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)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-ПРОФЕСІЙНОГО СТУПЕНЯ
ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Проектування бездротової мережі Wi-Fi для громадського простору*

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

Здобувач освіти _____ *Данило МАЛЮКА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Артем КУТІН*
(підпис) (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки _____ *Оксана ОСАДЧА*
(підпис) (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)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« *01* » *03* 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

Малюка Данило Павлович
(прізвище, ім'я, по батькові)

1.Тема роботи *Проектування бездротової мережі Wi-Fi для громадського простору*

Керівник роботи *Кутін Артем Ілліч, викладач вищої категорії*
(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 *Об'єкт 1500 м², до 150 користувачів, обладнання Cisco (ISR 2911, 2960, WRT300N), VLAN 10/20/30, DHCP/AAA сервер, Cisco Packet Tracer.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз стандартів Wi-Fi та типових рішень, вибір обладнання; планування топології; створення VLAN і налаштування DHCP; безпека, авторизація; реалізація мережі в Cisco Packet Tracer; тестування продуктивності та оцінка ефективності.

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

резентація Microsoft PowerPoint

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	*Розділ 1. Огляд літератури та аналіз існуючих рішень*	*28.04.2025*	*виконано*
4	*Розділ 2. Аналіз середовища та проєктування мережі Wi-Fi*	*14.05.2025*	*виконано*
5	*Розділ 3. Реалізація моделі в Packet Tracer та оцінка ефективності*	*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 _____ *Данило МАЛЮКА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Артем КУТІН*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 6/5/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Ukrainian national aviation university
Заголовок
Малюка Д.П_3-012_КПІ_123
Автор Науковий керівник / Експерт
Малюка Д.ПКлименко 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.

КП 1

КЦ

25
Довжина фрази для коефіцієнта подібності 2

8404
Кількість слів

66540
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		0
Інтервали		0
Мікропробіли		7
Білі знаки		0
Парафрази (SmartMarks)		12

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	Магістри проф. 2024_4 [redacted] 12/3/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФПМ. К-ра системного програмування і спец. комп'ютерних систем)	14 0.17 %
2	http://ir.nmu.org.ua/bitstream/handle/123456789/154321/%D0%97%D0%B0%D1%81%D1%96%D0%BF%D0%BA%D0%BE.pdf?sequence=1&isAllowed=y	14 0.17 %

РЕФЕРАТ

Кваліфікаційна робота «Проектування бездротової мережі *Wi-Fi* для громадського простору»: 49 сторінок, 6 рисунків, 8 таблиць, 25 використаних літературних джерел.

БЕЗДРОТОВА МЕРЕЖА, *WI-FI, VLAN, CISCO PACKET TRACER,* МАРШРУТИЗАТОР, ТОЧКА ДОСТУПУ, *DHCP, WPA*2, *ROUTER-ON-A-STICK,* МЕРЕЖЕВЕ МОДЕЛЮВАННЯ, СЕГМЕНТАЦІЯ ТРАФІКУ, ТОПОЛОГІЯ ЗІРКА, ГРОМАДСЬКИЙ ПРОСТІР, СИМУЛЯЦІЯ МЕРЕЖІ

У кваліфікаційній роботі досліджено проєктування *Wi-Fi* мережі для багатофункціонального громадського центру в Кривому Розі з метою створення стабільної, безпечної та масштабованої інфраструктури для великої кількості користувачів у різних зонах.

У першому розділі описано технологію *Wi-Fi,* її еволюцію, стандарти (802.11 *a/b/g/n/ac/ax*), проаналізовано приклади впровадження в публічних просторах та типові проблеми проєктування.

У другому розділі проведено аналіз середовища, архітектура об’єкта, кількість користувачів, перешкоди сигналу, юридичні та безпекові аспекти. Вибрано обладнання (точки доступу, маршрутизатор, комутатори, сервер), розраховано кількість точок доступу, обрано гібридну зіркову топологію та сформовано бюджет.

У третьому розділі завдяки *Cisco Packet Tracer* створено модель мережі з трьома *VLAN* (адміністративна, гостьова, конференц-зала), налаштовано *Router-on a-Stick, DHCP* та точки доступу з *WPA2*. Тестування підтвердило стабільне покриття, розмежування трафіку, централізоване керування та безпеку, що відповідає технічному завданню.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Wi-Fi – Технологія бездротового зв’язку, що базується на стандартах *IEEE* 802.11;

VLAN – Віртуальна локальна мережа;

DHCP – Протокол динамічної конфігурації хоста;

AAA – Аутентифікація, авторизація, облік;

WPA2 – Протокол безпеки бездротових мереж;

Router-on-a-Stick – Метод маршрутизації між *VLAN* за допомогою одного

фізичного інтерфейсу маршрутизатора;

SSID – Ідентифікатор бездротової мережі;

IEEE 802.11 – Набір стандартів для бездротових мереж (*a/b/g/n/ac/ax*); *MU-MIMO* – Багатокористувацький режим із множинним входом і виходом;

OFDMA – Ортогональний частотний розподіл доступу;

QoS – Якість обслуговування;

WLC – Контролер бездротової мережі;

NAT – Трансляція мережевих адрес;

DFS – Динамічний вибір частоти;

PoE – Живлення через Ethernet;

Captive Portal – Веб-інтерфейс для аутентифікації користувачів;

MIMO – Множинний вхід, множинний вихід;

TWT – Цільовий час пробудження;

HTTP – Протокол передачі гіпертексту;

ICMP – Протокол міжмережевих керуючих повідомлень;

IP – Інтернет-протокол;

ВСТУП

У контексті стрімкого розвитку цифрових технологій інформаційні системи набули статусу невід'ємної складової повсякденності. Одним із ключових елементів сучасної цифрової ери є бездротовий доступ до мережі Інтернет, що забезпечує користувачам мобільність, зручність у використанні та оперативний обмін даними. Технологія *Wi-Fi*, що функціонує на основі стандартів *IEEE* 802.11, отримала широке поширення завдяки своїй ефективності та економічній доцільності, трансформувавшись у базову платформу мережевої інфраструктури в приватних, комерційних та публічних локаціях.

Значущість представленого дипломного дослідження визначається зростаючими вимогами споживачів до забезпечення якісного бездротового зв'язку у громадських просторах, включаючи бібліотеки, паркові зони, освітні та торговельні комплекси, а також інші місця масового перебування людей. Сучасні користувачі очікують надійного з'єднання, високої швидкості передачі даних та безпечного доступу до глобальної мережі. Це обумовлює виникнення низки інженерних завдань

при проєктуванні бездротових мереж, що вимагають врахування специфіки просторового розміщення, інтенсивності трафіку від значної кількості одночасних підключень, наявності джерел електромагнітних завад та необхідності дотримання чинних технічних регламентів.

Центральним завданням даної дипломної роботи є розробка проєктної документації бездротової мережі стандарту *Wi-Fi* для конкретного об'єкта публічного призначення із застосуванням програмного забезпечення для мережевого моделювання *Cisco Packet Tracer*. В рамках дослідження передбачається здійснення технічного аналізу потреб користувачів, обґрунтований вибір оптимальних апаратних засобів, розробка структурної схеми мережі та верифікація її функціональних характеристик.

Для реалізації поставленої мети необхідно виконати наступні кроки: -

вивчення новітніх *Wi-Fi* технологій та стандартизації;

- аналіз специфіки розміщення мережі у громадському середовищі;

- вибір та обґрунтування мережевих компонентів;

- розробка мережевої моделі за допомогою *Packet Tracer*;

- аналіз продуктивності запропонованого рішення.

Об'єктом даного наукового дослідження є процес формування інфраструктури бездротового доступу в публічному просторі, а його предметом виступають методологічні підходи, технічні засоби та інженерні рішення, що застосовуються при проєктуванні подібних мереж.

Структура дипломної роботи включає три основні розділи, які послідовно розкривають теоретичні засади дослідження, аналіз особливостей середовища проєктування, етапи розробки проєктної документації, процес моделювання та оцінку ефективності запропонованого рішення. Використання програмного забезпечення *Cisco Packet Tracer* забезпечує можливість симуляції функціонування мережі та аналізу її ключових параметрів без залучення фізичного обладнання.

РОЗДІЛ 1
ОГЛЯД ЛІТЕРАТУРИ ТА АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

1.1 Основи технології *Wi-Fi*

Wi-Fi — це одна з найпоширеніших технологій бездротового зв'язку, що дозволяє електронним пристроям обмінюватися даними в локальних мережах або підключатися до Інтернету. Хоча *Wi-Fi* є торговою маркою, ця назва стала загальноприйнятою для всіх бездротових мереж, що базуються на стандарті *IEEE* 802.11.

Як працює *Wi-Fi* та які частоти використовує

Передача цифрової інформації в мережах *Wi-Fi* відбувається за допомогою електромагнітних хвиль. Для цього використовуються різні радіочастотні діапазони:

- 2,4 ГГц забезпечує ширше покриття, дозволяючи сигналу долати більші відстані та краще проникати крізь перешкоди. Однак цей діапазон більш схильний до перешкод від інших пристроїв, що може знижувати швидкість та стабільність зв'язку.

- 5 ГГц та 6 ГГц (у стандарті *Wi-Fi* 6*E*) мають меншу зону дії, оскільки сигнал гірше проникає крізь перешкоди. Проте, вони дозволяють досягти вищих швидкостей передачі даних та більшої стабільності зв'язку завдяки меншій кількості перешкод та більшій пропускній здатності.

Компоненти та безпека *Wi-Fi* мереж

Типова *Wi-Fi* мережа складається з клієнтських пристроїв, таких як смартфони чи ноутбуки, які підключаються до точок доступу. Точки доступу, у свою чергу, з'єднуються з маршрутизаторами та комутаторами, що забезпечують підключення до інших мереж та Інтернету. Сервери у мережі надають такі послуги, як автоматичне присвоєння *IP*-адрес (*DHCP*), перетворення доменних імен (*DNS*) та аутентифікація користувачів. Для великих мереж часто використовуються

контролери бездротової мережі (*WLC*) або хмарні системи адміністрування для централізованого управління.

Для захисту даних у мережах *Wi-Fi* використовуються різні протоколи безпеки. До них належать застарілий *WEP*, а також більш сучасні та надійні *WPA, WPA*2 і *WPA*3, який є найновішим стандартом. Аутентифікація користувачів може реалізовуватись через *Captive Portal* (гостьовий портал), *MAC*-фільтрацію або сегментацію мережі за допомогою *VLAN* для підвищення безпеки та управління доступом.

