

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання

(повна назва)

Кафедра інформаційно-мережної інженерії

(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищого освіти другий (магістерський)

Дослідження методів оптимізації параметрів бездротової мережі доступу

(тема)

Виконав:

здобувач 2 року навчання,

групи ІМІМ-24-1

Анастасія ПЕРЕВАЛО

(власне ім'я, прізвище)

Спеціальність 172 Електронні комунікації
та радіотехніка

(код і повна назва спеціальності)

Тип програми освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна
інженерія

(повна назва освітньої програми)

Керівник доц. Наталія ХАРЧЕНКО

(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри

(підпис)

Микола МОСКАЛЕЦЬ

(власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування.

Студент _____ / Перевало А.А./

Керівник _____ / Харченко Н.А./

Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання

Кафедра *інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Електронні комунікації та радіотехніка*

Тип програми *освітньо-професійна*

(код і повна назва)

Освітня програма *інформаційно-мережна інженерія*

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

«_____» _____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Перевало Анастасії Андріївни*

(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження методів оптимізації параметрів бездротової мережі доступу*

затверджено наказом університету від 20 жовтня 2025р. № 179 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 26 грудня 2025р.

3. Вихідні дані до роботи Дослідити особливості планування та оптимізації побудови бездротових локальних мереж. Відзначити характеристики та особливості стандарту 802.11ac. Дослідити необхідні етапи оптимізації безпроводового сегменту локальної корпоративної мережі у офісному центрі, що займає триповерхову будівлю. Необхідно оптимізувати вже існуючу мережу, яка складається з 42 робочих місць підключених проводним з'єднанням, та два бездротових сегменти, що створено для підключення користувачів у конференц-залах та кафе.

4. Перелік питань, що потрібно опрацювати в роботі _____

Вступ

1 Загальний аналіз бездротових технологій локальних мереж

2 Опис стандарту 802.11ac

3 Аналіз та вибір методів побудови корпоративної бездротової мережі

4 Розробка та оптимізація бездротової мережі доступу офісного центру

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____

Слайди у форматі Power Point (назва та мета роботи, стандарти Wi-Fi, стандарт 802.11ac (Wi-Fi 5), розподіл каналів у стандарті 802.11ac, методи та алгоритми оптимізації бездротової мережі, перелік недоліків при плануванні бездротових мереж, методика розрахунку кількості точок доступу, радіопланування і установка точок доступу, радіопланування трьох поверхів офісного центру, налаштування «безшовної» мережі Wi-Fi, результати оптимізації, тестування оптимізованої мережі, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	20.10.2025	вик.
2	Підбір літератури за темою роботи	21.10 - 12.11.2025	вик.
3	Загальний аналіз бездротових технологій локальних мереж	13.11 - 15.11.2025	вик.
4	Опис стандарту 802.11ac	16.11 - 19.11.2025	вик.
5	Аналіз та вибір методів побудови корпоративної бездротової мережі	20.11 - 09.12.2025	вик.
5	Розробка та оптимізація бездротової мережі доступу офісного центру	10.12 - 25.12.2025	вик.
6	Оформлення презентаційного матеріалу підготовка до захисту у ЕК	26.12.2025	

Дата видачі завдання 20 жовтня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____
(підпис)

доц. Наталія ХАРЧЕНКО
(посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 84 с., 41 рис., 13 табл., 2 додатки, 13 джерел.

Об'єкт дослідження – бездротові локальні мережі.

Мета роботи – визначення ефективності методів оптимізації робочої моделі безпроводової локальної мережі за технологією 802.11ac.

У роботі проведено детальний аналіз розвитку технології IEEE 802.11 та безпроводових Wi-Fi технологій в цілому. Досліджено актуальні на сьогодні методи та алгоритми оптимізації технології передачі даних у безпроводових локальних мережах та визначено властивості, які дозволяють забезпечити необхідні вимоги для систем доступу на базі IEEE 802.11ac. Саме цей стандарт технологій сімейства 802.11 є найбільш перспективним для використання у невеликих будівлях офісного типу, оскільки забезпечує для цього достатнє покриття.

Також проведено радіопланування трьох поверхів будівлі офісного центру, в результаті якого визначено оптимальні позиції для розміщення точок доступу.

БЕЗДРОТОВІ МЕРЕЖІ, АЛГОРИТМ ОПТИМІЗАЦІЇ, БЕЗШОВНА БЕЗДРОТОВА МЕРЕЖА, 802.11AC, РАДІОПЛАНУВАННЯ.

