National University "Zaporizhzhia Polytechnic" (Кафедра "Комп'ютерні системи та мережі")	17 0.17 %

РЕФЕРАТ

Кваліфікаційна робота на тему «Створення безпроводової мережі з підтримкою WPA3 з конфігурацією безпеки» містить 56 сторінок, 8 рисунків, 5 таблиць та 35 використаних джерел.

WI-FI 6, WPA3, БЕЗДРОТОВА МЕРЕЖА, МЕРЕЖНА БЕЗПЕКА, SAE, WPA3-PERSONAL, WPA3-ENTERPRISE, VLAN, SITE SURVEY, RADIUS

Кваліфікаційна робота присвячена дослідженню та реалізації сучасної бездротової мережевої інфраструктури з підвищеним рівнем захисту. У роботі розглянуто еволюцію технологій бездротового зв'язку, зокрема розвиток стандартів Wi-Fi (802.11a/b/g/n/ac/ax), та їхні технічні особливості. Особлива увага приділена питанням безпеки, зокрема аналізу стандартів WEP, WPA, WPA2 і впровадженню новітнього протоколу WPA3, що забезпечує високий рівень криптографічного захисту, автентифікацію за допомогою SAE (Simultaneous Authentication of Equals) та 192-бітне шифрування у корпоративному режимі. Практична частина роботи зосереджена на проектуванні безпроводової мережі: визначено вимоги до покриття, кількості користувачів, типів трафіку, проведено Site Survey, обрано топологію на основі контролера, підібрано обладнання з підтримкою WPA3 (зокрема точки доступу Wi-Fi 6, контролер, PoE комутатори, маршрутизатор), розроблено логічну структуру VLAN та IP адресацію. Реалізація передбачала налаштування мережевого обладнання, конфігурацію параметрів безпеки WPA3, ізоляцію трафіку та впровадження централізованої автентифікації на базі RADIUS-сервера.

У результаті реалізовано надійну, масштабовану, продуктивну та безпечну бездротову мережу, яка відповідає сучасним вимогам безпеки для корпоративного середовища.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AP – Access point;

WPA – Wi-Fi Protected Access;

WPA2 (WiFi Protected Access 2);

WPA3 (WiFi Protected Access 3);

PSK – Pre-shared key;

SAE – Simultaneous Authentication of Equals;

EAP-PWD – Extensible authentication protocol;

WLAN (Wireless Local Area Network) – бездротова локальна мережа; KRACK - Key Reinstallation Attack БМПІ – безпровідні мережі передачі інформації ТД – точка доступу;

Атака – певна послідовність дій, які, в разі успіху, призведуть до порушення безпеки інформації. Також атака –реалізація певної загрози; Загроза – подія, яка може спричинити порушення політики безпеки інформації або нанесення збитків інформаційно-комунікаційній системі; Зловмисник – фізична особа, яка умисно порушує політику безпеки; Wi-Fi (англ.Wireless Fidelity) – високоточні бездротові технології передачі даних, які представляють собою набір стандартів передачі цифрових потоків даних по радіоканалам;

ВСТУП

Стрімкий розвиток інформаційних технологій значно підвищив попит на надійні, високошвидкісні та безпечні безпроводові мережі. Мережі Wi-Fi, засновані на стандартах IEEE 802.11, стали основою сучасної комунікаційної інфраструктури, забезпечуючи безперебійне підключення для широкого спектра пристроїв у приватних і корпоративних середовищах. Однак зростання залежності від безпроводових мереж також підкреслило важливість надійних заходів безпеки для захисту конфіденційних даних від кіберзагроз. Впровадження стандарту WPA3 (Wi-Fi Protected Access 3) у 2018 році стало значним кроком вперед у сфері безпеки безпроводових мереж, пропонуючи покращений захист від атак, вдосконалені механізми аутентифікації та підтримку потужнішого шифрування, зокрема 192-бітного криптографічного набору для корпоративних мереж.

Ця кваліфікаційна робота спрямована на проектування та впровадження безпроводової мережі з підтримкою WPA3, зосереджуючись на налаштуванні параметрів безпеки відповідно до сучасних вимог кібербезпеки. Дослідження мотивоване необхідністю усунення вразливостей попередніх протоколів безпеки (WEP, WPA, WPA2) та використання можливостей WPA3 для забезпечення безпечної та ефективної роботи мережі. Завдання включають аналіз еволюції стандартів Wi-Fi та протоколів безпеки, визначення вимог до мережі, вибір відповідної топології та обладнання, планування розміщення точок доступу, налаштування безпеки WPA3 та інтеграцію безпроводової мережі з існуючою дротовою інфраструктурою. Робота структурована у три основні розділи: перший аналізує стан безпроводових технологій і стандартів безпеки, другий деталізує процес проектування мережі, а третій описує практичну реалізацію та конфігурацію. Результати роботи надають вичерпний посібник для створення безпечної,

масштабованої та високопродуктивної безпроводової мережі, придатної для корпоративних середовищ.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНОГО СТАНУ БЕЗПРОВОДОВИХ МЕРЕЖ ТА СТАНДАРТІВ БЕЗПЕКИ

1.1 Огляд технологій безпроводових мереж

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням кількості пристроїв, що потребують підключення до мережі Інтернет. Безпроводові мережі, завдяки своїй гнучкості та зручності, відіграють ключову роль у забезпеченні доступу до інформаційних ресурсів як у приватній, так і в корпоративній сферах. Проте, разом зі зростанням популярності безпроводових технологій зростає і важливість забезпечення їхньої безпеки.

Безпроводові мережі, зокрема Wi-Fi, є ключовим елементом сучасної інформаційної інфраструктури, забезпечуючи зручність, мобільність і гнучкість у передачі даних. Технології Wi-Fi базуються на стандартах IEEE 802.11, які еволюціонували протягом останніх десятиліть, щоб відповідати зростаючим вимогам до швидкості, пропускної здатності та енергоефективності. Нижче розглянуто основні стандарти Wi-Fi (802.11a/b/g/n/ac/ax) та їхні характеристики.

Стандарт 802.11, затверджений у 1997 році. Це перший стандарт Wi-Fi, що забезпечував максимальну швидкість передачі даних до 2 Мбіт/с у діапазоні 2.4 ГГц з використанням методів модуляції FHSS (Frequency-Hopping Spread Spectrum) та DSSS (Direct-Sequence Spread Spectrum). Через низьку швидкість та ряд технічних обмежень цей стандарт сьогодні практично не використовується.

Стандарт IEEE 802.11b було представлено у 1999. Значне покращення першого стандарту, що дозволило досягти максимальної швидкості передачі даних до 11 Мбіт/с у тому ж діапазоні 2.4 ГГц. 802.11b став першим комерційно успішним стандартом Wi-Fi завдяки відносно високій швидкості та низькій вартості обладнання. Проте, робота в перевантаженому діапазоні 2.4 ГГц часто призводила до інтерференції з іншими безпроводовими пристроями.

Паралельно з 802.11b у 1999 році було представлено стандарт 802.11a, який

використовував діапазон 5 ГГц та метод модуляції OFDM (Orthogonal Frequency-

Division Multiplexing). Це дозволило досягти максимальної швидкості передачі даних до 54 Мбіт/с. Перевагами 802.11a були вища швидкість та менша схильність до інтерференції порівняно з 2.4 ГГц діапазоном. Проте, обладнання 802.11a було дорожчим, а дальність зв'язку – меншою через вищу частоту.

Стандарт 802.11g, затверджений у 2003 році, поєднав у собі переваги 802.11b (робота в діапазоні 2.4 ГГц) та 802.11a (використання модуляції OFDM). 802.11g забезпечував максимальну швидкість передачі даних до 54 Мбіт/с, зберігаючи при цьому сумісність з обладнанням 802.11b. Завдяки цьому 802.11g став дуже популярним і протягом тривалого часу був основним стандартом Wi-Fi.

Затверджений у 2009 році стандарт 802.11n, отримав значний крок вперед у розвитку Wi-Fi технологій. 802.11n підтримував роботу як у діапазоні 2.4 ГГц, так і в 5 ГГц, використовував технологію MIMO (Multiple-Input Multiple-Output), що дозволило одночасно передавати та приймати кілька потоків даних, та збільшив ширину каналу до 40 МГц. Максимальна теоретична швидкість передачі даних для 802.11n становила 600 Мбіт/с (за умови використання чотирьох просторових потоків та ширини каналу 40 МГц). На практиці швидкість зазвичай була нижчою, але значно перевищувала попередні стандарти.

Стандарт 802.11ac, представлений у 2013 році, був розроблений для роботи виключно в діапазоні 5 ГГц та забезпечував значне збільшення швидкості передачі даних за рахунок використання ширших каналів (до 160 МГц), більшої кількості просторових потоків (до восьми) та вищої щільності модуляції (256-QAM). Теоретична максимальна швидкість передачі даних для 802.11ac могла сягати кількох гігабіт на секунду. 802.11ac став основним стандартом для високошвидкісних безпроводових мереж, забезпечуючи комфортну роботу з мультимедійним контентом, потоковим відео високої роздільної здатності та іншими вимогливими до пропускної здатності додатками.

Стандарт 802.11ax, відомий як Wi-Fi 6, був затверджений у 2019 році. Це останнє покоління Wi-Fi стандартів, спрямоване не лише на подальше збільшення швидкості передачі даних (теоретично до 9.6 Гбіт/с), але й на підвищення ефективності роботи мережі в умовах високої щільності клієнтських пристроїв.

Ключовими технологіями 802.11ax є OFDMA (Orthogonal Frequency-Division Multiple Access), яка дозволяє одночасно передавати дані кільком клієнтам в межах одного каналу, Target Wake Time (TWT), що оптимізує енергоспоживання мобільних пристроїв, та покращена схема модуляції 1024-QAM. 802.11ax підтримує роботу як у діапазонах 2.4 ГГц, так і 5 ГГц, забезпечуючи кращу продуктивність та стабільність з'єднання, особливо в завантажених безпроводових середовищах.

Для наочного порівняння основних характеристик розглянутих стандартів Wi Fi наведемо таблицю 1.1.

Таблиця 1.1 – Порівняння основних стандартів Wi-Fi

Стандарт	Рік випуску	Діапазон частот	Максимальна швидкість	Основні технології	Основні переваги
802.11	1997	2.4 ГГц	2 Мбіт/с	FHSS, DSSS	Перший стандарт
802.11b	1999	2.4 ГГц	11 Мбіт/с	DSSS	Широка сумісність, низька вартість
802.11a	1999	5 ГГц	54 Мбіт/с	OFDM	Вища швидкість, менша інтерференція
802.11g	2003	2.4 ГГц	54 Мбіт/с	OFDM	Висока швидкість, сумісність з 802.11b
802.11n	2009	2.4/5 ГГц	До 600 Мбіт/с	MIMO, 40 МГц канали	Значне збільшення швидкості та дальності
802.11ac	2013	5 ГГц	До кількох Гбіт/с	Ширші канали (до 160 МГц), MIMO, 256-QAM	Дуже висока швидкість передачі даних
802.11ax (Wi-Fi 6)	2019	2.4/5 ГГц	До 9.6 Гбіт/с	OFDMA, MU MIMO, 1024-QAM, TWT	Висока ефективність в завантажених мережах, економія енергії

Еволюція стандартів Wi-Fi відображає постійне прагнення до підвищення продуктивності та ефективності безпроводових мереж. Кожен новий стандарт вносив значні поліпшення, розширюючи можливості використання безпроводових

технологій у різноманітних сферах.

На рисунку 1.1 наглядно відображена еволюція стандартів Wi-Fi, починаючи з 1997 по 2019 роки.