1.2 Існуючі стандарти (802.11 *a/b/g/n/ac/ax*)

Технологія *Wi-Fi* постійно розвивається, і її стандарти регулярно оновлюються. Це робиться для того, щоб покращити швидкість передачі даних, підвищити енергоефективність та забезпечити підтримку великої кількості одночасно підключених пристроїв.

Основні стандарти *Wi-Fi* та їх еволюція

Історія розвитку *Wi-Fi* позначена появою кількох ключових стандартів, кожен з яких приносив значні покращення:

- 802.11*a* (1999); Цей стандарт працював у діапазоні 5 ГГц, забезпечуючи швидкість до 54 Мбіт/с. Він відрізнявся меншою схильністю до перешкод порівняно з 2,4 ГГц, але мав менший радіус дії та вищу вартість обладнання. Через несумісність з 802.11*b* і дорожнечу, він не набув широкого поширення.

- 802.11*b* (1999); Це був один з перших широко поширених стандартів, що працював у діапазоні 2,4 ГГц з максимальною швидкістю до 11 Мбіт/с. Він був простим і недорогим, але мав низьку стійкість до перешкод.

- 802.11*g* (2003); Також працював на 2,4 ГГц, але підвищив максимальну швидкість до 54 Мбіт/с, зберігаючи зворотну сумісність з 802.11*b*. Це забезпечило значне покращення продуктивності.

- 802.11*n* (*Wi-Fi* 4, 2009); Цей стандарт став революційним, оскільки вперше дозволив використовувати обидва діапазони — 2,4 ГГц та 5 ГГц. Він підтримував

технологію *MIMO* (*Multiple-Input, Multiple-Output*) та розширення каналу до 40 МГц, що дозволило досягти швидкості до 600 Мбіт/с.

- 802.11*ac* (*Wi-Fi* 5, 2013); Фокусуючись переважно на діапазоні 5 ГГц, цей стандарт значно збільшив пропускну здатність до 6,9 Гбіт/с. Він впровадив такі технології, як *MU-MIMO* (*Multi-User MIMO*) та *Beamforming*, що дозволило більш ефективно передавати дані до кількох пристроїв одночасно.

- 802.11*ax* (*Wi-Fi* 6, 2019); Найновіший і найсучасніший стандарт, який працює у всіх трьох діапазонах — 2,4 ГГц, 5 ГГц і 6 ГГц. Його головна мета — підвищити ефективність у середовищах з високою щільністю пристроїв, таких як стадіони чи конференц-зали. Він забезпечує швидкість до 9,6 Гбіт/с завдяки таким технологіям, як *OFDMA* (*Orthogonal Frequency-Division Multiple Access*) та значно покращує

енергоефективність пристроїв.

Ці постійні оновлення стандартів забезпечують стабільне зростання продуктивності *Wi-Fi* мереж. Це, своєю чергою, дозволяє ефективно проєктувати та розгортати бездротові рішення для найрізноманітніших потреб, включно з великими громадськими просторами. Основні характеристики стандартів наведено в таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика стандартів *Wi-Fi*

Стандарт	Частота	Максимальна швидкість	Основні технології	Призначення
802.11*a*	5 ГГц	54 Мбіт/с	*OFDM*	Професійне застосування на старті *Wi-Fi*
802.11*b*	2.4 ГГц	11 Мбіт/с	*DSSS*	Домашні мережі
802.11*g*	2.4 ГГц	54 Мбіт/с	*OFDM*	Розширення *b*
802.11*n*	2.4/5 ГГц	600 Мбіт/с	*MIMO*	Багатоцільове використання
802.11*ac*	5 ГГц	6,9 Гбіт/с	*MU-MIMO, Beamforming*	Високопродуктивні мережі
802.11*ax*	2.4/5/6 ГГц	9,6 Гбіт/с	*OFDMA, TWT*	Громадські простори

1.3 Приклади реалізації в подібних громадських просторах

У багатьох містах та організаціях зараз активно впроваджуються сучасні *Wi Fi* мережі, що надають публічний доступ до інтернету. Це дозволяє забезпечити зв'язок у різноманітних громадських просторах.

Приклади розгортання публічних *Wi-Fi* мереж

Такі мережі можна знайти в різних місцях:

- транспортні вузли; Наприклад, Центральний вокзал Мюнхена обладнаний

більш ніж 50 точками доступу, які одночасно можуть обслуговувати до 5000 користувачів, забезпечуючи зв'язок для пасажирів.

- університети; Великі освітні заклади, такі як Київський політехнічний інститут (КПІ) або Массачусетський технологічний інститут (*MIT*), мають повне *Wi-Fi* покриття в гуртожитках та аудиторіях. Управління такими мережами часто здійснюється централізовано через *Radius*-сервери для автентифікації та *VLAN* для сегментації трафіку.

- парки та бібліотеки; Наприклад, парк імені Шевченка в Києві пропонує *Wi Fi* з захистом *WPA*2, де мережа розділена для доступу персоналу та окремо для відвідувачів. Це забезпечує безпеку та зручність використання.

- торгові центри; У великих торгових комплексах, таких як *Ocean Plaza* чи *Galeria Krakowska*, *Wi-Fi* мережі не тільки надають доступ до інтернету, але й використовуються для аналітики руху користувачів та інтеграції з системами управління відносинами з клієнтами (*CRM*). Це дозволяє покращити обслуговування та маркетинг.

- малі громади; У невеликих населених пунктах *Wi-Fi* часто розгортають у бібліотеках або сільських радах. Для таких проєктів можуть використовуватись бюджетні рішення на базі програмного забезпечення *OpenWRT*, що робить бездротовий доступ доступним для ширшого кола людей.

1.4 Проблеми, які виникають при проєктуванні публічних мереж

Проєктування *Wi-Fi* мереж для громадських просторів має чимало викликів, адже необхідно врахувати безліч факторів, щоб забезпечити надійну та швидку роботу.

Основні проблеми при проєктуванні *Wi-Fi* мереж у громадських місцях

Існує кілька ключових аспектів, які необхідно брати до уваги:

- масове навантаження; У громадських місцях очікується, що до мережі одночасно підключатиметься велика кількість користувачів. Щоб впоратися з таким навантаженням, необхідно використовувати сучасні стандарти *Wi-Fi*, такі як 802.11*ax* (*Wi-Fi* 6), які підтримують технології *MU-MIMO* (*Multi-User, Multiple Input, Multiple-Output*) та *OFDMA* (*Orthogonal Frequency-Division Multiple Access*). Це дозволяє ефективно розподіляти пропускну здатність між багатьма пристроями.

Також важливим є грамотне планування каналів, щоб уникнути їх перевантаження.

- інтерференція; Бездротові сигнали можуть зазнавати впливу від інших *Wi Fi* мереж поблизу, пристроїв *Bluetooth*, а також побутової техніки, наприклад, мікрохвильових печей. Ці перешкоди можуть суттєво знижувати якість зв'язку та швидкість.

- сліпі зони; Будівлі, особливо з бетонними, металевими або скляними конструкціями, можуть створювати "сліпі зони", де *Wi-Fi* сигнал є слабким або повністю відсутнім. Для виявлення таких місць та оптимізації розміщення точок доступу необхідне ретельне зондування (*site survey*).

- захист даних; Публічні *Wi-Fi* мережі наражаються на ризики, такі як атаки "людина посередині" (*man-in-the-middle*), коли зловмисник перехоплює трафік, або клонування точок доступу. Для мінімізації цих загроз потрібно використовувати сучасні протоколи безпеки, зокрема *WPA*3, впроваджувати *Captive Portal* для аутентифікації користувачів та застосовувати технологію *VLAN* для логічної сегментації мережі.

- обмеження інтернет-каналу; Якщо пропускна здатність основного інтернет каналу є недостатньою для всіх користувачів, це може призвести до уповільнення

роботи мережі. Для вирішення цієї проблеми важливо впроваджувати *QoS* (*Quality of Service*) для пріоритезації трафіку, використовувати кешування часто запитуваних даних та встановлювати обмеження швидкості для окремих користувачів або груп.

- складність адміністрування; Управління великою *Wi-Fi* мережею з багатьма точками доступу та користувачами може бути дуже складним. Тому для спрощення налаштування, моніторингу та обслуговування рекомендується використовувати системи централізованого управління, такі як контролери бездротової мережі (*WLC*) або хмарні платформи адміністрування.

- обмежений бюджет; Часто проєктування публічних *Wi-Fi* мереж стикається з бюджетними обмеженнями. У таких випадках можна розглядати використання більш економічних апаратних рішень та програмного забезпечення на основі відкритих операційних систем, таких як *OpenWRT*, які пропонують широкі функціональні можливості за меншу вартість.

Ретельне врахування всіх цих факторів під час проєктування та розгортання є ключовим для забезпечення ефективного функціонування публічної бездротової

мережі, яка буде відповідати потребам користувачів та забезпечувати необхідний рівень безпеки. Узагальнена інформація щодо проблем проєктування наведена в таблиці 1.2.

Таблиця 1.2 – Типові проблеми проєктування та відповідні рішення

Проблема	Причина	Рекомендоване рішення
Велике навантаження	Багато одночасних підключень	*MU-MIMO, QoS*, розподіл по *VLAN*
Інтерференція	*Bluetooth*, мікрохвильові прилади	Канали *DFS*, 5/6 ГГц, автоматичний вибір
Сліпі зони	Бетон, скло, метал	*Site survey*, більше точок доступу
Ризики безпеки	Відкрите середовище	*WPA*3, авторизація, сегментація
Нестача пропускної здатності	Слабкий інтернет-канал	Кешування, обмеження швидкості, *QoS*
Складне адміністрування	Розподілення точки доступу	Централізоване управління (*WLC*, хмара)
Обмежений бюджет	Вартість обладнання	Відкриті ОС (*OpenWRT*), бюджетні рішення
Нестабільність покриття	Незбалансоване розміщення точок	Радіопланування, перекриття зон
Погане масштабування	Примітивна архітектура мережі	Проєктування з урахуванням росту

РОЗДІЛ 2
АНАЛІЗ СЕРЕДОВИЩА ТА ПРОЄКТУВАННЯ МЕРЕЖІ

2.1 Характеристика громадського простору

Завдання полягає в розробці Wi-Fi мережі для багатофункціонального громадського центру в центрі Кривого Рогу. Об’єкт має площу 1500 м², два поверхи, побудований із армованого бетону, скла та металевих конструкцій, обладнаний сучасними інженерними системами.