THE ABSTRACT

Explanatory note: 84 p., 41 figs., 13 tables, 13 sources, 2 appendices.

Object of research - wireless local area networks.

The purpose of the work - determining the effectiveness of methods for optimising the working model of a wireless local area network using 802.11ac technology.

The paper provides a detailed analysis of the development of IEEE 802.11 technology and wireless Wi-Fi technologies in general. It examines current methods and algorithms for optimising data transmission technology in wireless local area networks and identifies the properties that enable IEEE 802.11ac-based access systems to meet the necessary requirements. This standard of the 802.11 family of technologies is the most promising for use in small office-type buildings, as it provides sufficient coverage for this purpose.

Radio planning of three floors of an office centre building was also carried out, as a result of which the optimal positions for placing access points were determined.

WIRELESS NETWORKS, OPTIMISATION ALGORITHM, SEAMLESS WIRELESS NETWORK, 802.11AC, RADIO PLANNING.

ЗМІСТ

	С.
ПЕРЕЛІК СКОРОЧЕНЬ.....	8
ВСТУП.....	9
1 ЗАГАЛЬНИЙ АНАЛІЗ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ЛОКАЛЬНИХ МЕРЕЖ.....	11
1.1 Історія розвитку та базові стандарти Wi-Fi.....	11
1.2 Стандарти нового покоління Wi-Fi.....	14
1.3 Класифікація Wi-Fi.....	16
1.4 Архітектура безпроводових мереж.....	17
1.5 Безпека Wi-Fi мережі та способи захисту інформації.....	20
2 ОПИС СТАНДАРТУ 802.11AC.....	23
2.1 Характеристики роботи стандарту в мережі IEEE 802.11ac.....	24
2.1.1 Частотні характеристики.....	24
2.1.2 Фізичний рівень.....	25
2.2 Формат пакетів в мережі 802.11ac.....	28
3 АНАЛІЗ ТА ВИБІР МЕТОДІВ ПОБУДОВИ КОРПОРАТИВНОЇ БЕЗДРОТОВОЇ МЕРЕЖІ.....	30
3.1 Визначення методів оптимізації бездротової мережі.....	30
3.2 Алгоритми оптимізації бездротової мережі.....	30
3.3 Особливості реалізації корпоративної бездротової мережі.....	32
3.4 Недоліки існуючої мережі та розробка загальних вимог до оновлення обладнання.....	33
4 РОЗРОБКА ТА ОПТИМІЗАЦІЯ БЕЗДРОТОВОЇ МЕРЕЖІ ДОСТУПУ ОФІСНОГО ЦЕНТРУ.....	35
4.1 Розрахунок кількості точок доступу.....	35
4.2 Аналіз виробників обладнання.....	39
4.3 Вибір обладнання для бездротової мережі.....	45
4.3.1 Вибір маршрутизатора Wi-Fi.....	45
4.3.1 Вибір точки доступу.....	46
4.4 Радіопланування і установка точок доступу.....	48
4.4.1 Радіопланування на першому поверсі.....	50
4.4.2 Радіопланування на другому поверсі.....	52

4.4.3 Радіопланування на третьому поверсі.....	54
4.4.4 Тривимірне відображення планованої мережі.....	56
4.5 Налаштування «безшовної» мережі Wi-Fi.....	58
4.6 Налаштування Wi-Fi адаптерів користувачів.....	61
4.7 Налаштування захисту бездротової мережі.....	62
4.8 Визначення результатів оптимізації.....	63
ВИСНОВКИ.....	68
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	69
ДОДАТОК А ПУБЛІКАЦІЇ.....	71
ДОДАТОК Б СЛАЙДИ ПРЕЗЕНТАЦІЇ.....	75