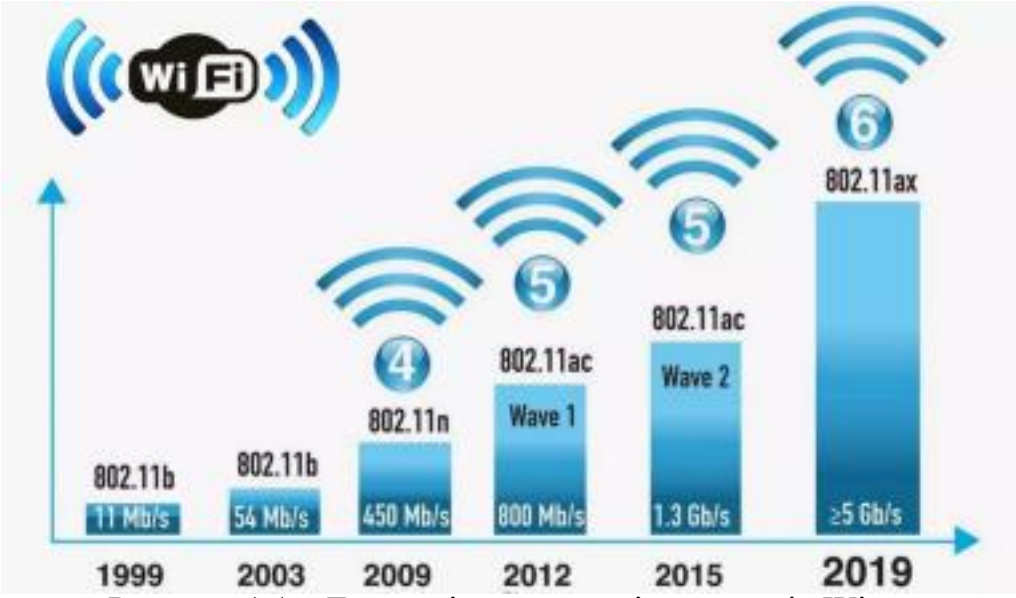

Рисунок 1.1 – Еволюція швидкості стандартів Wi-Fi

1.2 Еволюція стандартів безпеки безпроводових мереж (WEP, WPA, WPA2)

Разом з розвитком технологій безпроводових мереж еволюціонували і стандарти їхньої безпеки. Перші реалізації Wi-Fi мали серйозні вразливості, що робило безпроводові мережі легкою мішенню для атак. Безпека є критично важливою для безпроводових мереж, оскільки радіосигнали можуть бути перехоплені зловмисниками. За останні два десятиліття стандарти безпеки Wi-Fi еволюціонували від WEP до WPA3, кожна з яких вирішувала недоліки попередньої.

WEP (Wired Equivalent Privacy) представлений у 1999 році, був першим стандартом шифрування, вбудований у протокол IEEE 802.11. WEP використовував алгоритм потокового шифру RC4 з ключем довжиною 40 або 104 біти (плюс 24-бітний вектор ініціалізації – IV). Початково WEP мав забезпечити конфіденційність безпроводового зв'язку, еквівалентну захищеності дротових мереж. Однак, вже незабаром були виявлені серйозні вразливості в алгоритмі RC4 та способі використання IV. Зокрема, повторне використання IV призводило до можливості відновлення ключа шифрування шляхом збору достатньої кількості зашифрованого трафіку. Існують різноманітні інструменти, які дозволяють легко зламати WEP-

захищену мережу за відносно короткий час. На сьогоднішній день використання WEP є неприпустимим через його слабку захищеність.

Рисунок 1.2 ілюструє зашифроване повідомлення яке створюється шляхом застосування операції XOR до відкритого тексту, ICV (контрольної суми інтеграції) та ключового потоку.

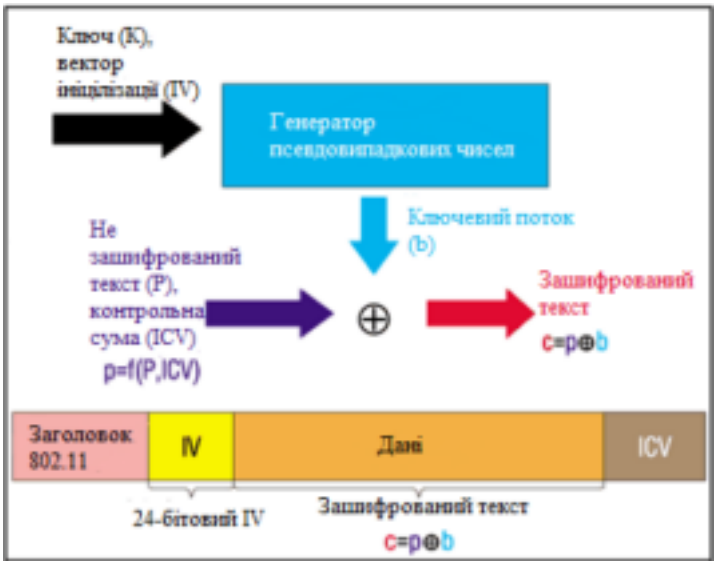

Рисунок 1.2 – Принцип роботи шифрування за протоколом WEP WPA (Wi-Fi Protected Access) представлений у 2003 році, був розроблений як тимчасова заміна WEP для усунення його основних вразливостей. Він використовував протокол TKIP (Temporal Key Integrity Protocol), який забезпечував динамічну зміну ключів шифрування, ускладнюючи атаки. WPA також підтримував аутентифікацію через сервер RADIUS у корпоративних мережах (WPA-Enterprise). Однак TKIP залишався частково вразливим до атак, таких як атака на повторне використання ключів. WPA впровадив кілька важливих покращень у безпеці: - TKIP (Temporal Key Integrity Protocol) -це протокол цілісності тимчасового ключа, який використовував той самий базовий алгоритм RC4, але значно покращив процес генерації та обміну ключами. TKIP генерував новий ключ шифрування для кожного пакета даних, що унеможливлювало атаки, засновані на повторному використанні IV. Також TKIP включав механізм перевірки цілісності повідомлень (MIC) для запобігання підробці пакетів.

- 802.1X аутентифікація - це централізована аутентифікація користувачів через RADIUS-сервер. Це особливо важливо для корпоративних мереж, де потрібен

строгий контроль доступу;

- покращене керування ключами WPA, що значно покращило процедури генерації та обміну ключами шифрування, ускладнивши їхнє перехоплення та розшифрування;

Незважаючи на значні поліпшення порівняно з WEP, WPA також мав певні вразливості, зокрема пов'язані з використанням RC4. Однак, атаки на WPA були значно складнішими і вимагали більше часу та ресурсів.

WPA2 (Wi-Fi Protected Access 2) затверджений у 2004 році, став наступним поколінням стандартів безпеки Wi-Fi, яке стало обов'язковим для сертифікації Wi Fi пристроїв з 2006 року. WPA2 впровадив значні зміни в архітектурі безпеки, засновані на повноцінному стандарті IEEE 802.11i. Ключовими особливостями WPA2 є:

- AES (Advanced Encryption Standard) з режимом роботи CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), це заміна RC4 на більш надійний та криптографічно стійкий алгоритм AES. Режим CCMP забезпечує як конфіденційність, так і цілісність даних. Використання 128-бітного ключа AES значно ускладнює несанкціоноване розшифрування трафіку.

- підтримка режимів Personal (PSK) та Enterprise (802.1X), у WPA2 підтримує два основні режими роботи. WPA2-Personal (також відомий як PSK – Pre-Shared Key) використовує попередньо встановлений пароль (ключ) для аутентифікації та шифрування. Цей режим широко використовується в домашніх та малих офісних мережах. WPA2-Enterprise використовує протокол 802.1X та RADIUS-сервер для централізованої аутентифікації кожного користувача за допомогою індивідуальних облікових даних. Цей режим є кращим для великих корпоративних мереж, де потрібен високий рівень контролю доступу.

WPA2 протягом тривалого часу вважався надійним стандартом безпеки. Однак, з часом були виявлені певні вразливості, такі як KRACK (Key Reinstallation Attacks) у 2017 році, які дозволяли зловмисникам перехоплювати та потенційно

розшифровувати трафік. Хоча ці вразливості були усунені за допомогою оновлень програмного забезпечення, вони підкреслили необхідність подальшого вдосконалення стандартів безпеки безпроводових мереж.

Рисунок 1.3 ілюструє діаграму Венна з відмінними та спільними характеристиками:

WEP використовує RC4, WPA — TKIP, WPA2 — AES/CCMP.

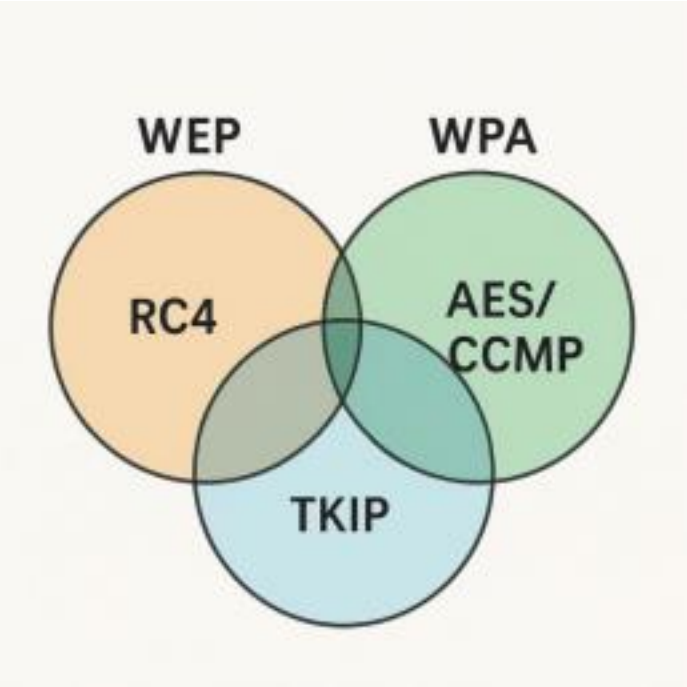

Рисунок 1.3 – Порівняння безпеки стандартів WEP, WPA та WPA2.

1.3. Детальний аналіз стандарту безпеки WPA3

WPA3 (Wi-Fi Protected Access 3) це третє покоління засобів захисту бездротових мереж Wi-Fi, представлений на Wi-Fi Alliance у 2018 році, є найновішим стандартом безпеки для безпроводових мереж. WPA3 розроблений для заміни WPA2 у широкому застосуванні, забезпечуючи надійнішу автентифікацію, підвищену криптографічну стійкість для глобальних ринків даних і підтримку безпеки критично важливих мереж.

WPA3 пропонує додаткові функції, адаптовані до потреб безпеки особистих і корпоративних Wi-Fi мереж. Користувачі WPA3-Personal отримують покращений захист від атак на паролі, тоді як WPA3-Enterprise підтримує протоколи безпеки для

глобальних мереж. При цьому WPA3 забезпечує зворотну сумісність із пристроями WPA2.

WPA3-Personal забезпечує надійніший захист для індивідуальних користувачів завдяки вдосконаленій автентифікації на основі паролів, навіть якщо паролі не відповідають стандартним вимогам до складності. Це досягається за допомогою технології одночасної автентифікації рівних (SAE), яка замінила метод спільного

ключа (PSK) у WPA2-Personal. SAE стійка до офлайнових словникових атак, коли зловмисник намагається підібрати пароль без взаємодії з мережею. Завдяки SAE пристрої з WPA3-Personal отримують посилений захист від брутфорс-атак, забезпечуючи безпеку навіть за використання слабких паролів.

Сильні сторони WPA3-Personal:

- дозволяє користувачам обирати прості для запам'ятовування паролі без шкоди для безпеки мережі;

- використання алгоритму SAE забезпечує покращений захист завдяки новій концепції автентифікації;

- підтримка прямої секретності (Forward Secrecy), яка зберігає безпеку ключів сесії навіть у разі компрометації пароля мережі;

Для корпоративних потреб застосовується специфікація WPA3-Enterprise, призначена для бездротових мереж у державних установах, бізнес-компаніях та фінансових організаціях.

На відміну від WPA3-Personal, WPA3-Enterprise використовує посилене 192-бітне шифрування ключа сесії замість 128-бітного. Цей режим безпеки поєднує криптографічні інструменти, забезпечуючи стабільну базову безпеку для мереж WPA3.