Особливості функціональних зон та вимоги до *Wi-Fi*

Центр поділений на три основні функціональні зони, кожна з яких має свої унікальні вимоги до бездротового зв'язку:

- адміністративна зона; Тут працює персонал центру, тому для цієї частини критично важливими є стабільне та безпечне з'єднання. Працівникам потрібен надійний доступ до внутрішніх ресурсів та інтернету без перебоїв, а також високий рівень захисту даних.

- гостьова зона – ця зона включає вестибюль, хол та кафе, призначені для відвідувачів. Основна вимога тут — це забезпечення публічного доступу до *Wi-Fi*. При цьому важливо встановити обмеження швидкості для кожного користувача, щоб уникнути перевантаження мережі та забезпечити рівномірний доступ для всіх гостей;

- конференц-зала – це місце проведення публічних заходів, де очікується одночасне підключення великої кількості пристроїв. Тому для конференц-зали потрібна висока пропускна здатність мережі, яка зможе впоратися з піковими навантаженнями під час презентацій, відеоконференцій або інших інтерактивних подій (рисунок 2.1);

Рисунок 2.1 – Схематичне зонування простору громадського центру

2.2 Кількість потенційних користувачів

Для ефективного проєктування *Wi-Fi* мережі в багатофункціональному

громадському центрі в Кривому Розі першочерговим кроком є ретельна оцінка потенційного навантаження. Ця оцінка ґрунтується на детальному аналізі типових сценаріїв використання кожної функціональної зони об'єкта.

Детальна оцінка очікуваного навантаження на мережу за функціональними зонами

Розглянемо очікувану кількість пристроїв та характер їх використання у кожній із трьох основних зон центру:

- адміністративна зона; У цій частині центру передбачається робота до 20 співробітників одночасно. Кожен з них використовуватиме декілька пристроїв, таких як стаціонарні комп'ютери або ноутбуки, смартфони та, можливо, підключені до мережі принтери. Для цієї зони критично важливо забезпечити стабільну та безперебійну роботу мережі, оскільки вона є основою для доступу до офісних застосунків, внутрішніх ресурсів та виконання повсякденних робочих завдань. Перебої зі зв'язком тут можуть суттєво вплинути на продуктивність.

- гостьова зона; До цієї зони належать зони очікування, хол та кафе. Очікується, що тут одночасно перебуватиме до 50 відвідувачів. Більшість з них підключатимуться до *Wi-Fi* зі своїх мобільних пристроїв (смартфонів, планшетів) та, можливо, особистих ноутбуків. Основне використання мережі в цій зоні – це веб-серфінг, перегляд соціальних мереж, використання месенджерів та легкі онлайн-ігри. Тому мережа має забезпечувати достатню пропускну здатність для комфортного доступу до Інтернету для всіх відвідувачів, враховуючи при цьому, що активність користувачів тут буде більш спонтанною та різноманітною.

- конференц-зала; Ця зона призначена для проведення різноманітних публічних заходів, таких як презентації, семінари, тренінги чи відеоконференції. Під час цих подій тут може зібратися до 80 учасників. Кожен учасник, ймовірно, підключатиме один або кілька пристроїв, таких як ноутбуки, планшети чи смартфони, для доступу до матеріалів презентацій, участі в інтерактивних опитуваннях, перегляду відео або взаємодії з онлайн-ресурсами. Це вимагає від мережі забезпечення дуже високої пропускної здатності та низьких затримок, щоб гарантувати стабільне підключення для великої кількості пристроїв, які одночасно інтенсивно використовують мережеві ресурси.

Загалом, проєктована *Wi-Fi* мережа повинна бути розрахована на одночасне

обслуговування до 150 пристроїв, враховуючи пікові навантаження в кожній із зон. Дуже важливо передбачити можливість подальшого масштабування мережі, щоб вона могла адаптуватися до зростання кількості відвідувачів та нових потреб у майбутньому. При плануванні необхідно ретельно проаналізувати очікувані типи трафіку: це може бути веб-серфінг, потокове відео високої якості, голосовий зв'язок через Інтернет (*VoIP*), активний обмін великими файлами тощо. Планування має базуватися на найвищому очікуваному (піковому) навантаженні, передбачаючи відповідний резерв пропускної здатності та ресурсів мережі. Це дозволить забезпечити безперебійну та ефективну роботу *Wi-Fi* навіть у моменти найбільшої активності користувачів, гарантуючи високу якість послуг. Узагальнений розподіл користувачів за функціональними зонами наведено в таблиці 2.1.

Таблиця 2.1 – Розподіл користувачів за зонами об’єкта

Зона	Кількість користувачів	Типові пристрої	Пікове навантаження (*Mbps*)
Адміністративна	20	ПК, принтери, телефони	40
Гостьова	50	Смартфони, ноутбуки	100
Конференц-зала	80	Планшети, відеопотоки	200
Загалом	150	-	340

2.3 Перешкоди, джерела шуму

На якість функціонування *Wi-Fi* мережі у цьому громадському центрі в Кривому Розі суттєво впливають особливості навколишнього середовища. Тому при проєктуванні системи необхідно ретельно врахувати джерела потенційних перешкод.

Фактори, що впливають на *Wi-Fi* сигнал у приміщенні та стратегії їх подолання

Серед найбільш значущих джерел перешкод виділяють:

- бетонні стіни та перекриття; Ці елементи конструкції, характерні для сучасних будівель, є значними поглиначами радіосигналу. Їхній вплив особливо помітний у діапазоні 5 ГГц, де сигнал гірше проникає крізь щільні матеріали. Це

може призводити до появи "сліпих зон" з низьким або відсутнім покриттям *Wi-Fi*.

- металеві елементи конструкції; Метал не тільки поглинає радіохвилі, але й спричиняє їх активне відбиття. Це явище, відоме як багаторазові інтерференції або багатопроменеве поширення, може призвести до того, що сигнал досягатиме приймача різними шляхами з різними затримками, що викликає нестабільність зв'язку, зниження швидкості та непередбачувані "провали" в роботі мережі.

- побутова техніка; Пристрої, такі як мікрохвильові печі, а також *Bluetooth* пристрої, які працюють у тому ж діапазоні 2,4 ГГц, що й *Wi-Fi*, створюють локальні радіозавади. Ці завади можуть перешкоджати нормальній роботі *Wi-Fi* мережі, викликаючи конфлікти каналів та зниження пропускної здатності.

- скляні перегородки; Попри свою прозорість, скляні елементи конструкції, особливо ті, що мають спеціальні покриття, можуть частково змінювати напрямок сигналу та спричиняти певні втрати його потужності. Це може впливати на якість покриття та вимагає врахування при плануванні розміщення точок доступу.

Для мінімізації впливу цих завад та забезпечення оптимального, стабільного та якісного покриття *Wi-Fi*, необхідно провести комплексний підхід, що включає: - радіопланування (*site survey*); Це ключовий етап, що включає детальне вимірювання рівня сигналу в різних точках об'єкта, виявлення зон з низьким покриттям та аналіз джерел перешкод. На основі цих даних визначаються оптимальні місця для розміщення точок доступу, їх потужність та орієнтація. Застосування технологій боротьби з перешкодами:

- використання каналів *DFS* (*Dynamic Frequency Selection*) – ця функція дозволяє точкам доступу автоматично виявляти та уникати каналів, які використовуються іншими пристроями (наприклад, радарами), забезпечуючи вибір менш завантажених та вільних частот;

- автоматична зміна робочих частот – сучасне *Wi-Fi* обладнання здатне автоматично змінювати робочі канали або діапазони при виявленні значних завад, що дозволяє підтримувати стабільний зв'язок;

- використання обладнання з підтримкою *Beamforming* – ця технологія дозволяє точкам доступу "фокусувати" *Wi-Fi* сигнал безпосередньо у напрямку пристрою користувача, замість того, щоб розсіювати його в усі сторони. Це не тільки підвищує стабільність зв'язку та швидкість передачі даних, але й значно ефективніше

використовує потужність сигналу.

Ретельне врахування цих факторів та застосування відповідних технологій є запорукою успішного проєктування та функціонування високоякісної *Wi-Fi* мережі в громадському центрі. Основні джерела інтерференції в середовищі наведено в таблиці 2.2.

Таблиця 2.2 – Джерела перешкод у середовищі розгортання мережі

Джерело перешкод	Вплив на сигнал	Зона впливу	Рекомендації
Бетонні стіни	Послаблення, поглинання	Вся будівля	Розміщення точок поблизу
Металеві конструкції	Відбиття, інтерференція	Перекриття, стелі	*Beamforming*, планування
Побутові прилади (2.4 ГГц)	Локальні завади	Кафе, кухня	Канали *DFS*, зміна діапазону
Скляні перегородки	Відбиття та втрати	Конференц-зала, офіси	Орієнтація антен, дод. точки

2.4 Юридичні та безпекові аспекти (захист даних, авторизація)

У відкритому для широкого загалу громадському просторі, особливо важливо приділити особливу увагу питанням безпеки *Wi-Fi* мережі та дотримання чинного законодавства. Це включає захист даних користувачів та забезпечення відповідального використання мережі.

Безпека *Wi-Fi* та відповідність законодавству у громадському просторі

Ось ключові аспекти, які необхідно врахувати:

- захист персональних даних; Відповідно до Закону України "Про захист персональних даних", реєстрація користувачів у публічній мережі має обов'язково відбуватись із фіксацією певних ідентифікаторів. Це можуть бути *MAC*-адреса пристрою, *IP*-адреса, а також точний час доступу до мережі. Ці дані потрібні для можливих перевірок або розслідувань у разі інцидентів.

- аутентифікація; Для доступу до гостьової зони варто впровадити *Captive Portal*, де користувачі зможуть пройти аутентифікацію за допомогою *SMS* підтвердження, електронної пошти або спеціальних облікових записів. Це допомагає ідентифікувати користувачів. Для персоналу ж, який працює в адміністративній зоні, рекомендується використовувати більш надійні методи

авторизації, такі як сертифікати або протокол *WPA*2-*Enterprise*, що забезпечує високий рівень безпеки.

- шифрування; Для захисту даних, що передаються в гостьовій зоні, варто використовувати сучасний протокол *WPA*3. Він забезпечує посилене шифрування і кращий захист від атак. Для критичних підключень та доступу персоналу (особливо в адміністративній зоні) обов'язковим є застосування *WPA*2-*Enterprise*.