ПЕРЕЛІК СКОРОЧЕНЬ

- Ad-Hoc або IBSS – Independent Basic Service Set – епізодична мережа;
- ESS – Extended Service Set – розширена зона обслуговування;
- BSS – Basic Service Set – основна зона обслуговування;
- QAM – Quadrature Amplitude Modulation – квадратурна амплітудна модуляція;
- DSSS – Direct Sequence Spread Spectrum – розширення спектра методом прямої послідовності;
- IoT – Internet of Things – інтернет речей;
- MLO – Multi-Link Operation – технологія стандарту Wi-Fi 7, яка дозволяє пристроям одночасно підключатися і передавати дані через кілька частотних діапазонів;
- MIMO (Multiple Input Multiple Output) – множинний вхід і вихід (технологія багатоканальної передачі даних);
- MU-MIMO – Multi User MIMO – технологія Wi-Fi, що дозволяє роутеру одночасно спілкуватися з кількома пристроями, надсилаючи їм дані через різні антенні потоки, замість того, щоб обслуговувати їх послідовно
- OFDM – Orthogonal Frequency-Division Multiplexing – ортогональне мультиплексування з розділенням каналів;
- OFDMA – Orthogonal Frequency Division Multiple Access – це метод забезпечення передавання інформації багатьом користувачам одного радіоспектра з використанням технології OFDM;
- SSID – Service Set Identifier – це унікальна назва мережі Wi-Fi;
- WEP – Wired Equivalent Privacy – протокол шифрування для захисту бездротових мереж Wi-Fi;
- WPA – Wi-Fi Protected Access – стандарт безпеки для бездротових Wi-Fi мереж, розроблений для захисту від несанкціонованого доступу та перехоплення даних;
- WLAN – Wireless Local Area Network – бездротова локальна мережа.

ВСТУП

Сучасна діяльність будь-якої організації нерозривно пов'язана з функціонуванням корпоративної мережі, що забезпечує оперативний обмін даними як в межах локальної інфраструктури, так і в глобальному масштабі через мережу Інтернет. Паралельно спостерігається стрімка тенденція до мобільності, де ноутбуки, планшети та смартфони поступово витісняють традиційні настільні комп'ютери, залишаючи останнім лише специфічні завдання, що потребують високої обчислювальної потужності.

Збільшення кількості мобільних пристроїв у типовому офісі, що вже сягає десятків одиниць, ставить під сумнів ефективність застарілого мережевого обладнання, яке не дозволяє повноцінно використовувати їх потенціал. Зростання обсягів даних, де робота з файлами розміром у десятки гігабайт стала звичною справою, вимагає забезпечення якісного доступу до мережі з будь-якої точки приміщення.

Ключовим рішенням для подолання цих викликів є створення зручних та високошвидкісних Wi-Fi мереж. Хоча бездротові технології мають певні притаманні недоліки, такі як:

- вплив навколишнього середовища на передачу даних: фактори зовнішнього середовища можуть негативно впливати на стабільність та якість сигналу;
- обмежений радіус дії: кожен Wi-Fi модуль має свій радіус покриття, який, хоч і може сягати до 500 метрів, все ж є обмеженим;
- вплив перешкод: товщина стін, розташування меблів та інші фізичні перешкоди можуть суттєво погіршувати якість зв'язку;
- слабкий захист від злому: бездротові мережі потенційно більш вразливі до несанкціонованого доступу порівняно з дротовими;
- нижча швидкість передачі даних: порівняно з традиційним дротовим підключенням, швидкість передачі даних у Wi-Fi може бути нижчою [1].

Проте, більшість цих недоліків можуть бути мінімізовані шляхом правильного проектування та побудови бездротової мережі. Особливо перспективним рішенням є використання новітнього стандарту 802.11ac. При належному проектуванні Wi-Fi мережі за цим стандартом можна досягти

чудової зони покриття, значно меншої чутливості до сторонніх радіоперешкод та високої швидкості передачі даних, яка навряд чи розчарує користувачів.

Незважаючи на те, що не всі проблеми можуть бути повністю вирішені виключно за допомогою сучасних стандартів, неминучість переходу користувачів на швидкісні бездротові мережі доступу є очевидною. Побудова таких мереж лягає на плечі технічних спеціалістів.

Вирішення подібних завдань має ключове значення для підвищення операційної ефективності підприємств та сприяє прискоренню розвитку інформаційних технологій в Україні. Однак, в умовах фінансової кризи, державні установи часто змушені економити на мережевому обладнанні, що призводить до використання застарілих та менш ефективних технологій. Це, в свою чергу, призводить до того, що Wi-Fi мережі проектуються без дотримання необхідних норм, що унеможливорює раціональне використання їх ресурсів.

У рамках кваліфікаційної роботи магістра було сформульовано науково-методичну задачу оптимізації мережі доступу в офісному приміщенні. Для її вирішення було запропоновано комплекс методів та алгоритмів, що дозволили побудувати власний оптимізований сегмент корпоративної бездротової локальної мережі, який відповідає специфічним можливостям та потребам установи.