За заявою Wi-Fi Alliance, 192-бітне шифрування є надлишковим для домашніх мереж, але для конфіденційних корпоративних мереж воно слугує додатковим заходом захисту. Використання 192-бітного шифрування ключа в WPA3-Enterprise не є обов'язковим, але ця специфікація орієнтована на застосування в корпоративних мережах для забезпечення підвищеного рівня безпеки.

Для наочного відображення відмінностей між WPA2 та WPA3 наведемо таблицю 1.2.

Таблиця 1.2 – Порівняння стандартів безпеки WPA2 та WPA3

Характеристика	WPA2	WPA3
Протокол шифрування	AES-CCMP	AES-CCMP, GCMP-256

Аутентифікація	PSK, 802.1X	SAE, 802.1X
Захист від офлайн-атак	Обмежений	Високий (SAE)
Forward Secrecy	Відсутня	Присутня
Безпека відкритих мереж	Відсутня	OWE

1.3.1. Режими роботи WPA3 (WPA3-Personal, WPA3-Enterprise, OWE) WPA3-Personal замінює чотиристоронніє рукостискання на одночасну автентифікацію (SAE), визначену в стандарті IEEE 802.11s. Хоча SAE спочатку розроблявся для мережевих ліній, він тепер застосовується для масштабування інфраструктурних бездротових мереж. WPA3 підтримує кілька режимів роботи, призначених для різних типів безпроводових мереж та вимог до безпеки: - WPA3-Personal – це стандарт призначений для використання в домашніх та малих офісних мережах. Як і WPA2-Personal, використовує попередньо встановлений пароль (PSK) для аутентифікації. Однак, ключовою відмінністю є використання протоколу SAE замість чотирьохстороннього handshake (Four-Way Handshake) для встановлення з'єднання. Це значно підвищує стійкість до офлайн атак на пароль.

- WPA3-Enterprise -це стандарт призначений для використання у великих корпоративних мережах, де потрібна централізована аутентифікація користувачів. Як і WPA2-Enterprise, використовує протокол 802.1X та RADIUS-сервер для аутентифікації кожного користувача за допомогою індивідуальних облікових даних (логін/пароль, сертифікати тощо). WPA3-Enterprise також надає опціональну підтримку 192-бітного набору алгоритмів безпеки (Suite B), забезпечуючи

підвищений рівень криптографічної стійкості для організацій з високими вимогами до безпеки.

- OWE (Opportunistic Wireless Encryption) - призначений для використання у відкритих безпроводових мережах, де не потрібна аутентифікація за допомогою пароля. OWE забезпечує автоматичне шифрування з'єднання між кожним клієнтом та точкою доступу за допомогою протоколу PMKSA (Pairwise Master Key Security

Association). Це захищає дані користувачів від перехоплення в публічних Wi-Fi мережах. Важливо зазначити, що OWE забезпечує лише шифрування трафіку, але не аутентифікацію точки доступу.

На рисунку 1.4 схематично зображено основні режими роботи WPA3.

Рисунок 1.4 – Режими роботи WPA3

1.3.2. Технологія Simultaneous Authentication of Equals (SAE) у WPA3-Personal

SAE – це новий криптографічний метод «рукостискання», також відомий як Dragonfly Key Exchange, який замінив використання спільного ключа (PSK) у WPA3.

Основні принципи роботи SAE:

- протокол обміну ключами на основі еліптичних кривих (Elliptic Curve Cryptography – ECC);
- захист від атак з використанням попередньо обчислених таблиць (precomputed table attacks);

- пряма секретність (Forward Secrecy);
- стійкість до атак повторного відтворення (replay attacks);

На відміну від чотирьохстороннього handshake у WPA2-Personal, який виявився вразливим до офлайн-атак на пароль, SAE забезпечує більш безпечний процес аутентифікації та встановлення ключа шифрування. Проблема з PSK стала актуальною кілька років тому через атаки типу KRACK (Key Reinstallation Attacks), що дозволяють перехоплювати та повторно встановлювати ключі сесії.

Атаки KRACK використовують вразливість чотиристороннього «рукостискання» WPA2, яке активується під час підключення клієнта до захищеної Wi-Fi мережі. Цей процес перевіряє наявність коректних облікових даних у клієнта і точки доступу та узгоджує ключ шифрування для захисту трафіку. Зловмисник, застосовуючи атаку типу «людина посередині», може примусити учасників мережі перевстановити ключі шифрування, що дозволяє розшифрувати трафік, здійснити HTTP-ін'єкції, перехопити TCP-з'єднання тощо.

SAE усуває вразливості до атак типу KRACK та словникових атак, спрямованих на підбір значень для PSK-з'єднань. Ключова відмінність SAE від PSK полягає в тому, що обидві сторони бездротового зв'язку можуть одночасно ініціювати запити на з'єднання, замість послідовного обміну повідомленнями. Це унеможливлює атаки типу KRACK і словникові атаки.

На рисунку 1.5 та 1.6 продемонстрована робота мережі без KRACK атаки та безпосередньо з KRACK атакою на мережу.

Рисунок 1.5 – Робота мережі без KRACK

Рисунок 1.6 – Робота мережі при проведені KRACK атаки

Завдяки цим особливостям SAE значно підвищує рівень безпеки WPA3- Personal порівняно з WPA2-Personal, роблячи офлайн-атаки на пароль практично неможливими.

1.3.4. Enhanced Open (OWE)

Enhanced Open (OWE) є режимом роботи WPA3, призначеним для забезпечення шифрування даних у відкритих безпроводових мережах. Традиційно, у відкритих Wi-Fi мережах трафік передається без шифрування, що створює значні ризики для конфіденційності користувачів. OWE розв'язує цю проблему шляхом автоматичного встановлення зашифрованого з'єднання між кожним клієнтським пристроєм та точкою доступу.

Основні принципи роботи OWE:

1. Диференційоване шифрування для кожного клієнта.

2. Проста інтеграція.

3. Покращення конфіденційності в публічних мережах.

Важливо зазначити, що OWE забезпечує лише шифрування трафіку між клієнтом та точкою доступу. Він не забезпечує аутентифікацію точки доступу, тому користувачі повинні бути обережними при підключенні до невідомих відкритих мереж.

1.3.5. Підтримка 192-бітного шифрування у WPA3-Enterprise Для організацій з особливо високими вимогами до безпеки WPA3-Enterprise пропонує опціональну

підтримку 192-бітного набору криптографічних алгоритмів, визначених у рамках Suite B cryptography. Використання 192-бітного шифрування значно підвищує криптографічну стійкість мережі до сучасних та майбутніх загроз. Основні компоненти 192-бітного набору Suite B у WPA3-Enterprise: 1. Алгоритм шифрування AES-GCM (Galois/Counter Mode) з 192-бітним ключем.

2. Протокол автентифікації HMAC-SHA384 (Hash-based Message Authentication Code using SHA-384).

3. Протокол обміну ключами ECDH (Elliptic Curve Diffie-Hellman) з використанням еліптичної кривої з 384 бітами (NIST P-384).

4. Алгоритм цифрового підпису ECDSA (Elliptic Curve Digital Signature Algorithm) з використанням еліптичної кривої з 384 бітами (NIST P-384). Впровадження 192-бітного шифрування у WPA3-Enterprise забезпечує значно вищий рівень безпеки порівняно зі стандартним 128-бітним шифруванням AES CCMP у WPA2-Enterprise, роблячи мережу більш стійкою до сучасних та перспективних криптографічних атак. Однак, використання 192-бітного шифрування може вимагати більших обчислювальних ресурсів від обладнання. Для наочного відображення відмінностей шифрування між WPA2 та WPA3 наведемо таблицю 1.3.

Таблиця 1.3 – Порівняння шифрування у WPA3-Enterprise

Режим	Алгоритм	Довжина ключа	Застосування
WPA2-Enterprise	AES-CCMP	128 біт	Корпоративні мережі
WPA3-Enterprise	AES-GCMP	192 біт	Високобезпечні мережі

Також на рисунку 1.7 зображене детальне порівняння криптографічної стійкості між WPA2 та WPA3.

Рисунок 1.7 – Порівняння криптографічної стійкості WPA2 і WPA3

1.4 Висновки до розділу 1

Проведений аналіз сучасного стану безпроводових мереж та стандартів безпеки показав значну еволюцію технологій Wi-Fi. Від перших стандартів з низькою швидкістю передачі даних та слабким захистом до сучасних стандартів 802.11ax (Wi-Fi 6) та новітнього стандарту безпеки WPA3, безпроводові мережі пройшли довгий шлях розвитку.

Стандарти Wi-Fi постійно вдосконалювалися, забезпечуючи значне збільшення швидкості передачі даних, покращення ефективності використання радіочастотного спектра та підвищення надійності з'єднання. Паралельно відбувалася еволюція стандартів безпеки, починаючи з вразливого WEP, через більш захищені WPA та WPA2, і завершуючи найновішим стандартом WPA3, який пропонує значні поліпшення в галузі безпеки безпроводових мереж.

WPA3 вносить ключові зміни, спрямовані на усунення вразливостей попередніх стандартів та забезпечення більш високого рівня захисту. Впровадження протоколу SAE у WPA3-Personal ефективно захищає від офлайн атак на пароль. Технологія OWE забезпечує шифрування даних у відкритих

мережах. WPA3-Enterprise пропонує опціональну підтримку 192-бітного шифрування для організацій з високими вимогами до безпеки.

Таким чином, WPA3 є значним кроком вперед у забезпеченні безпеки безпроводових мереж, пропонуючи більш надійний захист як для особистих, так і для корпоративних користувачів. Подальший розвиток та впровадження WPA3 є важливим фактором для створення безпечних та надійних безпроводових інфраструктур в умовах зростаючих кіберзагроз. У наступних розділах буде розглянуто практичні аспекти створення безпроводової мережі з підтримкою WPA3 та конфігурації параметрів безпеки.

РОЗДІЛ 2
ПРОЕКТУВАННЯ БЕЗПРОВОДОВОЇ МЕРЕЖІ

2.1 Визначення вимог до безпроводової мережі

Першим і фундаментальним кроком у проектуванні будь-якої безпроводової мережі є ретельне визначення вимог. Від точності та повноти цього етапу залежить, наскільки майбутня мережа буде відповідати очікуванням користувачів та завданням організації. Процес визначення вимог охоплює аналіз кількох ключових аспектів: площі покриття, очікуваної кількості користувачів та їхніх пристроїв, типів трафіку, що передаватиметься, та специфічних вимог до безпеки.

Проектування безпроводової мережі починається з чіткого визначення вимог, які формуються на основі потреб користувачів, умов експлуатації та цілей організації. Основними параметрами, які необхідно врахувати, є:

1. Аналіз планів приміщень. Для точного визначення площі покриття необхідно отримати та проаналізувати детальні плани будівлі або території. На цих планах слід відзначити всі зони, де потрібен доступ до Wi-Fi. Важливо враховувати не тільки горизонтальну площу, але й вертикальну (кількість поверхів).

2. Характеристики будівельних матеріалів. Тип та товщина стін, перекриттів, наявність металевих конструкцій, скла – все це суттєво впливає на поширення радіосигналу. Наприклад, залізобетонні стіни значно сильніше послаблюють сигнал, ніж гіпсокартонні перегородки. Необхідно зібрати інформацію про матеріали, використані в конструкції будівлі.

Таблиця 2.1. Орієнтовний рівень загасання сигналу для різних матеріалів (на частоті 2.4 ГГц та 5 ГГц).

Матеріал	Загасання на 2.4 ГГц (дБ)	Загасання на 5 ГГц (дБ)
Гіпсокартон	3-5	4-7
Дерево	5-10	7-15
Скло (звичайне)	2-4	3-6
Скло (тоноване)	5-12	8-18
Цегла	8-15	12-25
Бетон	10-20	15-30
Метал	20-30+	25-40+

3. Зони з високою щільністю користувачів. Окремо слід виділити зони, де очікується велике скупчення користувачів (конференц-зали, аудиторії, зони відпочинку). У таких місцях вимоги до пропускної здатності та стабільності сигналу будуть вищими.