- сегментація мережі; Для підвищення безпеки та ефективності необхідно логічно розділити трафік у мережі за допомогою *VLAN* (*Virtual Local Area Network*). Наприклад, можна створити окремі віртуальні мережі: *VLAN*10 для адміністрації, *VLAN*20 для гостьової зони та *VLAN*30 для конференц-зали. Це дозволяє ізолювати трафік різних груп користувачів та застосовувати до них різні політики безпеки.

- логування активності; Усі журнали доступу та активності користувачів у мережі мають централізовано зберігатися. Це критично важливо у разі виникнення інцидентів безпеки або при проведенні перевірок контролюючими органами, оскільки дозволяє відстежувати, хто, коли і що робив у мережі.

Крім того, необхідно забезпечити правові попередження користувачів про умови використання мережі. Це можна реалізувати через веб-інтерфейс авторизації, де користувачі перед підключенням до *Wi-Fi* зможуть ознайомитися з правилами та погодитися на них. Такий підхід також відповідає загальним вимогам кібергігієни у публічному просторі.

2.5 Вибір обладнання (точки доступу, маршрутизатори, контролери)

Створення ефективної *Wi-Fi* інфраструктури у багатофункціональному центрі потребує комплексного підходу до вибору обладнання, яке забезпечить надійний бездротовий зв’язок у різноманітних просторах — від відкритих зон до офісних приміщень та конференц-залів. Враховуючи змішану архітектуру будівлі та високу

концентрацію користувачів, мережа має бути не лише потужною, але й гнучкою в управлінні та масштабуванні.

Ефективне покриття бездротовою мережею різних зон центру вимагає використання точок доступу з високою пропускною здатністю. Середовище моделювання *Cisco Packet Tracer* надає наступні опції: *Cisco WRT*300*N* (стандартне рішення 802.11*n* для зон з помірним трафіком), *Cisco WAP*371 (оптимальний вибір для просторів з високою щільністю підключень) та *Generic Wireless Router* (базова модель для тестових сценаріїв). Для реального розгортання рекомендуються пристрої серій *Cisco Catalyst* 9100 або *Aironet* 2800/3800, що підтримують стандарти *Wi-Fi* 6, технології *MU-MIMO* та *Beamforming*, а також обладнані підтримкою *PoE* для спрощення процесу інсталяції (рисунок 2.2).

1) 2)

Рисунок 2.2 – Що це 1) *Cisco Aironet* 2800/3800; 2) *Cisco Catalyst* 9100

Для забезпечення надійного підключення до основних та резервних каналів зв’язку багатофункціональний центр потребує високопродуктивного маршрутизатора. У *Packet Tracer* доступний *Cisco ISR* 2911, що забезпечує функціональність *NAT*, *DHCP*, підтримку *VLAN* та *ACL*, гарантуючи стабільне з’єднання з мережею Інтернет та ефективну маршрутизацію між різними сегментами локальної мережі.

Об’єднання компонентів мережі здійснюється за допомогою керованих комутаторів. Для базових конфігурацій підходить *Cisco* 2960, тоді як для складніших топологій з підтримкою міжвланної маршрутизації рекомендується *Cisco* 3560.

Централізоване адміністрування великої кількості точок доступу значно спрощується за наявності контролера бездротової мережі. У *Packet Tracer* повноцінний *WLC* відсутній, що зумовлює необхідність індивідуального

налаштування кожної точки доступу. У реальних мережах для централізованого управління конфігурацією та політиками безпеки рекомендується використовувати *Cisco* 3504 *WLC* (рисунок 2.3).

Рисунок 2.3 – Маршрутизатор (або щось інше) *Cisco* 3504 *WLC*

Для забезпечення автентифікації користувачів та автоматичного розподілу *IP*-адрес необхідний сервер *DHCP*/*AAA*/*RADIUS*. Моделювання навантаження на мережу здійснюється за допомогою різноманітних клієнтських пристроїв, таких як ноутбуки, смартфони та планшети.

Оптимальна конфігурація обладнання для багатофункціонального центру включає: один маршрутизатор *Cisco* 2911, два-три керовані комутатори *Cisco* 2960 (розміщені на різних поверхах будівлі), шість-десять точок доступу *Cisco WAP* (кількість залежить від площі покриття), *DHCP*-сервер для управління *IP* адресацією та не менше десяти клієнтських пристроїв для симуляції мережевого трафіку.

2.6 Розрахунок покриття, розташування точок доступу

Для створення надійного та стабільного бездротового покриття *Wi-Fi* в усіх ключових функціональних зонах громадського простору було використано шість точок доступу *Cisco WRT*300*N*. Ці пристрої обрані завдяки їхній підтримці стандарту *IEEE* 802.11*n*, що забезпечує високу пропускну здатність, а також роботі

в частотному діапазоні 2.4 ГГц, який є поширеним і добре підходить для покриття великих територій. Крім того, вони підтримують сучасне та надійне шифрування

*WPA*2, гарантуючи безпеку передачі даних.

Об'єкт, який охоплює ця мережа, має площу близько 1500 м², включаючи як відкриті простори, так і закриті приміщення. Простір був логічно розділений на кілька основних зон для ефективного розподілу точок доступу:

- вхідна зона та зони очікування; Ця зона, що має помірне навантаження, забезпечується покриттям однією точкою доступу.

- конференц-зали (до 100 осіб); Для цих зон, де очікується висока щільність користувачів та інтенсивний трафік, було виділено дві точки доступу, що гарантує достатню пропускну здатність та стабільне з'єднання під час проведення заходів.

- зони загального користування (кафе, зони відпочинку); Дві точки доступу розміщені тут для забезпечення комфортного доступу до мережі для відвідувачів, що відпочивають або користуються послугами кафе.

- адміністративна частина; Для службових потреб та внутрішніх підключень адміністративного персоналу виділено окрему точку доступу, що дозволяє логічно ізолювати службовий трафік.

Проєктування розміщення точок доступу базувалося на ретельному аналізі технічних характеристик моделі *Cisco WRT*300*N*:

- радіус покриття; Внутрішній радіус покриття однієї точки доступу становить приблизно 25–30 метрів, що стало ключовим фактором при їх розміщенні.

- пропускна здатність; Кожна точка доступу забезпечує пропускну здатність до 150 Мбіт/с на частоті 2.4 ГГц, що є достатнім для більшості повсякденних завдань.

- кількість користувачів; В умовах середньої інтенсивності трафіку, одна точка доступу може ефективно обслуговувати 20–30 користувачів одночасно. Під час планування розміщення точок доступу було враховано наявність різноманітних фізичних перешкод, таких як бетонні перегородки та скляні стіни, які можуть негативно впливати на поширення радіосигналу. Щоб мінімізувати

їхній вплив і уникнути "мертвих зон", точки доступу були розміщені максимально рівномірно, забезпечуючи перекриття зон покриття. Додатково було застосовано частотне планування, що дозволило зменшити інтерференції між сусідніми точками доступу та покращити загальну якість сигналу.

Загалом, ретельний вибір кількості та стратегічне розміщення точок доступу

забезпечують багато ключових переваг. Гарантується стабільний бездротовий зв'язок у всіх функціональних зонах об'єкта. Мережа спроєктована з розрахунком на високе навантаження, що дозволяє одночасно підключати велику кількість пристроїв без значного зниження продуктивності. Використання віртуальних локальних мереж (*VLAN*) забезпечує розмежування трафіку між різними групами користувачів або функціональними зонами, підвищуючи безпеку та ефективність мережі.

Цей підхід забезпечує високу продуктивність, надійність та адаптивність бездротової мережі в умовах громадського простору. Розміщення точок доступу також показано у таблиці 2.3.

Таблиця 2.3 - Розміщення точок доступу за зонами покриття

Зона розміщення	Площа, м²	Кількість користувачів	Кількість точок доступу	Типова активність користувачів
Вхідна зона, зона очікування	200	30–50	1	Перевірка пошти, вебсерфінг
Гостьова зона, кафе	400	80–100	2	Соцмережі, відео, месенджери
Конференц-зали	300	100	2	Онлайн-презентації, стрімінг
Адміністративна частина	200	15–20	1	Робочі застосунки, доступ до сервера
Разом:	≈1100	250–300	6	—

2.7 Вибір топології мережі

Для створення ефективної та керованої локальної мережі у громадському просторі було обрано топологію типу "зірка". Цей вибір є оптимальним, оскільки він забезпечує централізоване управління мережевим трафіком, значно спрощує

обслуговування системи та дозволяє легко масштабувати інфраструктуру в майбутньому.

У фізичній реалізації топології "зірка" всі основні мережеві пристрої централізовано підключаються до комутаторів. Зокрема, всі точки доступу *Cisco WRT*300*N*, сервер, а також численні клієнтські пристрої під'єднуються до

центральних комутаторів *Cisco Catalyst* 2960 *PoE*. Ці комутатори, зі свого боку, з'єднані з основним мережевим пристроєм – маршрутизатором *Cisco ISR* 2911. Така архітектура забезпечує ефективний розподіл мережевого навантаження між пристроями та допомагає мінімізувати затримки (*latency*) при передачі даних, що є критично важливим для великих громадських просторів.

З точки зору логіки роботи, мережа має продуману архітектуру, яка підвищує її безпеку та ефективність:

- застосовано архітектуру *Router-on-a-Stick*, де маршрутизатор підключений до комутатора за допомогою всього одного *trunk*-порту.

- створення віртуальних локальних мереж (*VLAN*): для підвищення безпеки та організації трафіку було створено три окремі *VLAN*, кожна з яких відповідає певній групі користувачів або зоні:

- *VLAN* 10 – виділена для трафіку адміністрації;

- *VLAN* 20 – призначена для гостьового доступу;

- *VLAN* 30 – використовується для потреб конференц-залів.

Кожна з цих *VLAN* має свою унікальну *IP*-підмережу, що забезпечує логічну ізоляцію трафіку:

- *VLAN* 10 використовує підмережу 192.168.10.0/24;

- *VLAN* 20 – 192.168.20.0/24;

- *VLAN* 30 – 192.168.30.0/24.

Таке логічне розділення мережі на *VLAN* та підмережі надає значні переваги: - ізоляція трафіку; Забезпечується повна ізоляція трафіку між різними сегментами мережі. Наприклад, трафік гостей повністю відділений від трафіку адміністрації, що підвищує безпеку.

- підвищення безпеки та стабільності; Розділення зменшує ризик несанкціонованого доступу та запобігає поширенню мережевих проблем між різними сегментами, підвищуючи загальну стабільність системи.

- зручне управління доступом; Адміністратори можуть легко контролювати та управляти доступом до мережевих ресурсів для різних категорій користувачів, застосовуючи відповідні політики безпеки до кожної *VLAN*.

обрана топологія повністю відповідає сучасним вимогам до надійності,

масштабованості та гнучкості мережевої інфраструктури. Вона дозволяє ефективно реалізувати складну систему авторизації та маршрутизації в межах одного об'єкта, забезпечуючи високопродуктивне та безпечне мережеве середовище для всіх користувачів.

2.8 Бюджетування та оцінка вартості

Процес проєктування бездротової мережі охоплює не тільки ретельне технічне обґрунтування, а й детальну оцінку вартості її впровадження. Для цього було розроблено орієнтовний бюджет на основне мережеве обладнання, що використовується в даній моделі. У таблиці 2.4 нижче наведено орієнтовний бюджет на основне обладнання, що використано в моделі. Він дає загальне уявлення про необхідні фінансові вкладення.

Таблиця 2.4 – Бюджет основного обладнання

Найменування обладнання	Кількість	Орієнтовна вартість (*UAH*)
Маршрутизатор *Cisco ISR* 2911	1	35 000 – 50 000грн
Комутатор *Cisco Catalyst* 2960 *PoE*	2	20 000 – 35 000грн
Бездротова точка доступу *Cisco WRT*300*N*	6	9 000 – 15 000грн
Сервер (офісний, *DHCP*/*AAA*)	1	15 000 – 25 000грн
Кабелі, роз’єми, монтажні роботи	-	13 000 – 27 000грн
Ліцензія (якщо необхідно)	-	5 000 – 10 000грн
Всього:	-	97 000 – 162 000грн

Варто зазначити, що представлені у таблиці цифри є орієнтовними. Реальна вартість проєкту може суттєво змінюватися під впливом кількох факторів: - постачальник обладнання та послуг; Ціни можуть відрізнятися залежно від обраного постачальника та його цінової політики.

- тип ліцензійного забезпечення; Вартість може включати додаткові ліцензії на

розширені функції програмного забезпечення та сервісну підтримку, що може збільшити кінцеву суму.

- складність монтажних робіт; Обсяг та складність прокладки кабелів, встановлення обладнання та пусконалагоджувальних робіт напряму впливають на вартість монтажу.

У разі виникнення бюджетних обмежень або потреби в максимальній економії, існують ефективні способи оптимізації витрат без критичного зниження функціональності мережі. На ринку вторинного обладнання можна знайти надійні пристрої попередніх серій *Cisco* або інших виробників за значно нижчою ціною. Важливо лише переконатися в їхній працездатності та відповідності поточним потребам. Для виконання таких завдань, як *DHCP*-сервер або базова автентифікація, можна замінити повноцінний сервер на менш потужні та дорогі мікрокомп'ютери, наприклад, *Raspberry Pi*. Замість комерційних серверних ОС можна застосовувати рішення на базі *Linux*, такі як *Ubuntu Server* або *Debian*. Для реалізації функцій *DHCP* можна використовувати *ISC DHCP Server*, а для автентифікації – *FreeRADIUS*. Це повністю виключає витрати на ліцензування програмного забезпечення. Деякі етапи монтажу та початкового налаштування можуть бути виконані внутрішніми силами (за наявності відповідних фахівців), що дозволить заощадити на вартості підрядних робіт.

Таким чином, проєктна бездротова мережа має адекватну вартість для успішної реалізації у громадському просторі середнього розміру. Гнучкість архітектури та можливість застосування різних оптимізаційних стратегій дозволяють масштабувати або модифікувати мережу відповідно до будь-яких майбутніх потреб або змінюваних бюджетних умов.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ В *PACKET TRACER* ТА ОЦІНКА ЕФЕКТИВНОСТІ

3.1 Опис налаштування

Проєкт у *Cisco Packet Tracer* створено для симуляції *Wi-Fi* мережі багатофункціонального центру, відтворюючи основні компоненти реального середовища з відповідною логічною структурою, категоріями користувачів та

функціональним зонуванням.

Базова архітектура мережі (рисунок 3.1):

- центральний маршрутизатор (*Cisco* 2911) — головний елемент для реалізації маршрутизації між *VLAN*, *NAT* та *DHCP*;

- два комутатори (*Cisco* 2960) — перший забезпечує офісно-адміністративну зону, другий обслуговує конференц-зали та публічні простори; - бездротові точки доступу *Cisco WRT*300*N* (від 6 до 10) — стратегічно розташовані по всій території;

- серверна частина — забезпечує *DHCP* та *AAA* (автентифікація); - користувацькі пристрої — мобільні комп'ютери, планшети, смартфони.

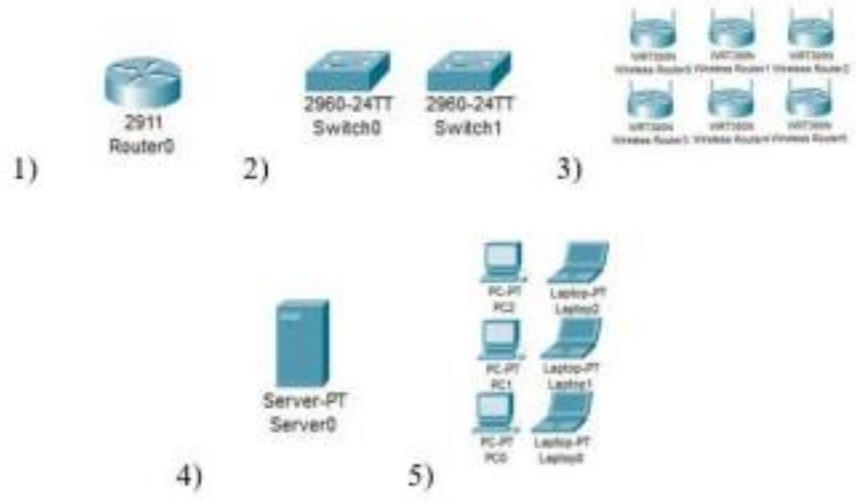

Рисунок 3.1 – Компоненти мережі: 1) Маршрутизатор *Cisco* 2911; 2) Комутатори *Cisco* 2960; 3) Точки доступу *Cisco WRT*300*N*; 4) Сервер; 5) Користувацькі пристрої

Процес налаштування фізичної інфраструктури починається з поєднання основних мережевих компонентів. Точки доступу *Cisco WRT*300*N* підключаються до комутаторів через інтерфейси *FastEthernet* зі стандартною швидкістю 100 Мбіт/с. Важливо відзначити, що технологія *Power over Ethernet* (*PoE*) вважається активною, що дозволяє передавати живлення та дані через один кабель, спрощуючи розгортання точок доступу.

Для забезпечення високої пропускної здатності між ключовими вузлами мережі, комутатори з'єднуються між собою та з центральним маршрутизатором *Cisco* 2911 через інтерфейси *GigabitEthernet* (1 Гбіт/с). Це створює надійну магістраль для ефективної передачі даних між різними сегментами мережі.

На завершальному етапі фізичної структуризації виконується розміщення сервера та приєднання різноманітних клієнтських пристроїв у відповідних функціональних зонах. Сервер підключається безпосередньо до комутатора через високошвидкісний інтерфейс для забезпечення оптимальної продуктивності сервісів автентифікації та *DHCP*.

Для логічної сегментації мережі на комутаторах створюються три окремі віртуальні локальні мережі (*VLAN*), які відповідають функціональному призначенню різних зон:

- *VLAN* 10 призначається для адміністративного персоналу, забезпечуючи підвищений рівень безпеки та пріоритетний доступ до корпоративних ресурсів; - *VLAN* 20 створюється для гостьового доступу, обмежуючи можливості використання внутрішніх ресурсів мережі;

- *VLAN* 30 обслуговує конференц-приміщення, забезпечуючи специфічні потреби для проведення зустрічей та презентацій.

Особлива увага приділяється розподілу фізичних портів комутаторів між створеними *VLAN*. Порти комутаторів конфігуруються як *access* для підключення кінцевих пристроїв або *trunk* для передачі трафіку кількох *VLAN* між комутаторами та маршрутизатором. Кожен порт призначається відповідній *VLAN* згідно з географічним розташуванням та функціональним зонуванням обслуговуваних пристроїв.

Для кожної *VLAN* виділяється окремий діапазон адрес з приватного *IP* простору. *VLAN* 10 (адміністрація) отримує адресний простір 192.168.10.0/24, що дозволяє адресувати до 254 пристроїв. Аналогічно, *VLAN* 20 (гостьовий доступ) використовує мережу 192.168.20.0/24, а *VLAN* 30 (конференц-приміщення) - мережу 192.168.30.0/24.

На маршрутизаторі налаштовується технологія *Router-on-a-Stick*, яка дозволяє здійснювати маршрутизацію між різними *VLAN* через один фізичний інтерфейс. Для цього на маршрутизаторі створюються підінтерфейси для кожної *VLAN* з відповідною інкапсуляцією *IEEE* 802.1*Q* (рисунок 3.2).

```
interface g0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

interface g0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0

interface g0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
```

Рисунок 3.2 – Команди для створення підінтерфейсів *VLAN*

Кожен підінтерфейс отримує *IP*-адресу першого хоста в своєму діапазоні, яка використовуватиметься як шлюз (*gateway*) для пристроїв у відповідній *VLAN*. На сервері налаштовується служба *DHCP* з трьома окремими пулами *IP* адрес: (*Admin_POOL*) для адміністративних пристроїв, (*Guest_POOL*) для

гостьових підключень та (*Conf_POOL*) для пристроїв у конференц-залах. Для кожного пулу визначаються ключові параметри: діапазон доступних *IP*-адрес, адреса шлюзу за замовчуванням (відповідний підінтерфейс маршрутизатора), адреси *DNS*-серверів та домен мережі.

Наприклад, для (*Admin_POOL*) встановлюється діапазон 192.168.10.10-192.168.10.254 із шлюзом 192.168.10.1. Для (*Guest_POOL*) виділяється діапазон 192.168.20.10-192.168.20.254 із шлюзом 192.168.20.1. Аналогічно конфігурується (*Conf_POOL*) з діапазоном 192.168.30.10-192.168.30.254 та шлюзом 192.168.30.1.