4. Зовнішні території. Якщо покриття потрібне і на прилеглій території (парковки, внутрішні двори), необхідно врахувати вплив погодних умов, наявність перешкод (дерева, інші будівлі) та необхідність використання спеціалізованих зовнішніх точок доступу.

5. Масштабованість. Важливо закласти можливість розширення покриття в майбутньому.

На рисунку 2.1 для наочності, зображено приклад проектування мережі для триповерхової офісної будівлі загальною площею 1500 м² (500 м² на поверх).

Рисунок 2.1 - Приклад плану поверху офісної будівлі з позначенням зон необхідного покриття

Наступним важливим параметром є визначення кількості одночасних користувачів та типів пристроїв, які будуть підключатися до мережі. - середня та пікова кількість користувачів, тут необхідно оцінити, скільки користувачів одночасно будуть користуватися мережею в середньому та під час пікових навантажень;

- стаціонарні користувачі - це працівники з ноутбуками, стаціонарними ПК з Wi-Fi адаптерами;

- мобільні користувачі - це працівники зі смартфонами, планшетами; - гостьові користувачі – це відвідувачі, клієнти, партнери. Для них часто створюється окрема гостьова мережа з обмеженим доступом;

- типи пристроїв та їхні стандарти Wi-Fi, тут важливо розуміти, які стандарти

Wi-Fi (802.11a/b/g/n/ac/ax) підтримують пристрої користувачів. Мережа повинна забезпечувати сумісність зі старішими пристроями, але орієнтуватися на переваги нових стандартів. Підтримка WPA3 є ключовою вимогою, тому пристрої мають бути сумісними з цим протоколом;

- пристрої IoT, якщо в мережі будуть використовуватися пристрої IoT, їх кількість та вимоги до трафіку також слід врахувати. Часто для таких пристроїв створюють окремий VLAN для ізоляції та безпеки;

Припустимо, в нашому офісі на 100 співробітників кожен має в середньому 2 пристрої (ноутбук та смартфон). Також очікується до 20 гостьових підключень одночасно. Таким чином, пікове навантаження може становити:

*(100 * 2) + 20 = 220 пристроїв* (1.1) Розуміння того, які програми та сервіси будуть використовуватися в мережі, дозволяє визначити вимоги до пропускної здатності та затримок. Основні типи трафіку:

- веб-серфінг та електронна пошта;

- файлообмін та доступ до мережевих ресурсів;

- voip (voice over ip) та відеоконференції;

- стримінг відео (навчальні матеріали, презентації);

- робота з хмарними сервісами;

- спеціалізоване програмне забезпечення;

Пріоритезація трафіку (QoS - Quality of Service). Для критично важливих додатків (наприклад, VoIP, відеоконференції) необхідно передбачити механізми пріоритезації трафіку. Це дозволить забезпечити їх стабільну роботу навіть при високому завантаженні мережі.

На основі аналізу типів трафіку та кількості користувачів можна розрахувати орієнтовну сумарну пропускну здатність, яка потрібна від мережі продемонстрована у таблиці 2.2.

Таблиця 2.2 - Орієнтовні вимоги до пропускної здатності для різних типів трафіку на одного користувача.

Тип трафіку	Пропускна здатність (Мбіт/с)	Чутливість до затримок
Веб-серфінг	1–5	Середня
E-mail	0.5–1	Низька
VoIP (якісний)	0.1–0.5	Висока
Відеоконференція SD	1–2	Висока
Відеоконференція HD	3–5	Висока
Стрімінг відео HD	5–8	Середня
Файлообмін	5–20+ (залежно від розміру)	Низька
Хмарні сервіси	2–10+ (залежно від активності)	Середня

Наприклад, якщо 50 користувачів одночасно беруть участь у відеоконференціях HD (5 Мбіт/с кожен), а інші 170 користувачів активно працюють з хмарними сервісами та веб-серфінгом (в середньому 3 Мбіт/с кожен), то пікова потреба може складати:

*(50 * 5) + (170 * 3) = 250 + 510 = 760 Мбіт/с.* (1.2) Це значення є орієнтовним і потребує подальшого уточнення при виборі обладнання.

Безпека є одним із найважливіших аспектів сучасної безпроводової мережі. У контексті даної дипломної роботи ключовою вимогою є підтримка WPA3 (Wi-Fi Protected Access 3).

Автентифікація користувачів:

- для корпоративних користувачів, рекомендується використовувати WPA3-Enterprise з автентифікацією через сервер RADIUS. Це дозволяє централізовано керувати доступом, використовувати унікальні облікові дані для кожного користувача та легко відкликати доступ у разі потреби.

- для гостьових користувачів, можливі варіанти:

- WPA3-Personal з окремим, регулярно змінюваним паролем;

- Використання порталу авторизації (Captive Portal) у поєднанні з OWE або WPA3-Personal;

Сегментація мережі (VLAN), а саме розділення мережі на логічні сегменти є важливим заходом безпеки. Це обмежує можливість поширення атак та несанкціонованого доступу між різними групами користувачів та пристроїв.

Системи виявлення та запобігання вторгнень (WIDS/WIPS). Для великих та критично важливих мереж може бути доцільним впровадження систем Wireless Intrusion Detection/Prevention System для моніторингу радіоефіру, виявлення неавторизованих точок доступу, атак типу «людина посередині» (MitM) та інших загроз. Всі точки доступу, комутатори та маршрутизатори повинні бути розміщені в місцях, що унеможливлюють несанкціонований фізичний доступ до них. Регулярне оновлення програмного забезпечення. Розробка та впровадження чітких політик безпеки для користувачів.

Визначення цих вимог на початковому етапі дозволяє сформувати чітке технічне завдання для подальшого проектування та вибору обладнання, що гарантуватиме створення ефективної, надійної та, головне, безпечної безпроводової мережі з підтримкою WPA3.

2.2 Вибір топології мережі

Після визначення вимог наступним кроком є вибір відповідної топології безпроводової мережі. Топологія визначає, як точки доступу (AP) з'єднуються між собою та з дротовою інфраструктурою, а також як клієнтські пристрої взаємодіють з мережею. Вибір топології залежить від розміру мережі, вимог до мобільності,

бюджету та доступної кабельної інфраструктури. Для безпроводових мереж основними топологіями є:

Топологія на основі автономних точок доступу (Standalone APs). Це найпростіша топологія, де кожна точка доступу налаштовується та керується індивідуально. На рисунку 2.2 для наочності продемонстрована топологія Standalone APs.

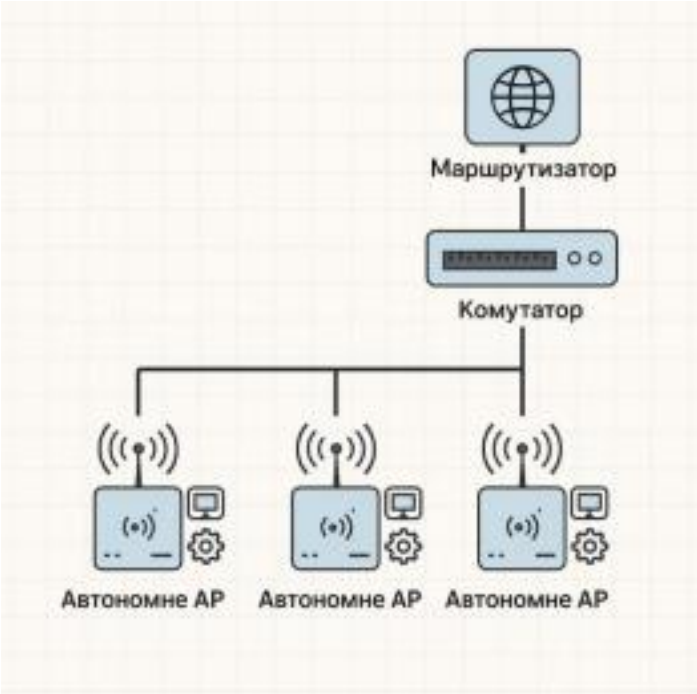

Рисунок 2.2 - Схема топології на основі автономних точок доступу

Топологія на основі контролера (Controller-based WLAN). Це найбільш поширена топологія для середніх та великих безпроводових мереж. Вона передбачає використання центрального пристрою – контролера безпроводової мережі (WLAN Controller). У таблиці 2.3 продемонстровано переваги та недоліки топології.

Таблиця 2.3 - Переваги та недоліки топології Controller-based WLAN

Переваги	Недоліки
централізоване управління та моніторинг	вища початкова вартість
покращений роумінг	єдина точка відмови (Single Point of Failure)
масштабованість	вимоги до продуктивності контролера
розширені функції безпеки	складність налаштування та управління
оптимізація радіочастотного середовища	обмежена масштабованість

На рисунку 2.3 та 2.4 для наочності продемонстрована топологія Controller based WLAN основі фізичний та хмарного контролера.

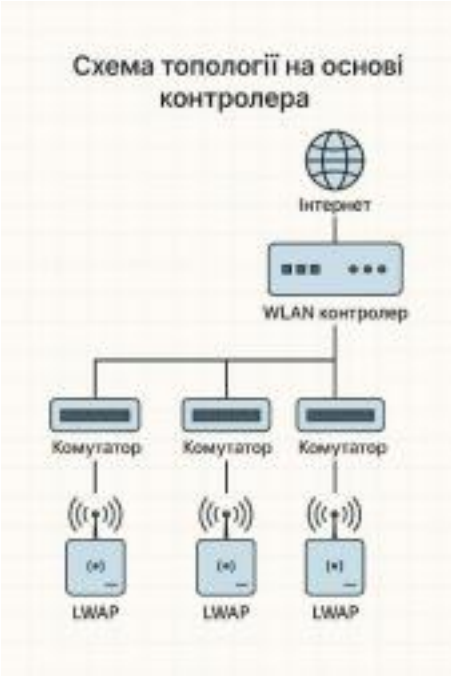

Рисунок 2.3 - Схема топології на основі контролера (фізичний контролер)

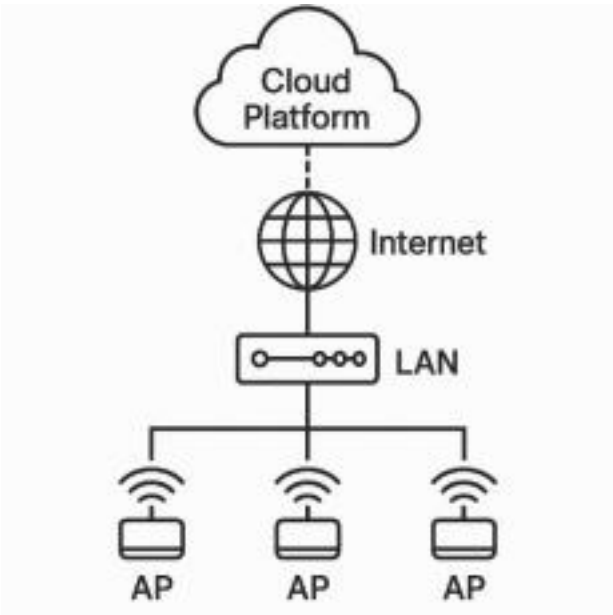

Рисунок 2.4 - Схема топології на основі хмарного контролера

Mesh-топологія (Безпроводова комірчаста мережа). Mesh-мережі використовуються для розширення покриття в місцях, де прокладання кабелю до кожної точки доступу є складним або неможливим.

На рисунку 2.5 для наочності продемонстрована Mesh-топологія.