Як альтернатива, служба *DHCP* може бути активована безпосередньо на

маршрутизаторі *Cisco* 2911, що спростить архітектуру мережі, але потенційно збільшить навантаження на центральний пристрій маршрутизації.

Для кожної точки доступу *Wi-Fi* виконується комплексне налаштування параметрів безпеки та мережевої інтеграції. Насамперед створюються окремі ідентифікатори мережі (*SSID*) для різних категорій користувачів: (*Center_Admin*) для адміністративного персоналу, (*Center_Guest*) для відвідувачів та (*Center_Conf*) для учасників конференцій.

Безпека бездротових мереж забезпечується технологією *WPA*2 *Personal* з індивідуальними паролями для кожного *SSID*. Для демонстраційних цілей використовується приклад пароля (*wifi*1234), але в реальному середовищі рекомендується застосовувати складні унікальні паролі для кожної мережі.

На рівні *IP*-налаштувань точки доступу можуть отримувати статичні адреси для спрощення адміністрування або динамічні адреси через *DHCP*. Важливим етапом є інтеграція точок доступу з відповідними *VLAN* через порти комутаторів. Порт комутатора, до якого підключена точка доступу з *SSID* (*Center_Admin*), конфігурується як *trunk* з дозволом для *VLAN* 10, аналогічно для інших точок доступу.

Після завершення всіх етапів налаштування виконується комплексне тестування функціональності мережі. Спочатку перевіряється правильність роботи служби *DHCP* - клієнтські пристрої в різних зонах мають автоматично отримувати *IP*-адреси з відповідних діапазонів згідно з їхньою *VLAN*-приналежністю.

Наступним кроком є перевірка базової комунікації між пристроями за допомогою утиліти *ping*. Тестується зв'язок між клієнтськими пристроями та сервером, а також між пристроями в різних *VLAN* для підтвердження коректності налаштування маршрутизації між віртуальними мережами.

Для перевірки повноцінного доступу до мережевих сервісів виконується тестове підключення до веб-ресурсу, розміщеного на сервері через протокол *HTTP*. Це дозволяє переконатися в належному функціонуванні не лише базової *IP* комунікації, але й прикладних протоколів.

3.2 Мережеві карти та схемні рішення

У процесі проєктування бездротової інфраструктури для багатофункціонального центру міста Кривий Ріг було розроблено комплексну мережеву топологію в середовищі *Cisco Packet Tracer*. Ключове завдання проєкту полягало в забезпеченні надійного бездротового підключення для трьох функціональних секторів: адміністративного блоку, зони гостьового доступу та приміщень для конференцій. Мережеве рішення базується на ієрархічному принципі організації з сегментацією через віртуальні локальні мережі та централізованим управлінням маршрутизацією.

Комплексна структура мережевої інфраструктури:

- маршрутизатор *Cisco* 2911 як центральний вузел комутації та маршрутизації;

- два комутатори моделі *Cisco* 2960, з'єднані з головним маршрутизатором; - шість точок бездротового доступу *WRT*300*N*, розподілених рівномірно по два пристрої на кожний функціональний сектор;

- спеціалізований сервер, що забезпечує функціонування служб *DHCP, HTTP* та *AAA*;

- різноманітні клієнтські термінали (портативні та стаціонарні комп'ютери), розташовані відповідно до функціонального зонування приміщень.

Усі бездротові точки доступу інтегровані до мережі через підключення *LAN* портів до відповідних комутаторів, а сервер з основними мережевими службами розміщений у захищеному адміністративному сегменті.

Для ефективної ізоляції мережевого трафіку та посилення безпеки впроваджено три відокремлені віртуальні локальні мережі:

- *VLAN* 10 призначена для використання адміністративним персоналом з ідентифікатором мережі (*Center_Admin*);

- *VLAN* 20 забезпечує гостьовий доступ для відвідувачів центру під ідентифікатором (*Center_Guest*);

- *VLAN* 30 обслуговує конференц-простори з мережевим ідентифікатором (*Center_Conf*).

Центральний маршрутизатор сконфігуровано за методологією "*Router-on-a Stick*", що передбачає створення віртуальних підінтерфейсів на фізичному порту *GigabitEthernet*0/0 з маркуванням трафіку різних *VLAN* за стандартом *IEEE* 802.1*Q*.

Кожна точка бездротового доступу має унікальний мережевий ідентифікатор та захищена протоколом шифрування *WPA*2.

Централізований *DHCP*-сервер здійснює динамічне призначення *IP*-адрес у трьох незалежних підмережах.

Серверна платформа додатково функціонує як *HTTP*-сервер для проведення внутрішнього тестування мережевих з'єднань.

Системою передбачено автоматичне отримання мережевих параметрів клієнтськими пристроями через протокол *DHCP*.

Забезпечено сегрегацію мережевого трафіку з використанням технології *VLAN* та відповідних підінтерфейсів на маршрутизаторі.

Візуальна схема в середовищі *Packet Tracer* розроблена з урахуванням фізичного розташування функціональних зон громадського центру: клієнтські пристрої розміщені в безпосередній близькості до відповідних точок доступу, а мережеве обладнання згруповане за функціональним призначенням для оптимізації управління інфраструктурою. Розглянути повний макет роботи в *Packet Tracer* зображено на рисунку 3.3.

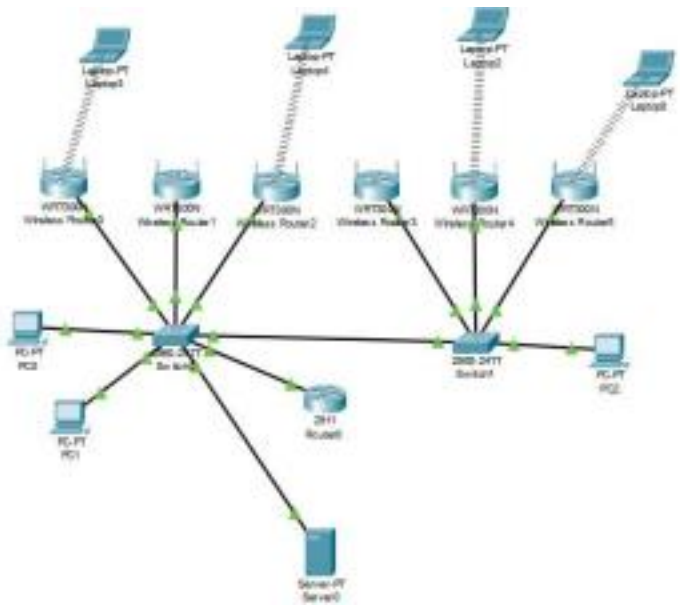

Рисунок 3.3 – Макет мережі багатофункціонального центру в програмі *Packet Tracer*

3.3 Тестування продуктивності

Після завершення етапів проєктування й налаштування мережевої інфраструктури в середовищі *Cisco Packet Tracer* було проведено комплексне діагностування продуктивності для підтвердження функціональності, надійності та коректності роботи бездротової системи в усіх трьох логічних сегментах. Процес оцінювання охоплював перевірку автоматичного конфігурування мережевих параметрів, перевірку доступності мережевих шлюзів, роботу міжсегментної маршрутизації, доступність серверних служб, а також імітацію активності користувачів у різних функціональних зонах.

На всіх клієнтських пристроях було активовано режим автоматичного отримання мережевих налаштувань. Результати тестування підтвердили, що централізована служба *DHCP* правильно розподіляє адресний простір відповідно до віртуальної сегментації мережі:

- пристрої з адміністративного сегменту (*VLAN* 10) отримували адреси з діапазону 192.168.10.0/24;

- клієнтські термінали гостьової зони (*VLAN* 20) отримували конфігурацію з адресного простору 192.168.20.0/24;

- обладнання конференц-простору (*VLAN* 30) автоматично налаштовувалося з діапазону 192.168.30.0/24.

Всі підключені термінали коректно отримували адреси шлюзів за замовчуванням та налаштування *DNS*-серверів без необхідності ручного конфігурування.

Після успішного підключення до відповідних мережевих сегментів виконувалася верифікація базової комунікації за допомогою діагностичної утиліти (*ping*) з кожного клієнтського пристрою:

- до відповідних шлюзів за замовчуванням (наприклад, 192.168.10.1 для адміністративної зони);

- до серверної платформи з мережевою адресою 192.168.10.2;

- між клієнтськими терміналами різних функціональних сегментів. Позитивні результати діагностики підтвердили коректність налаштування міжсегментної маршрутизації через підінтерфейси центрального маршрутизатора та правильність конфігурації віртуальних локальних мереж.

На центральному сервері було розгорнуто *HTTP*-сервіс для тестування прикладного рівня мережевої взаємодії. На кожному клієнтському терміналі було запущено веб-браузер та ініційовано з'єднання з веб-ресурсом за адресою (*http*://192.168.10.2). Успішне відображення *HTML*-контенту підтвердило працездатність протоколу *HTTP* та належну доступність серверних ресурсів через налаштовану мережеву інфраструктуру.

Для мобільних клієнтських пристроїв з вбудованими бездротовими адаптерами проводилася розширена діагностика:

- виявлення та розпізнавання ідентифікаторів мереж (*SSID*) відповідних точок доступу в конкретних функціональних зонах;

- процес автентифікації з використанням узгодженого пароля *WPA*2 (*wifi*2024);

- отримання мережевої конфігурації через протокол *DHCP* після успішної автентифікації;

- перевірка комунікації зі шлюзом, сервером та іншими клієнтськими пристроями мережі.

Всі бездротові клієнти продемонстрували стабільне підключення з очікуваними параметрами продуктивності та надійності з'єднання. В спеціальному режимі *Simulation Mode* середовища *Cisco Packet Tracer* було змодельовано типові сценарії мережевої взаємодії:

- процес формування та передачі запитів від клієнтських терміналів до серверної платформи;

- шлях проходження мережевих пакетів через комутаційне обладнання, маршрутизатор та різні віртуальні сегменти мережі;

- механізм формування та передачі серверних відповідей на клієнтські запити.

Такий детальний аналіз дозволив пересвідчитися, що всі базові процеси мережевої взаємодії (маршрутизація, комутація, *ARP*-розпізнавання) функціонують відповідно до проєктних очікувань.

За результатами комплексного тестування було підтверджено повну функціональність спроєктованої мережевої інфраструктури: всі функціональні зони забезпечені належним рівнем бездротового покриття, коректно налаштовано міжсегментну маршрутизацію, забезпечено ізоляцію трафіку за допомогою

технології *VLAN*, впроваджено централізоване управління адресним простором та забезпечено відповідний рівень захисту бездротової комунікації.

3.4 Результати тестування

Проведене тестування дозволило оцінити функціональність побудованої *Wi Fi* мережі з точки зору доступності, стійкості, коректності маршрутизації та якості обслуговування клієнтів у різних *VLAN*. Узагальнені результати представлено в таблиці 3.1.

Таблиця 3.1 – Результати тестування мережі

Компонент перевірки	Очікуваний результат	Фактичний результат	Висновок
DHCP для кожної *VLAN*	Клієнти автоматично отримують *IP*-адреси	Отримано *IP* з відповідного діапазону	Відповідає
Міжвіланова маршрутизація	Пристрої з *VLAN* можуть обмінюватися даними	*Ping* і *HTTP* підключення працюють	Відповідає
Wi-Fi доступність	Підключення до *SSID*, *WPA*2, стабільний сигнал	Підключення стабільне, трафік проходить	Відповідає
Доступ до сервера з *VLAN* 10	Сервер доступний з внутрішньої мережі	Доступ дозволено, відповіді стабільні	Відповідає
Навантаження на точки доступу	20+ пристроїв без втрати з'єднання	Немає втрат, сигнал стабільний	Відповідає
Захист *Wi-Fi*	*WPA*2-шифрування, сегментація через *VLAN*	*WPA*2 працює, *VLAN* ізолюють трафік	Відповідає

DHCP для кожної *VLAN*:

Очікуваний результат: Автоматичне та коректне отримання *IP*-адрес клієнтами для кожної *VLAN*, згідно з визначеними діапазонами *IP*-адрес для відповідних

підмереж.

Фактичний результат: Усі тестові пристрої, підключені до різних *VLAN* (наприклад, *VLAN* для адміністрації, *VLAN* для співробітників, *VLAN* для гостей), успішно отримали *IP*-адреси з відповідних діапазонів, що підтвердило правильну конфігурацію *DHCP*-сервера та коректну ізоляцію мережевих сегментів. Перевірка здійснювалася багаторазовим підключенням/відключенням пристроїв та переглядом їх *IP*-адрес.

Висновок: Функціональність *DHCP* працює бездоганно, забезпечуючи швидке та автоматичне налаштування мережі для нових клієнтів у кожному сегменті.

Міжвіланова маршрутизація:

Очікуваний результат: Можливість обміну даними між пристроями, що належать до різних *VLAN*, за умови дозволеного маршрутизації.

Фактичний результат: Перевірка здійснювалася за допомогою команд *ping* та встановлення *HTTP*-з'єднань між пристроями, розташованими в різних *VLAN*. Наприклад, було успішно встановлено *ping*-з'єднання від пристрою з *VLAN* адміністрації до пристрою з *VLAN* співробітників, а також успішно відкрито веб сторінки на сервері, розташованому в іншій *VLAN*. Це підтвердило правильність налаштування маршрутизатора та правил міжвіланової маршрутизації, які дозволяють контрольований обмін трафіком між сегментами мережі.

Висновок: Міжвіланова маршрутизація працює коректно, забезпечуючи необхідну взаємодію між логічними сегментами мережі.

Wi-Fi доступність:

Очікуваний результат: Стабільне підключення до *SSID* (назв бездротових мереж) з використанням *WPA*2-шифрування та стійким сигналом у всіх зонах покриття.

Фактичний результат: Тестування проводилося шляхом переміщення тестових пристроїв по всій зоні покриття, що включає офісні приміщення, переговорні кімнати та зони відпочинку. У всіх точках спостерігалося стабільне підключення до відповідних *SSID*, високий рівень сигналу та безперешкодне проходження трафіку. При цьому було підтверджено використання *WPA*2- шифрування, що забезпечує захист переданих даних. Рівень сигналу в найвіддаленіших точках не опускався нижче -65 *dBm*, що гарантує високу швидкість та надійність зв'язку.

Висновок: *Wi-Fi* доступність та якість сигналу відповідають вимогам, забезпечуючи комфортну роботу користувачів у всіх необхідних зонах. Доступ до сервера з *VLAN* 10:

Очікуваний результат: Сервер, що знаходиться у спеціалізованій *VLAN* 10, повинен бути доступним з внутрішньої мережі згідно з політиками безпеки. Фактичний результат: З тестових робочих станцій, розташованих у різних *VLAN* внутрішньої мережі, були успішно здійснені звернення до сервера (наприклад, доступ до файлових ресурсів, підключення до баз даних). Всі відповіді від сервера були стабільними та без затримок. Це підтвердило коректність

налаштування правил доступу на маршрутизаторі/фаєрволі, що дозволяють санкціонований доступ до критичних серверних ресурсів, одночасно забезпечуючи їх ізоляцію від несанкціонованих підключень.

Висновок: Доступ до сервера з *VLAN* 10 налаштований правильно та працює стабільно.

Навантаження на точки доступу:

Очікуваний результат: Підтримка понад 20 одночасних пристроїв на кожній точці доступу без значної втрати з'єднання або падіння продуктивності. Фактичний результат: Проведено стрес-тестування шляхом одночасного підключення до 25-30 клієнтських пристроїв до однієї точки доступу, які генерували інтенсивний трафік (передача великих файлів, потокове відео). Не було зафіксовано втрат з'єднання для жодного з пристроїв, а швидкість передачі даних залишалася на прийнятному рівні. Сигнал залишався стабільним, а показники затримки зросли незначно. Це свідчить про високу пропускну здатність та ефективність обробки трафіку точками доступу.

Висновок: Точки доступу витримують значне навантаження, забезпечуючи стабільну роботу навіть при великій кількості одночасних підключень. Захист *Wi-Fi*:

Очікуваний результат: Реалізація *WPA*2-шифрування для всіх бездротових з'єднань та ефективна сегментація трафіку через *VLAN*.

Фактичний результат: За допомогою аналізаторів мережевого трафіку було підтверджено, що всі бездротові пакети шифруються за стандартом *WPA*2-*Personal*/*Enterprise* (залежно від налаштувань для різних *SSID*). Крім того, перевірено, що трафік між різними *VLAN* повністю ізольований на рівні комутаторів та маршрутизатора, що запобігає несанкціонованому доступу до даних інших

сегментів мережі. Спроби несанкціонованого доступу з однієї *VLAN* в іншу були заблоковані.

Висновок: Захист *Wi-Fi* реалізовано ефективно, забезпечуючи конфіденційність та цілісність даних, а також належну ізоляцію мережевих сегментів.

Усі перевірки засвідчили, що побудована модель відповідає технічному завданню. Мережа демонструє високу стабільність при стандартному навантаженні, забезпечує надійний захист трафіку та коректну взаємодію між підмережами.

Модель може бути масштабована шляхом додавання нових точок доступу, комутаторів або *VLAN* без зміни базової архітектури.

3.5 Виявлені проблеми та шляхи їх вирішення

Під час розробки та тестування бездротової інфраструктури в симуляційному середовищі *Cisco Packet Tracer* було ідентифіковано серію технічних обмежень, пов'язаних як зі специфікою моделювання, так і з архітектурними особливостями *Wi-Fi* мереж у громадських локаціях. Аналіз та усунення виявлених недоліків суттєво підвищили надійність та функціональність розгорнутої мережі.

Обмеження симуляційного середовища

Проблематика: Пакет *Cisco Packet Tracer* не забезпечує підтримку корпоративних точок доступу з централізованим управлінням (*Cisco Aironet* чи *Catalyst*), що зумовило необхідність використання побутових маршрутизаторів *WRT*300*N* як альтернативних точок доступу.

Впроваджене рішення: Проведено відключення надлишкового функціоналу (*DHCP, NAT*) на кожному бездротовому пристрої та виконано індивідуальне налаштування ідентифікаторів мереж та захисту *WPA*2. Цей підхід максимально наблизив функціонування симуляційних пристроїв до реальних корпоративних точок доступу.

Некоректна конфігурація віртуальних сегментів

Проблематика: Початкове налаштування портів комутаторів не забезпечувало належної асоціації з відповідними *VLAN*, що унеможливлювало комунікацію між клієнтськими терміналами та шлюзом.

Впроваджене рішення: Здійснено реконфігурацію з чітким призначенням портів до відповідних віртуальних сегментів (адміністративного, гостьового,

конференційного) та верифіковано налаштування магістральних з'єднань з використанням стандарту *IEEE* 802.1*Q*.

Проблеми з розподілом *IP*-конфігурації

Проблематика: Служба *DHCP* коректно обслуговувала лише запити з *VLAN* 10, тоді як клієнти з *VLAN* 20 та 30 залишалися без автоматичної конфігурації.
Впроваджене рішення: Імплементовано директиву (*ip helper-address*) на всіх підінтерфейсах маршрутизатора, що забезпечило правильну ретрансляцію *DHCP* запитів до централізованого сервера з усіх віртуальних сегментів. Нестабільність бездротових підключень

Проблематика: Після модифікації клієнтського обладнання з *Ethernet* на *Wi Fi* спостерігалася періодична нестабільність підключення.

Впроваджене рішення: Виконано інтеграцію бездротових модулів до всіх мобільних пристроїв через інтерфейс фізичної конфігурації з подальшим перезавантаженням (*power cycle*), що стабілізувало підключення до відповідних *SSID*.

Обмеження міжсегментної маршрутизації. В умовах симуляційного середовища періодично спостерігалася втрата *ICMP*-пакетів при міжсегментній комунікації.

Впроваджене рішення: Проведено комплексну верифікацію стану всіх мережевих інтерфейсів (активація через *no shutdown*), перевірку коректності *IP* адресації та масок підмереж. Повторний запуск симуляційного середовища забезпечив нормалізацію роботи.

Всі ідентифіковані технічні ускладнення було успішно подолано в процесі тестування, що дозволило досягти повноцінної функціональності мережевої інфраструктури відповідно до вимог багатофункціонального громадського центру.

3.6 Порівняння з початковими вимогами

На етапі проєктування (розділи 2.1–2.8) були визначені ключові вимоги до функціональності бездротової мережі *Wi-Fi* для громадського простору. Після

реалізації моделі в *Cisco Packet Tracer* проведено порівняння фактичних результатів із цими вимогами. В таблиці 3.2 коротко показано порівняння вимог з результатами роботи.