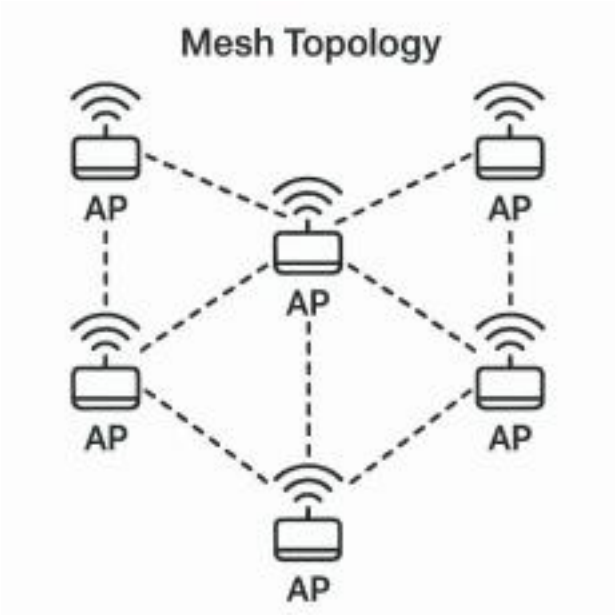

Рисунок 2.5 - Схема Mesh-топології

Для проекту «Створення безпроводової мережі з підтримкою WPA3 з конфігурацією безпеки», особливо якщо йдеться про корпоративне середовище середнього або великого розміру (як у прикладі офісної будівлі), рекомендованою топологією є топологія на основі контролера (Controller-based WLAN). Причини такого вибору:

1. Централізоване управління безпекою.
2. Масштабованість та керованість.
3. Оптимізація радіосередовища та роумінгу.
4. Розширені функції.

Для нашої триповерхової офісної будівлі з орієнтовно 220 пристроями, топологія на основі контролера (ймовірно, фізичного або віртуального, розміщеного локально, або хмарного) буде оптимальним вибором для забезпечення надійного, безпечного та керованого Wi-Fi покриття з підтримкою WPA3.

2.3 Планування розміщення точок доступу (Site Survey)

Планування розміщення точок доступу, відоме як радіообстеження (Site Survey), є критично важливим етапом проектування безпроводової мережі. Його мета – визначити оптимальні місця встановлення точок доступу (AP) для

забезпечення необхідного покриття, пропускної здатності та мінімізації інтерференції, враховуючи специфіку приміщень та вимоги до мережі. Неправильне

розміщення AP може призвести до «мертвих зон» (ділянок без сигналу), низької швидкості передачі даних, нестабільного з'єднання та проблем з безпекою. Процес Site Survey можна розділити на кілька етапів: 1. Підготовчий етап:

- збір вихідних даних;

- вибір типу Site Survey;

На рисунку 2.6 для наочності продемонстровано приклад карти прогнозного покриття Wi-Fi .

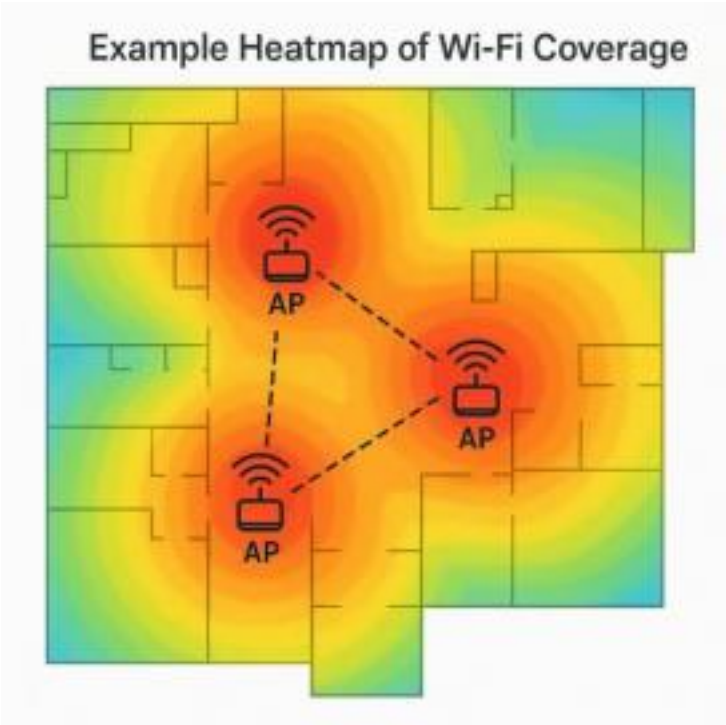

Рисунок 2.6 - Приклад карти прогнозного покриття Wi-Fi

2. Проведення прогнозного моделювання (Predictive Site Survey): -

імпорт планів приміщень;

- визначення зон покриття;

- налаштування параметрів середовища;

- вибір моделі AP;

- розміщення віртуальних AP;

- ітераційний процес;

3. Проведення обстеження на місці (On-Site Survey):

Після прогнозного моделювання виконується обстеження безпосередньо на об'єкті.

- необхідне обладнання;

- процедура пасивного обстеження;

- процедура активного обстеження;

- аналіз результатів обстеження на місці;

4. Документування результатів Site Survey:

Після завершення всіх етапів Site Survey необхідно підготувати детальний звіт, який зазвичай включає:

- опис методики проведення обстеження;

- плани приміщень з остаточним розташуванням всіх AP;

- для кожної AP: модель, MAC-адреса, IP-адреса, місце встановлення, канал, потужність передачі;

- карти покриття (heatmaps) для рівня сигналу, SNR, інтерференції; -

результати вимірювань продуктивності;

- рекомендації щодо налаштувань мережі (SSID, безпека, VLAN); -

фотографії місць встановлення AP;

Ретельне планування розміщення точок доступу є запорукою створення високопродуктивної та надійної безпроводової мережі, яка відповідатиме всім вимогам користувачів та бізнесу. Для мережі з підтримкою WPA3 особливо важливо забезпечити якісне покриття, оскільки проблеми з сигналом можуть негативно впливати на процеси автентифікації та шифрування.

2.4 Вибір мережевого обладнання з урахуванням підтримки WPA3

Вибір правильного мережевого обладнання є вирішальним для успішної реалізації безпроводової мережі, особливо з урахуванням вимоги підтримки сучасного стандарту безпеки WPA3. На цьому етапі необхідно підібрати точки доступу, маршрутизатори (якщо потрібна їх заміна або новий), комутатори та, у

випадку контролерної архітектури, WLAN-контролер.

Загальні критерії, якими слід керуватися при виборі будь-якого мережевого обладнання:

-підтримка стандартів;

-продуктивність;

-масштабованість;

-надійність;

-керованість;

-безпека;

-сумісність;

-вартість;

-гарантія та технічна підтримка;

Точки доступу є серцем безпроводової мережі. Їх вибір безпосередньо впливає на якість покриття, швидкість та безпеку. Для нашого проекту слід обирати AP стандарту Wi-Fi 6 з підтримкою WPA3 та можливістю централізованого управління. Рекомендується використовувати точки доступу, такі як Cisco Catalyst 9120AX або Ubiquiti UniFi 6 Pro, які підтримують WPA3, Wi-Fi 6 і забезпечують високу пропускну здатність (до 3.5 Гбіт/с у діапазоні 5 ГГц).

Для нашого проекту з офісною будівлею та орієнтовно 10-20 AP (кількість буде уточнена після Site Survey), підійде фізичний контролер початкового або середнього рівня, віртуальний контролер на існуючому сервері або хмарне рішення. Вибір залежатиме від бюджету та IT-інфраструктури компанії.

Комутатори забезпечують підключення точок доступу до дротової мережі та живлення через PoE. Для нашого проекту знадобляться керовані L2/L3 комутатори доступу з достатньою кількістю портів Gigabit Ethernet та підтримкою PoE+ з відповідним бюджетом PoE. Рекомендується використовувати PoE-комутатор (Cisco Catalyst 9200) для живлення точок доступу та підключення до мережі.

Маршрутизатор забезпечує підключення локальної мережі до Інтернету, маршрутизацію трафіку між різними підмережами (VLAN), а також може

виконувати функції міжмережевого екрану (Firewall), VPN-сервера, DHCP-сервера та NAT. Для нашого проекту підійде маршрутизатор MikroTik hAP ax³, який

підтримує WPA3 і має достатню продуктивність для обробки трафіку 150 користувачів.

Рекомендується обирати обладнання від відомих виробників, що спеціалізуються на корпоративних рішеннях, для забезпечення надійності, безпеки та підтримки. Остаточний вибір моделей буде залежати від результатів Site Survey, бюджету та специфічних потреб організації.

2.5 Розробка логічної структури мережі (VLANи, IP-адресація)

Після вибору фізичного обладнання та планування його розміщення, наступним важливим кроком є розробка логічної структури мережі. Це включає планування віртуальних локальних мереж (VLAN), розробку схеми IP-адресації та налаштування серверів DHCP. Грамотно спроектована логічна структура підвищує безпеку, керованість та ефективність мережі.

Планування віртуальних локальних мереж (VLAN) (Virtual Local Area Network) – це технологія, що дозволяє логічно розділити одну фізичну мережу на декілька незалежних широкомовних доменів. Кожен VLAN функціонує як окрема логічна мережа, навіть якщо пристрої підключені до одного й того ж комутатора.

Переваги використання VLAN:

-безпека;

-зменшення широкомовного трафіку;

-гнучкість;

-організація;

-покращена керованість;

Рекомендації щодо створення VLAN для безпроводової мережі з підтримкою WPA3. Логічна структура мережі включає сегментацію за допомогою VLAN і планування IP-адресації:

1. VLAN: Для ізоляції трафіку створюються окремі VLAN:

- VLAN 10: для працівників (основна мережа).

- VLAN 20: для гостьового доступу.

- VLAN 30: для IoT-пристроїв (наприклад, розумних датчиків). 2. IP-адресація: Використовується приватна адресація класу C (192.168.0.0/24). Наприклад:

- VLAN 10: 192.168.10.0/24 (для працівників);

- VLAN 20: 192.168.20.0/24 (для гостей);

- VLAN 30: 192.168.30.0/24 (для IoT);

3. DHCP: Центральний DHCP-сервер на маршрутизаторі розподіляє IP-адреси в межах кожної VLAN.

На рисунку 2.7 більш детально розглянемо приклад схеми для триповерхової офісної будівлі, де була обрана топологія на основі контролера та реалізовано сегментацію за допомогою VLAN з підтримкою WPA3.

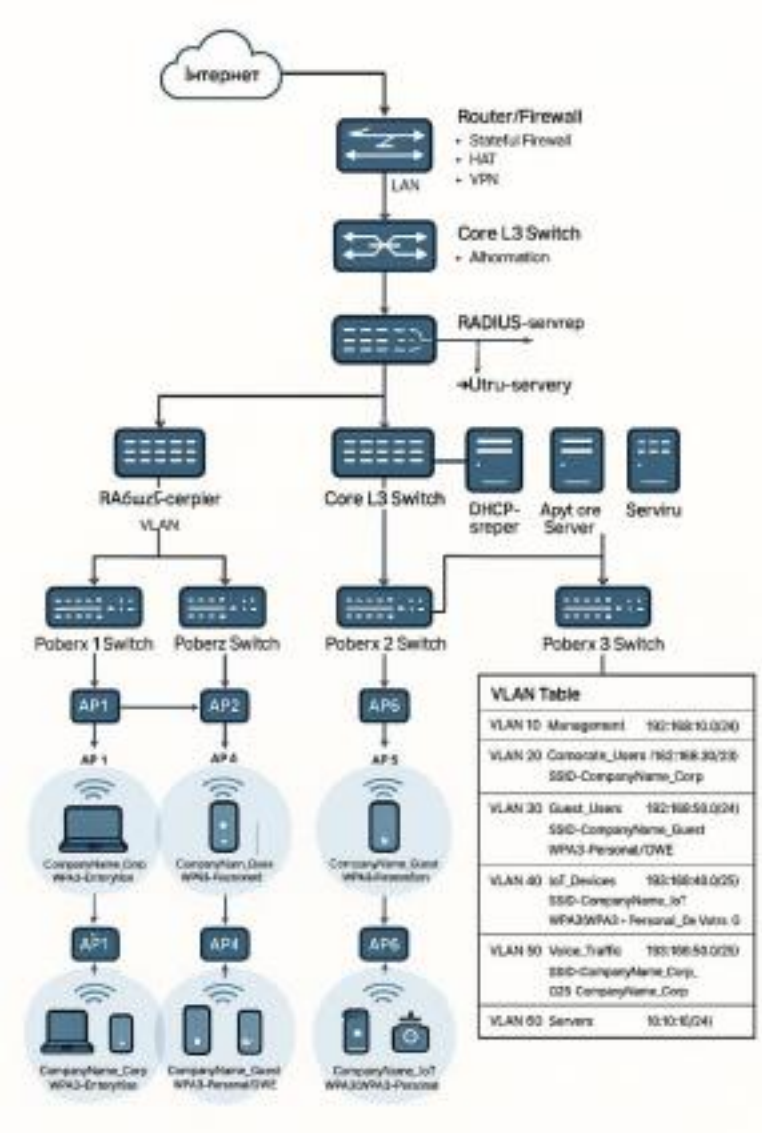

Рисунок 2.7 - Фізично-логічна схема спроектованої безпроводової мережі

Розробка детальної логічної структури мережі є запорукою її безпеки, керованості та ефективності. Правильне планування VLAN, IP-адресації, DHCP та DNS, а також належне налаштування RADIUS для WPA3-Enterprise, створюють міцний фундамент для надійної безпроводової інфраструктури.