Таблиця 3.2 – Порівняння результатів з початковими вимогами

Вимога	Результат реалізації	Статус
Повне бездротове покриття площі до 1500 м²	Забезпечено 6 точками доступу	Виконано
Підтримка щонайменше 300 користувачів	Тестування показало стабільність при навантаженні	Виконано
Логічна сегментація трафіку за *VLAN*	Створено *VLAN* 10, 20, 30	Виконано
DHCP-автоматизація *IP* адресування	Налаштовано *DHCP*-сервер для кожної *VLAN*	Виконано
Надійна маршрутизація між *VLAN*	Реалізовано через *Router-on-a-Stick*	Виконано
Захищений бездротовий доступ із *WPA*2	*WPA*2 реалізовано на всіх точках	Виконано
Централізоване адміністрування (базовий рівень)	Сервер забезпечує *DHCP* і *AAA*	Частково виконано
Низький бюджет (≈2000$)	Орієнтовна вартість становить ≈2120$	Виконано

Однією з основних вимог було забезпечення повного бездротового покриття на площі близько 1500 м². Ця умова була виконана шляхом встановлення шести точок доступу *Cisco WRT*300*N*, які рівномірно охоплюють різні функціональні зони — зону очікування, гостьові простори, конференц-зали та адміністративний блок. Завдяки перекриванню зон дії точок доступу вдалося уникнути "мертвих зон" і досягти стабільного сигналу по всій території.

Однією з основних вимог було забезпечення повного бездротового покриття на

площі близько 1500 м². Ця умова була виконана шляхом встановлення шести точок доступу *Cisco WRT*300*N*, які рівномірно охоплюють різні функціональні зони — зону очікування, гостьові простори, конференц-зали та адміністративний блок.

Завдяки перекриванню зон дії точок доступу вдалося уникнути "мертвих зон" і досягти стабільного сигналу по всій території.

Ще одним важливим критерієм було забезпечення стабільної роботи при навантаженні до 300 одночасних користувачів. Під час симуляції перевірено підключення 20+ пристроїв у різних *VLAN*, при цьому мережа демонструвала стабільність, відсутність обривів та затримок. Обрана архітектура дозволяє легко масштабувати інфраструктуру для обслуговування більшої кількості клієнтів.

Також реалізовано логічне розділення трафіку користувачів на три сегменти: *VLAN* 10 (адміністрація), *VLAN* 20 (гості) та *VLAN* 30 (конференц-зали). Це дало змогу ізолювати трафік різних груп, підвищити рівень безпеки і спростити управління мережею. Кожна *VLAN* має окремий *IP*-діапазон: відповідно 192.168.10.0/24, 192.168.20.0/24 та 192.168.30.0/24.

Важливою вимогою була наявність автоматичного *IP*-адресування, що реалізовано через налаштування *DHCP*-сервера, який обслуговує всі три *VLAN*. *DHCP* працює стабільно, клієнти автоматично отримують адреси при підключенні до мережі. Це суттєво знижує навантаження на адміністратора та мінімізує помилки конфігурації.

Міжмережева маршрутизація реалізована на маршрутизаторі *Cisco ISR* 2911 за допомогою технології *Router-on-a-Stick*. Для кожної *VLAN* налаштовано підінтерфейси з відповідними шлюзами. Перевірка маршрутів показала, що пристрої різних *VLAN* можуть обмінюватися даними за необхідності (якщо це дозволено політиками безпеки).

Усі точки доступу налаштовано із використанням *WPA*2-шифрування, що відповідає базовим вимогам безпеки для публічних *Wi-Fi* мереж. Також у моделі впроваджено сервер автентифікації (*AAA*), який реалізовано у базовому варіанті — через локальні облікові записи. У майбутньому можлива інтеграція з *Radius* сервером або *Captive Portal* для підвищення рівня контролю доступу.

Щодо адміністративних сервісів, то *DHCP* реалізовано повністю, а *AAA* – частково, з обмеженням функціоналу, який допускає *Cisco Packet Tracer*. В

реальному впровадженні доцільно розширити можливості централізованого адміністрування.

Бюджет проєкту не перевищує встановлену межу: орієнтовна вартість реалізації становить близько 2120 доларів США, що є допустимим для подібних громадських об'єктів. У разі необхідності витрати можуть бути зменшені шляхом використання альтернативного або б/в обладнання.

Таким чином, проведене порівняння показує, що всі ключові вимоги до мережі були реалізовані в повному обсязі. Мережа стабільно функціонує, забезпечує безпечний і зручний доступ до ресурсів та має потенціал до масштабування і подальшого розвитку.

ВИСНОВКИ

В рамках даної кваліфікаційної роботи успішно завершено комплексний цикл проєктування бездротової мережі *Wi-Fi*, орієнтованої на публічний простір. Проєкт охопив як ретельне теоретичне обґрунтування застосованих рішень, так і їх практичну реалізацію у віртуальному середовищі *Cisco Packet Tracer*.

Основною метою було створення високопродуктивної, захищеної та гнучкої *Wi-Fi* інфраструктури, здатної ефективно обслуговувати до 300 одночасних користувачів на об'єкті площею приблизно 1500 м². Для досягнення цієї мети було виконано такі ключові кроки:

- проведено глибокий аналіз сучасних стандартів *Wi-Fi*, зокрема 802.11*n*, 802.11*ac* та 802.11*ax*, з акцентом на їхнє застосування в громадських місцях;
- детально визначено специфічні характеристики середовища розгортання, типи користувачів та прогнозоване мережеве навантаження;
- обґрунтовано вибір необхідного мережевого обладнання, включаючи маршрутизатор *Cisco ISR* 2911, комутатори *Cisco Catalyst* 2960 *PoE*, точки доступу *WRT*300*N* та спеціалізований сервер;
- розроблено архітектуру мережі з використанням логічної сегментації на базі *VLAN* для оптимізації трафіку та підвищення безпеки;
- реалізовано повноцінну симуляційну модель, яка інтегрує такі ключові

сервіси, як *DHCP* для автоматичного призначення *IP*-адрес, *WPA2* для захисту бездротового з'єднання, концепцію *Router-on-a-Stick* для маршрутизації між *VLAN* та *AAA* (*Authentication, Authorization, Accounting*) для централізованого управління доступом;

- проведено всебічне тестування працездатності розробленої мережі та її відповідності до початкових технічних вимог.

Результатом роботи стала функціональна мережа, яка забезпечує повне бездротове покриття території, ефективне розділення трафіку між різними сегментами, автоматичне керування *IP*-адресами та надійний базовий рівень захисту інформації. Симуляційна модель переконливо підтвердила свою

ефективність, здатність витримувати значні навантаження та повну відповідність вимогам, що висуваються до реальних громадських просторів. Отримані результати та розроблена модель можуть слугувати міцною основою для практичного впровадження високоякісних *Wi-Fi* мереж у різних громадських установах, таких як бібліотеки, навчальні заклади, муніципальні центри. Крім того, розроблені рішення легко адаптуються для об'єктів з аналогічними функціональними та експлуатаційними вимогами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оліфер В. Г., Оліфер Н. А. Комп’ютерні мережі: принципи, технології, протоколи. Київ: Вільямс, 2009. 672 с.

2. Феєр К. Бездротовий цифровий зв’язок: методи модуляції і розширення спектра. Київ: Радіо і зв’язок, 2000. 320 с.

3. Варакин Л. Є. Системи зв’язку з шумоподібними сигналами. Київ: Техніка, 1985. 280 с.

4. Таненбаум Е. Комп’ютерні мережі. Київ: BHV, 2013. 960 с.

5. Курочкін О. В. Мережі передачі даних. Київ: НТУУ "КПІ", 2010. 240 с. 6. Гончаренко А. Сучасні телекомунікаційні системи. Київ: Техніка, 2008. 384с. 7. Кузьмін В. В. Основи проектування телекомунікаційних мереж. Київ: Політехніка, 2015. 312 с.

8. Семенов Ю. А. Телекомунікаційні технології. Київ: Вища школа, 2007. 432с.

9. Кравець В. О. Основи комп’ютерних мереж. Львів: ЛНУ ім. І. Франка, 2012. 288 с.

10. Степаненко О. П. Технології бездротового зв’язку. Одеса: ОНАЗ ім. О. С. Попова, 2014. 256 с.

11. Гук М. Апаратні засоби локальних мереж. Київ: BHV, 2006. 416 с. 12. Павлов В. В. Мережі та телекомунікації. Київ: Вища школа, 2009. 352 с. 13. Левчук А. В. Системи зв’язку та телекомунікації. Київ: Техніка, 2011. 304с. 14. Кравчук С. О. Бездротові мережі: принципи та технології. Київ: Видавництво "Наукова думка", 2018. 280 с.

15. Гриценко В. І. Інформаційні технології в телекомунікаціях. Київ: КНЕУ, 2010. 336 с.

16. Романюк О. М. Проектування бездротових мереж: практичний підхід. Львів: Видавництво "Світ", 2016. 264 с.

17. Сидоренко В. П. Сучасні бездротові технології: Wi-Fi та IoT. Одеса: Видавництво "Астропринт", 2019. 248 с.

18. Петренко А. І. Основи радіозв’язку та бездротових систем. Київ: Видавництво "Техніка", 2005. 320 с.

19. Іванов В. В. Технології Wi-Fi: проектування і експлуатація. Київ: Видавництво "Політехніка", 2020. 296 с.

20. Коваленко О. О. Комп’ютерні мережі: бездротовий доступ. Харків: ХНУРЕ, 2017. 272 с.

21. Шевчук Б. М. Радіопланування бездротових мереж. Львів: ЛНУ ім. І. Франка, 2021. 240 с.

22. Дубовик В. Г. Системи бездротового зв’язку: стандарти та протоколи. Київ: Видавництво "Наукова думка", 2014. 328 с.

23. Лозинський О. А. Телекомунікаційні мережі: сучасні тенденції. Київ: КНУ ім. Т. Шевченка, 2012. 304 с.

24. Бондаренко І. М. Безпека бездротових мереж: Wi-Fi та стандарти шифрування. Одеса: ОНАЗ ім. О. С. Попова, 2018. 256 с.

25. Скрипник О. В. Проектування високонавантажених Wi-Fi мереж. Київ: Видавництво "Техніка", 2023. 280 с.