На основі всіх попередніх етапів проектування – визначення вимог, вибору топології, планування розміщення точок доступу, вибору обладнання та розробки логічної структури – формується фінальна схема безпроводової мережі. Ця схема візуалізує як фізичне, так і логічне підключення компонентів мережі.

Схема повинна бути достатньо детальною, щоб інженери могли використовувати її для монтажу та налаштування обладнання, а також для подальшого обслуговування та модернізації мережі.

На рисунку 2.8 буде приведений приклад більш деталізованого фрагменту

схеми для одного поверху будівлі нашого проеку.

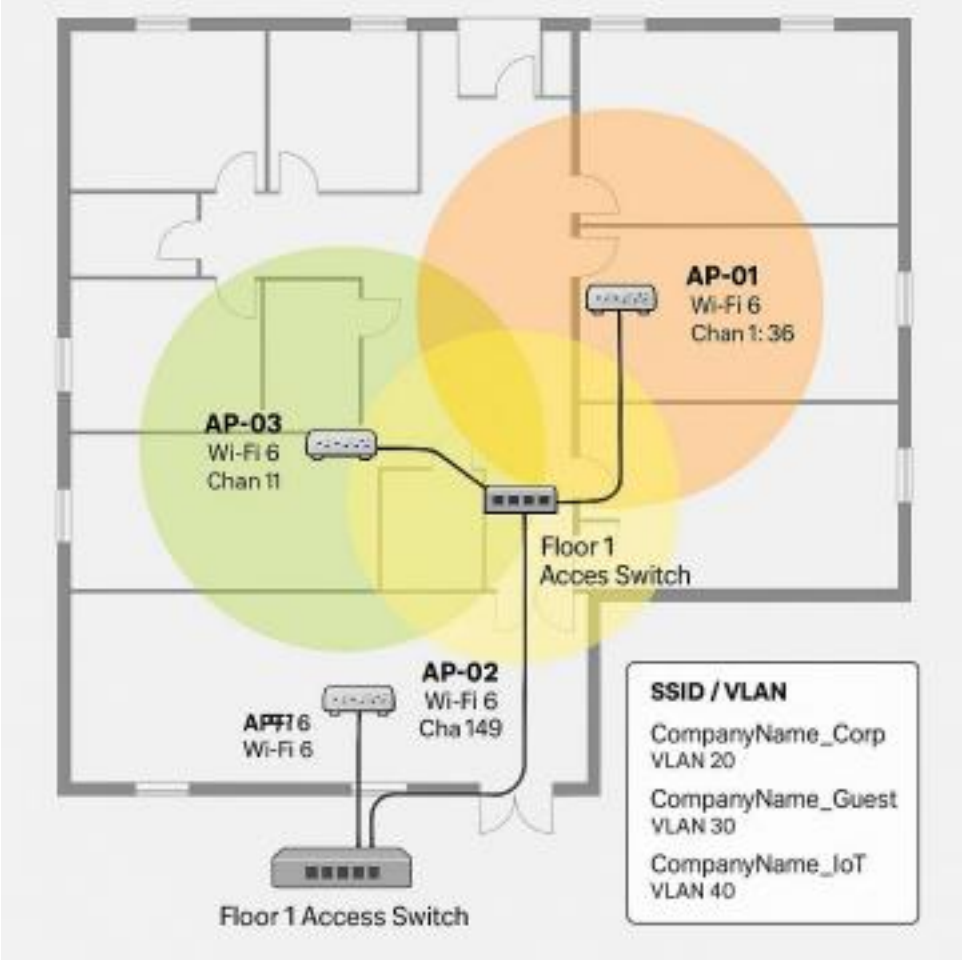

Рисунок 2.8 - Фрагмент схеми безпроводової мережі для одного поверху

2.6 Висновки до Розділу 2

У даному розділі було детально розглянуто процес проектування безпроводової мережі з акцентом на підтримку сучасного стандарту безпеки WPA3 та конфігурацію відповідних параметрів безпеки.

Було наголошено на важливості ретельного аналізу потреб майбутніх користувачів, включаючи визначення площі покриття, очікуваної кількості користувачів та типів пристроїв, аналізу типів трафіку та ключових вимог до безпеки. Розглянуто основні топології безпроводових мереж на основі автономних точок доступу, на основі контролера (фізичного, віртуального, хмарного) та mesh топологію. Детально описано методику проведення радіообстеження, включаючи прогнозний (predictive) та фізичний (on-site) етапи. Наголошено на необхідності аналізу планів приміщень, будівельних матеріалів, потенційних джерел інтерференції та правильного планування каналів.

Сформульовано критерії вибору точок доступу, WLAN-контролерів,

комутаторів та маршрутизаторів з обов'язковим урахуванням підтримки стандарту Wi-Fi 6 (802.11ax) як технологічної основи для WPA3, а також відповідних стандартів PoE, швидкостей портів та функцій управління. Акцентовано увагу на необхідності вибору AP та контролерів, що гарантовано підтримують різні режими WPA3.

Представлено підхід до сегментації мережі за допомогою VLAN для ізоляції трафіку різних груп користувачів (корпоративні, гостьові, IoT-пристрої, голосовий трафік, управління). Розроблено схему IP-адресації, принципи роботи DHCP та DNS. Особливу увагу приділено необхідності налаштування RADIUS-сервера для реалізації WPA3-Enterprise, що забезпечує надійну автентифікацію та авторизацію корпоративних користувачів.

Запропоновано структуру фінальної фізично-логічної схеми, яка візуалізує всі прийняті проектні рішення, включаючи розміщення обладнання, його підключення, розподіл VLAN, SSID та налаштування безпеки. Ця схема слугує дорожньою картою для впровадження та подальшого обслуговування мережі.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ТА КОНФІГУРАЦІЯ БЕЗПРОВОДОВОЇ МЕРЕЖІ З ПІДТРИМКОЮ WPA3.

3.1 Опис процесу встановлення та підключення мережевого обладнання

Ефективність та надійність безпроводової мережі значною мірою залежать від коректного встановлення та підключення мережевого обладнання. Цей процес включає кілька ключових етапів:

1. Планування розміщення обладнання:

- аналіз зони покриття, перед фізичним встановленням необхідно провести

аналіз приміщення або території, де планується розгортання мережі. - мінімізація

«мертвих зон», розташування ТД повинно бути таким, щоб мінімізувати або

повністю виключити зони зі слабким або відсутнім сигналом. - фізична безпека

обладнання, обладнання слід розміщувати в місцях, що унеможливлюють

несанкціонований фізичний доступ, крадіжку або пошкодження. 2. Монтаж точок доступу:

- вибір типу монтажу, залежно від конструкції ТД та умов експлуатації, можливий настінний, стельовий або настільний монтаж.

- точки доступу можуть живитися від стандартного блоку живлення або за технологією Power over Ethernet (PoE). У випадку PoE необхідно переконатися, що комутатор або інжектор підтримують відповідний стандарт PoE (802.3af, 802.3at, 802.3bt) та забезпечують достатню потужність.

- підключення до кабельної інфраструктури, кожна ТД підключається до комутатора або маршрутизатора за допомогою кабелю Ethernet Cat 5e або Cat 6. 3. Встановлення маршрутизатора:

- розміщення маршрутизатора, що виконує функції DHCP-сервера, міжмережевого екрану та шлюзу до Інтернету, зазвичай встановлюється в центральному місці або в серверній кімнаті.

- підключення до провайдера Інтернету, маршрутизатор підключається до модема або оптичного терміналу провайдера послуг Інтернету (ISP) через WAN порт.

- підключення до локальної мережі, LAN-порти маршрутизатора використовуються для підключення комутаторів, точок доступу та інших дротових пристроїв локальної мережі.

4. Перевірка фізичних з'єднань:

- індикація портів, після підключення необхідно перевірити світлодіодні індикатори на портах маршрутизатора, комутаторів та точок доступу. - тестування кабелів, за потреби, особливо при використанні самостійно обжатих кабелів, слід провести їх тестування за допомогою кабельного тестера для виявлення можливих обривів, коротких замикань або неправильного розведення. Умовне зображення

типової схеми підключення обладнання може бути представлене наступним чином (див. рисунок 3.1).

Рисунок 3.1 – Схема підключення мережевого обладнання

Правильне фізичне встановлення та підключення є фундаментом для подальшого успішного налаштування та стабільної роботи безпроводової мережі.

3.2 Початкова конфігурація точок доступу та маршрутизатора

Після фізичного монтажу та підключення обладнання необхідно здійснити його початкову конфігурацію. Цей процес зазвичай передбачає доступ до веб інтерфейсу керування пристроями.

1. Доступ до інтерфейсу керування:

- IP-адреса за замовчуванням маршрутизаторів та точок доступу мають попередньо налаштовану IP-адресу для доступу до веб-інтерфейсу (наприклад, 192.168.1.1, 192.168.0.1). Ця інформація зазвичай вказана в документації до пристрою або на його корпусі.

- підключення комп'ютера для початкового налаштування підключаємося кабелем Ethernet до одного з LAN-портів маршрутизатора або безпосередньо до точки доступу (якщо вона не отримує IP-адресу від DHCP-сервера). Мережевий

адаптер комп'ютера налаштовується на автоматичне отримання IP-адреси або на статичну IP-адресу з тієї ж підмережі, що й пристрій.

- вхід через веб-браузер де вводиться IP-адреса пристрою. З'явиться запит на введення логіна та пароля адміністратора (також вказані в документації, наприклад, admin/admin або admin/password).

2. Початкова конфігурація маршрутизатора:

- зміна пароля адміністратора, це першочергове завдання – встановлення надійного, унікального пароля для облікового запису адміністратора. - налаштування WAN-з'єднання, конфігурація параметрів підключення до Інтернету відповідно до вимог провайдера (тип підключення: DHCP, Static IP, PPPoE, PPTP, L2TP; введення логіна/пароля, якщо потрібно).

- налаштування DHCP-сервера, де є визначення діапазону IP-адрес, які будуть динамічно видаватися клієнтам у локальній мережі, налаштування терміну оренди IP-адреси, DNS-серверів.

- налаштування часового поясу, тут є становлення правильного часового поясу для коректного відображення логів та роботи розкладів;

- оновлення прошивки (Firmware), тут необхідна перевірка наявності та встановлення останньої версії прошивки для маршрутизатора;

3. Початкова конфігурація точок доступу:

- зміна пароля адміністратора, тут аналогічно до маршрутизатора, негайна зміна стандартного пароля адміністратора;

- режим роботи точки доступу, якщо ТД працюватиме в керованому режимі (наприклад, під управлінням контролера WLAN), її необхідно перевести у відповідний режим;

- налаштування IP-адреси, якщо ТД може отримувати IP-адресу динамічно від DHCP-сервера (маршрутизатора) або їй може бути присвоєна статична IP-адреса для зручності керування;

У таблиці 3.1 продемонстровано початкові конфігурації які необхідно налаштувати при першому використанні.

Таблиця 3.1 – Типові параметри початкової конфігурації

Параметр	Маршрутизатор	Точка доступу	Примітки
IP-адреса за замовчуванням	192.168.1.1	192.168.1.254 (або DHCP)	Перевірити документацію
Логін/Пароль за замовчуванням	admin/admin	admin/admin	Негайно змінити!
Режим роботи WAN	DHCP / Static IP / PPPoE	N/A	Залежить від провайдера
Діапазон DHCP	192.168.1.100 - 192.168.1.199	N/A (якщо DHCP клієнт)	Налаштовується на маршрутизаторі
IP-адреса ТД (статична)	N/A	192.168.1.2	Поза діапазоном DHCP, в одній підмережі з маршрутизатором
Маска підмережі	255.255.255.0	255.255.255.0	Зазвичай однакова для всієї локальної мережі
Шлюз за замовчуванням (для ТД)	N/A	IP-адреса маршрутизатора	Необхідно для доступу ТД до мережі та Інтернету (наприклад, для оновлень)
DNS-сервери (для ТД)	N/A	IP-адреса маршрутизатора/публічні DNS	Необхідно для розв'язання імен (наприклад, для серверів оновлень)

Після завершення початкової конфігурації обладнання готове до детального налаштування параметрів безпроводової мережі та безпеки.

3.3. Налаштування безпроводової мережі

Цей підрозділ описує ключові параметри, що визначають функціонування та ефективність безпроводової мережі.

1. Вибір режиму роботи (Infrastructure, Ad-Hoc):

- Infrastructure Mode (Режим інфраструктури) - це найпоширеніший режим роботи для безпроводових мереж. У цьому режимі всі безпроводові клієнти підключаються до центральної точки доступу, яка виступає мостом між безпроводовими клієнтами та дротовою мережею (або іншими безпроводовими клієнтами через цю ж ТД). Цей режим забезпечує централізоване керування, кращу безпеку та можливість підключення до Інтернету через маршрутизатор.

Для створення мережі з підтримкою WPA3 використовується саме цей режим (див. рисунок 3.2).

Рисунок 3.2 – Режим інфраструктури

- Ad-Hoc Mode (Режим «точка-точка» або «комп'ютер-комп'ютер») - у цьому режимі безпроводові клієнти з'єднуються безпосередньо один з одним без використання центральної точки доступу. Цей режим підходить для тимчасового створення невеликих мереж для обміну файлами між кількома пристроями. Однак

він має обмежену зону покриття, нижчу пропускну здатність та обмежені

можливості безпеки.

2. Налаштування SSID (Service Set Identifier):

- ім'я мережі SSID – це ім'я вашої безпроводової мережі, яке бачать користувачі при пошуку доступних Wi-Fi мереж. Воно може містити до 32 символів (літери, цифри).

- рекомендації щодо вибору SSID:

- унікальність ім'я, щоб уникнути плутанини з сусідніми мережами; - не персоналізуйте надмірного використання особистої інформації в SSID з міркувань приватності та безпеки;

- професійний вигляд (для корпоративних мереж);

- приховування SSID (SSID Hiding/Cloaking), у цьому випадку деякі адміністратори приховують SSID, вважаючи, що це підвищує безпеку. Однак це слабкий захід безпеки, оскільки SSID все одно передається в деяких керуючих кадрах і може бути легко виявлений за допомогою спеціалізованих інструментів;

- кілька SSID, сучасні точки доступу часто дозволяють створювати кілька SSID на одному фізичному пристрої;

3. Вибір каналів та потужності сигналу:

- радіочастотні діапазони Wi-Fi 2.4 ГГц та 5 ГГц (6 ГГц для Wi-Fi 6E): - 2.4 ГГц має більше покриття, але меншу кількість каналів, що не перекриваються;

- 5 ГГц пропонує значно більше каналів, що не перекриваються, вищу швидкість передачі даних, але має менший радіус покриття та гірше долає перешкоди порівняно з 2.4 ГГц;

- 6 ГГц (для Wi-Fi 6E/7) надає ще більше каналів та менше інтерференції, але вимагає відповідних клієнтських пристроїв та точок доступу; - Вибір каналу:

- перед вибором каналу рекомендується просканувати радіоефір за допомогою спеціальних програм (Wi-Fi Analyzer для Android, inSSIDer

для Windows) для визначення найменш завантажених каналів та каналів, що використовуються сусідніми мережами;

- для діапазону 2.4 ГГц слід обирати канали 1, 6 або 11, щоб мінімізувати взаємні перешкоди. У діапазоні 5 ГГц вибір каналів значно ширший, і перекриття менш проблематичне, але все одно варто уникати використання тих самих каналів, що й потужні сусідні мережі;

- Ширина каналу (Channel Width): Визначає обсяг частотного спектру, що використовується для передачі даних;

Вибір ширини каналу залежить від щільності Wi-Fi мереж та вимог до пропускної здатності, для наочності у таблиці 3.2 відображені рекомендовані канали за регіонами, а на рисунку 3.3 графічно представлене перекриття каналів у діапазоні 2.4 ГГц.

Таблиця 3.2 – Рекомендовані канали для 2.4 ГГц (для регіонів з 13 каналами)

Група каналів, що не перекриваються	Канали
1	1, 6, 11
2	2, 7, 12
3	3, 8, 13
4	4, 9
5	5, 10

Рисунок 3.3 – Канали, що не перекриваються, у діапазоні 2.4 ГГц -
Потужність передачі сигналу (Transmit Power):

- більшість точок доступу дозволяють регулювати потужність передавача;

- рекомендується налаштовувати потужність таким чином, щоб забезпечити необхідне покриття без надмірного «розливу» сигналу за межі цільової зони;

- деякі сучасні ТД та WLAN-контролери підтримують автоматичне керування потужністю передачі (Automatic Transmit Power Control - ATPC), що динамічно підлаштовує потужність на основі аналізу радіосередовища;

Коректне налаштування цих параметрів є критично важливим для забезпечення стабільної, швидкої та надійної роботи безпроводової мережі перед тим, як переходити до конфігурації безпеки.

3.4 Детальна конфігурація безпеки за стандартом WPA3

Стандарт WPA3 пропонує значні покращення безпеки порівняно з попередніми стандартами WPA2. Розглянемо налаштування різних режимів WPA3. 1.

Налаштування WPA3-Personal (SAE - Simultaneous Authentication of Equals): - WPA3-

Personal призначений для домашніх користувачів та малих офісів. Він замінює WPA2-Personal (PSK) і забезпечує більш надійний захист від офлайн-атак на підбір пароля завдяки використанню протоколу SAE (Simultaneous Authentication of Equals), також відомого як Dragonfly Key Exchange. Навіть якщо пароль слабкий, SAE

ускладнює його компрометацію.

2. Налаштування WPA3-Enterprise (з використанням сервера RADIUS): - WPA3-Enterprise призначений для великих організацій та підприємств, де потрібен високий рівень безпеки та централізоване керування автентифікацією користувачів. Він використовує стандарт IEEE 802.1X для автентифікації кожного користувача окремо, зазвичай через сервер RADIUS (Remote Authentication Dial-In User Service).

- компоненти WPA3-Enterprise:

- Supplicant – це клієнтський пристрій, що запитує доступ до мережі;

- Authenticator – це точка доступу, яка виступає посередником між клієнтом та сервером автентифікації;
- Authentication Server – це сервер, що перевіряє облікові дані користувача та дозволяє або забороняє доступ.

3. Конфігурація Enhanced Open (OWE - Opportunistic Wireless Encryption): - Enhanced Open (також відоме як Wi-Fi Certified Enhanced Open™) призначене для підвищення безпеки відкритих (незахищених паролем) Wi-Fi мереж, таких як гостьові мережі в кафе, аеропортах тощо. OWE забезпечує шифрування трафіку між кожним клієнтом та точкою доступу, запобігаючи пасивному прослуховуванню, навіть без використання пароля. OWE не забезпечує автентифікацію, тобто не перевіряє, хто підключається до мережі, але захищає дані в процесі передачі.

4. Налаштування додаткових параметрів безпеки:

- фаєрвол (Firewall):

- вбудований фаєрвол маршрутизатора слід налаштувати для блокування небажаного вхідного трафіку з Інтернету.
- якщо створюються різні SSID, фаєрвол може використовуватися для ізоляції трафіку між цими сегментами мережі.

- фільтрація MAC-адрес (MAC Address Filtering):

- дозволяє створити «білий» або «чорний» список MAC-адрес пристроїв, яким дозволено або заборонено підключатися до мережі;

- фільтрація MAC-адрес є слабким заходом безпеки, оскільки MAC адреси легко підробити (MAC spoofing);

- ізоляція клієнтів (Client Isolation / AP Isolation):

- якщо ця функція увімкнена на точці доступу, забороняє безпроводовим клієнтам, підключеним до однієї ТД, безпосередньо обмінюватися даними один з одним;

- може блокувати роботу деяких додатків, що вимагають прямого зв'язку між пристроями в локальній мережі;

- Захист керуючих кадрів (Protected Management Frames - PMF, або MFP - Management Frame Protection):

- WPA3 вимагає використання PMF (стандарт IEEE 802.11w). PMF захищає важливі керуючі кадри Wi-Fi.

- регулярне оновлення прошивок, є критично важливо підтримувати прошивки маршрутизатора та точок доступу в актуальному стані для отримання останніх виправлень безпеки.

- налаштування та регулярний перегляд системних журналів на маршрутизаторі та точках доступу може допомогти виявити підозрілу активність або спроби несанкціонованого доступу.

У таблиці 3.3 продемонстровано порівняння режимів безпеки за різними характеристиками.

Таблиця 3.3 – Порівняння режимів безпеки WPA3

Характеристика	WPA3-Personal (SAE)	WPA3-Enterprise (802.1X)	Enhanced Open (OWE)
Цільове використання	Домашні мережі, малі офіси	Корпоративні мережі, великі організації	Публічні, гостьові мережі (без пароля)
Автентифікація	Спільний пароль (стійкий до офлайн атак)	Індивідуальні облікові дані (сервер RADIUS, EAP)	Відсутня (тільки шифрування)
Шифрування	AES-CCMP (128-bit)	AES-CCMP (128-bit), опціонально GCMP 256 (192-bit mode)	AES-CCMP (на основі Діффі-Геллмана)
Захист від підбору пароля	Високий (завдяки SAE)	Високий (залежить від політик паролів та EAP-методів)	Не застосовується (немає пароля)
Захист керуючих кадрів (PMF)	Обов'язковий	Обов'язковий	Опціональний (рекомендований, якщо підтримується ТД OWE)
Складність налаштування	Середня	Висока (потребує сервера RADIUS)	Низька
Основна перевага	Значно покращена безпека пароля порівняно з WPA2- PSK	Централізована автентифікація, індивідуальні ключі	Шифрування трафіку у відкритих мережах

Впровадження WPA3 разом із додатковими заходами безпеки створює надійний захист безпроводової мережі від більшості сучасних загроз.

3.5 Інтеграція безпроводової мережі з існуючою дротовою інфраструктурою

У більшості випадків новостворена безпроводова мережа повинна бути інтегрована з вже існуючою дротовою локальною обчислювальною мережею (ЛОМ) для забезпечення доступу до спільних ресурсів, серверів та Інтернету. 1. Фізичне підключення:

- Як описано в підрозділі 3.1, точки доступу підключаються до портів

комутаторів існуючої дротової мережі. Якщо ТД підтримують PoE, а комутатори забезпечують живлення PoE, це спрощує розгортання, усуваючи необхідність в окремих блоках живлення для ТД.

- Маршрутизатор, що обслуговує безпроводову мережу (якщо він окремий від основного шлюзу дротової мережі), також підключається до дротової інфраструктури.

2. IP-адресація та DHCP:

- Єдиний простір IP-адрес: Найпростіший варіант – використання єдиного простору IP-адрес та одного DHCP-сервера (зазвичай на головному маршрутизаторі або виділеному сервері) як для дротових, так і для безпроводових клієнтів. Це дозволяє всім пристроям легко взаємодіяти між собою.

- Окремі підмережі (VLAN): Для підвищення безпеки та керованості, особливо в корпоративних мережах, рекомендується розділяти трафік безпроводових клієнтів від трафіку дротових клієнтів за допомогою віртуальних локальних мереж (VLAN).

- Кожному SSID на точці доступу може бути призначений окремий VLAN ID. - Порти комутатора, до яких підключені ТД, налаштовуються як транкові (tagged ports), що дозволяють передавати трафік кількох VLAN. - Для кожного VLAN потрібен свій DHCP-сервер або окремий діапазон (scope) на центральному DHCP-сервері.

- Маршрутизатор повинен підтримувати маршрутизацію між VLAN (inter VLAN routing), якщо потрібна взаємодія між пристроями з різних VLAN, та мати налаштовані правила фаєрволу для контролю цього трафіку.

На рисунку 3.4 продемонстрована умовна схема інтеграції з використанням VLAN:

Рисунок 3.4 – Інтеграція безпроводової мережі з використанням VLAN 3.

Налаштування DNS:

- Безпроводові клієнти повинні отримувати адреси DNS-серверів (через DHCP), які можуть розв'язувати як внутрішні імена ресурсів дротової мережі (якщо такі є), так і зовнішні інтернет-імена. Зазвичай це DNS-сервери, що використовуються в дротовій мережі (наприклад, DNS-сервер контролера домену або внутрішній DNS-сервер компанії).

4. Доступ до спільних ресурсів:

- Після коректного налаштування IP-адресації, маршрутизації та DNS, безпроводові клієнти (залежно від правил фаєрволу та політик VLAN) зможуть отримувати доступ до спільних файлових серверів, принтерів, баз даних та інших

ресурсів, доступних у дротовій мережі.

- Якщо використовується WPA3-Enterprise з автентифікацією через RADIUS, який інтегрований, наприклад, з Active Directory, то права доступу до ресурсів можуть базуватися на облікових записах користувачів.

5. Управління та моніторинг:

- Якщо в дротовій мережі використовується система централізованого управління мережевим обладнанням (NMS - Network Management System) або контролер WLAN, точки доступу слід інтегрувати в цю систему. Це дозволить централізовано моніторити стан ТД, збирати статистику, оновлювати прошивки та керувати конфігураціями.

6. Забезпечення якості обслуговування (QoS):

- Для забезпечення належної якості роботи критично важливих додатків (наприклад, VoIP, відеоконференцзв'язок) як у дротовій, так і в безпроводовій мережі, необхідно налаштувати механізми QoS. Це може включати пріоритезацію трафіку на основі типу додатку, SSID, VLAN або IP-адреси. WMM (Wi-Fi Multimedia) є стандартом, який забезпечує базові функції QoS у безпроводових мережах і повинен бути увімкнений на ТД.

Інтеграція безпроводової мережі WPA3 з існуючою дротовою інфраструктурою вимагає ретельного планування мережевої топології, IP-адресації та політик безпеки для забезпечення безшовної та безпечної взаємодії всіх пристроїв у мережі.

3.6 Висновки до розділу 3

У третьому розділі дипломної роботи було детально розглянуто практичні аспекти реалізації та конфігурації безпроводової мережі з підтримкою стандарту безпеки WPA3. Було охоплено весь життєвий цикл розгортання мережі, починаючи

від фізичного встановлення обладнання і закінчуючи його тонким налаштуванням та інтеграцією.

Ключові етапи та результати, представлені в розділі:

1. Встановлення та підключення обладнання: Описано важливість правильного планування розміщення точок доступу та маршрутизатора, їх фізичного монтажу, забезпечення живлення (включаючи PoE) та коректного кабельного підключення. Наголошено на необхідності перевірки фізичних з'єднань для уникнення проблем на наступних етапах.

2. Початкова конфігурація: Деталізовано процес первинного доступу до інтерфейсів керування мережевими пристроями, зміни стандартних облікових даних, налаштування базових параметрів маршрутизатора (WAN, DHCP, час) та точок доступу (IP-адресація, режим роботи). Підкреслено важливість оновлення прошивок обладнання.

3. Налаштування безпроводової мережі: Розглянуто вибір оптимального режиму роботи (інфраструктурний), конфігурацію SSID з урахуванням рекомендацій щодо безпеки та зручності, а також критично важливі аспекти вибору радіочастотних каналів та регулювання потужності сигналу для забезпечення стабільного покриття та мінімізації інтерференції.

4. Детальна конфігурація безпеки WPA3: Це ядро розділу, де докладно описано налаштування трьох основних режимів WPA3:

- WPA3-Personal (SAE) продемонстровано його переваги для домашніх та малих офісних мереж завдяки стійкості до офлайн-атак на пароль. - WPA3-Enterprise описано його застосування в корпоративному середовищі з використанням сервера RADIUS для індивідуальної автентифікації користувачів та можливості застосування 192-бітного режиму безпеки.

- Enhanced Open (OWE) розглянуто як засіб шифрування трафіку у відкритих гостьових мережах без необхідності введення пароля, що підвищує приватність користувачів. Також було акцентовано увагу на додаткових заходах безпеки, таких як налаштування фаєрволу, ізоляції клієнтів та обов'язковості використання Protected Management Frames (PMF).

5. Інтеграція з дротовою інфраструктурою: Показано методи інтеграції безпроводової мережі з існуючою дротовою мережею, включаючи питання IP

адресації, використання VLAN для сегментації трафіку, налаштування DNS, забезпечення доступу до спільних ресурсів та важливість QoS.

Практичне виконання кроків, описаних у цьому розділі, дозволяє створити сучасну, швидку та, що найголовніше, безпечну безпроводову мережу, захищену передовим стандартом WPA3. Успішна реалізація цих налаштувань є фундаментом для надійної експлуатації мережі та захисту даних користувачів. Подальші розділи можуть бути присвячені тестуванню продуктивності та безпеки створеної мережі, а також аналізу отриманих результатів.

ВИСНОВКИ

У межах виконаної кваліфікаційної роботи було детально досліджено та реалізовано повний цикл створення сучасної безпроводової мережі з акцентом на високий рівень безпеки шляхом впровадження стандарту WPA3. Проведене дослідження охопило теоретичні засади, проектування, вибір обладнання, практичну реалізацію та налаштування безпекових параметрів, що дозволило досягти поставленої мети – створити надійну, масштабовану та захищену Wi-Fi інфраструктуру для корпоративного середовища.

У теоретичній частині роботи було проведено огляд еволюції технологій бездротового зв’язку, починаючи зі стандарту 802.11 та закінчуючи Wi-Fi 6 (802.11ax), який забезпечує підвищену швидкість, надійність та ефективність у високонавантажених середовищах. Особливу увагу приділено аналізу еволюції протоколів безпеки – від WEP до сучасного WPA3, який суттєво покращує захист користувацьких та корпоративних даних завдяки таким технологіям як SAE, Forward Secrecy, 192-бітне шифрування та шифрування в публічних мережах (OWE).

У проектній частині було сформульовано вимоги до мережі на прикладі триповерхової офісної будівлі, розраховано необхідну кількість точок доступу з урахуванням площі, кількості користувачів, типу трафіку та його пікових значень. Обґрунтовано вибір топології мережі на основі контролера (Controller-based WLAN) як найоптимальнішого варіанту для забезпечення централізованого управління та високої безпеки.

У практичній частині було підібрано обладнання, що відповідає сучасним вимогам (Wi-Fi 6, підтримка WPA3), проведено планування логічної структури

мережі із впровадженням VLAN для сегментації користувачів (персонал, гості, IoT пристрої), а також налаштовано IP-адресацію та механізми автентифікації. Особливо важливою стала реалізація WPA3-Enterprise для авторизації користувачів через RADIUS-сервер, що значно підвищує рівень контролю доступу.

Таким чином, виконана кваліфікаційна робота не лише поглибила знання в галузі комп'ютерних мереж, бездротових технологій та інформаційної безпеки, але й дала практичні навички у створенні захищених корпоративних мереж. Запропоновані технічні рішення можуть бути успішно застосовані для побудови реальних Wi-Fi інфраструктур у компаніях, навчальних закладах, бізнес-центрах, забезпечуючи високу продуктивність, надійність та стійкість до сучасних кіберзагроз.

Перспективою подальших досліджень може стати впровадження хмарних рішень для централізованого управління безпроводовими мережами, автоматизованих систем моніторингу та захисту (WIDS/WIPS), а також використання штучного інтелекту для адаптивного керування навантаженням та виявлення аномалій у трафіку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ванхоф, М., Піссенс, Ф., «Атаки повторного встановлення ключів: Примус повторного використання nonce в WPA2,» ACM CCS, 2017.

2. Гаст, М. С., «Безпроводові мережі 802.11: Вичерпний посібник,» O'Reilly Media, 2005.

3. Колеман, Д. Д., Весткотт, Д. А., «CWNA: Офіційний посібник адміністратора безпроводових мереж,» Sybex, 2018.

4. Wi-Fi Alliance, «Wi-Fi 6: Наступне покоління Wi-Fi,» 2019.

5. Cisco Systems, «Технічний опис точок доступу Cisco Catalyst 9100,» 2020. 6. Ubiquiti Networks, «Посібник користувача UniFi 6 Pro,» 2021. 7. MikroTik, «Посібник користувача маршрутизатора hAP ax³,» 2022. 8. O'Ніл, Дж., «Безпека безпроводових мереж: Посібник для початківців,» McGraw-Hill, 2012.

9. RFC 2865, «Служба віддаленої аутентифікації користувачів (RADIUS),» IETF, 2000.

10. IEEE Std 802.1X-2020, «Контроль доступу на основі портів,» IEEE, 2020.

11. Wi-Fi Alliance, «Wi-Fi CERTIFIED Enhanced Open,» 2018.

12. Сталлінгс, В., «Криптографія та безпека мереж: Принципи та практика,» Pearson, 2017.

13. Едні, Дж., Арбо, В. А., «Реальна безпека 802.11: Wi-Fi Protected Access та 802.11i,» Addison-Wesley, 2003.

14. Ekahau, «Посібник з радіообстеження та планування Wi-Fi,» 2020. 15. Cisco Systems, «Посібник з конфігурації контролерів безпроводових мереж,» 2021.

16. Aruba Networks, «Посібник користувача ArubaOS 8.x,» 2020. 17. RFC 7296, «Протокол обміну ключами в Інтернеті версії 2 (IKEv2),» IETF, 2014.

18. NIST SP 800-38D, «Рекомендація для режимів роботи блокового шифру: Galois/Counter Mode (GCM),» NIST, 2007.

19. IEEE Std 802.11w-2009, «Захист керуючих кадрів,» IEEE, 2009. 20. Райт, Дж., Кеш, Дж., «Хакерство безпроводових мереж,» McGraw-Hill, 2015.

21. RFC 5216, «Протокол аутентифікації EAP-TLS,» IETF, 2008. 22. RFC 7542, «Ідентифікатор мережевого доступу,» IETF, 2015. 23. Cisco Systems, «Технічний опис комутаторів Catalyst 9200,» 2021. 24. Juniper Networks, «Посібник з проектування безпроводових мереж,» 2019. 25. Wi-Fi Alliance, «Білий документ про покращення безпеки WPA3,» 2020. 26. Шнайєр, Б., «Прикладна криптографія: Протоколи, алгоритми та вихідний код на C,» Wiley, 2015.

27. RFC 8032, «Алгоритм цифрового підпису на основі кривих Едвардса (EdDSA),» IETF, 2017.

28. Степаненко С. В. Бездротові мережі Wi-Fi 6: проектування і безпека. Харків: Фоліо, 2021.

29. Ковальчук О. М. Безпека комп’ютерних систем та мереж. Львів: Видавництво ЛНУ, 2020.

30. Ubiquiti Inc. UniFi Best Practices for WPA3 Deployment. Ubiquiti Networks, 2021.

31. Павлюк В. В. Комп’ютерні мережі. Основи побудови та функціонування. Київ: Кондор, 2020.

32. Мельничук В. І. Технології комп’ютерних мереж. Львів: Магнолія, 2019. 33. Amazon Web Services. Security Best Practices for WPA3 Networks on AWS. AWS

Whitepaper, 2024.

34. European Union Agency for Cybersecurity (ENISA). Securing Wi-Fi Networks: WPA3 and Beyond. ENISA, 2020.

35. Гриценко В. М. Архітектура комп’ютерних мереж. Київ: Академвидав, 2018.