1 ЗАГАЛЬНИЙ АНАЛІЗ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ЛОКАЛЬНИХ МЕРЕЖ

1.1 Історія розвитку та базові стандарти Wi-Fi

Сучасне життя неможливо уявити без бездротових мереж, які зробили доступ до інформації та послуг значно зручнішим. У світі, де знання – це сила, постійно з'являються нові стандарти зв'язку, що забезпечують вищу швидкість, ширше покриття та надійніший захист даних. Одним із ключових інструментів, що дозволяє нам бути в курсі подій і ефективно взаємодіяти зі світом, є технологія Wi-Fi (Wireless Fidelity). Вона розроблена консорціумом "Wi-Fi Alliance" на основі стандартів IEEE 802.11, а сама назва "Wi-Fi" є торговою маркою цього альянсу. Спочатку технологія отримала назву Wireless-Fidelity, що означає "бездротова надійність" [2].

Історія Wi-Fi розпочалася у 1991 році в Нідерландах, коли компанії NCR Corporation/AT&T (пізніше Lucent і Agere Systems) створили її для систем касового обслуговування під брендом WaveLAN. На початковому етапі швидкість передачі даних становила від 1 до 2 Мбіт/с. [2]

Сьогодні ми маємо чотири основні стандарти перших поколінь: 802.11a, 802.11b, 802.11g та 802.11n, які широко використовуються в комп'ютерній та побутовій техніці. Незважаючи на відмінності у швидкості передачі даних, базова архітектура Wi-Fi залишається незмінною. Важливо пам'ятати, що дальність дії мережі залежить від таких факторів, як потужність сигналу, кількість антен, а також від обраних методів модуляції та корекції помилок.

У стандарті *802.11a* для передачі даних використовується технологія OFDM. Це означає, що один великий потік інформації розбивається на багато менших, які передаються одночасно на різних частотах. Уявіть собі, що замість однієї широкої дороги ви будете багато вузьких паралельних доріжок. Кожна доріжка несе свою частину даних [1].

Такий підхід дозволяє ефективно працювати навіть у місцях з великою кількістю перешкод, наприклад, у місті. Якщо одна з "доріжок" (частот) буде заблокована або спотворена, інші залишаться неушкодженими, і зв'язок продовжиться. Однак, якщо поблизу працюватиме багато точок доступу, вони

можуть заважати одна одній.

802.11a працює на частоті 5 ГГц. Це перевага, оскільки ця частота менш завантажена, ніж 2,4 ГГц (яку використовують мікрохвильові печі, Bluetooth та старі телефони). Але є й недолік: хвилі на частоті 5 ГГц гірше проходять крізь перешкоди (стіни, меблі). Тому в приміщеннях дальність зв'язку обмежена: до 12 метрів при максимальній швидкості (54 Мбіт/с) і до 91 метра при нижчій швидкості (6 Мбіт/с). На відкритому просторі дальність значно більша: до 30 метрів при 54 Мбіт/с і до 305 метрів при 6 Мбіт/с [1].

Стандарт 802.11a може використовувати два канали одночасно, що дозволяє досягти швидкості до 54 Мбіт/с.

Стандарт *802.11b* використовує іншу технологію передачі даних – DSSS. Він забезпечує нижчу швидкість (до 11 Мбіт/с) і має слабкий захист. Протокол шифрування WEP, який використовувався раніше, вже давно зламаний. Важливо пам'ятати, що навіть найсучасніші технології захисту не допоможуть, якщо мережа налаштована неправильно [1].

У приміщеннях 802.11b працює на відстані до 30 метрів при швидкості 11 Мбіт/с і до 91 метра при 1 Мбіт/с. На відкритому просторі дальність збільшується до 120 метрів при 11 Мбіт/с і до 460 метрів при 1 Мбіт/с [1].

Цей стандарт варто використовувати лише тоді, коли немає можливості застосувати новіші, швидші та безпечніші технології. Він працює на частоті 2,4 ГГц і використовує 3 канали, які не заважають один одному.

Стандарт *802.11g*, як і 802.11a, використовує OFDM для передачі даних. Це дозволяє досягти значно вищої швидкості порівняно з 802.11b – до 54 Мбіт/с. При цьому він зберігає сумісність зі старими пристроями стандарту 802.11b, що працюють на частоті 2,4 ГГц. Це робить його привабливим вибором для багатьох мереж, оскільки він поєднує в собі переваги швидкості та широкої доступності обладнання [1].

Стандарт *802.11n* став значним кроком вперед, поєднуючи в собі найкращі риси попередніх стандартів та додаючи нові можливості. Він використовує технологію MIMO (Multiple-Input Multiple-Output), що означає використання кількох антен для одночасної передачі та прийому даних. Це дозволяє значно збільшити швидкість (рис. 1.1) та надійність зв'язку, оскільки

сигнали можуть надсилатися різними шляхами, оминаючи перешкоди [2].

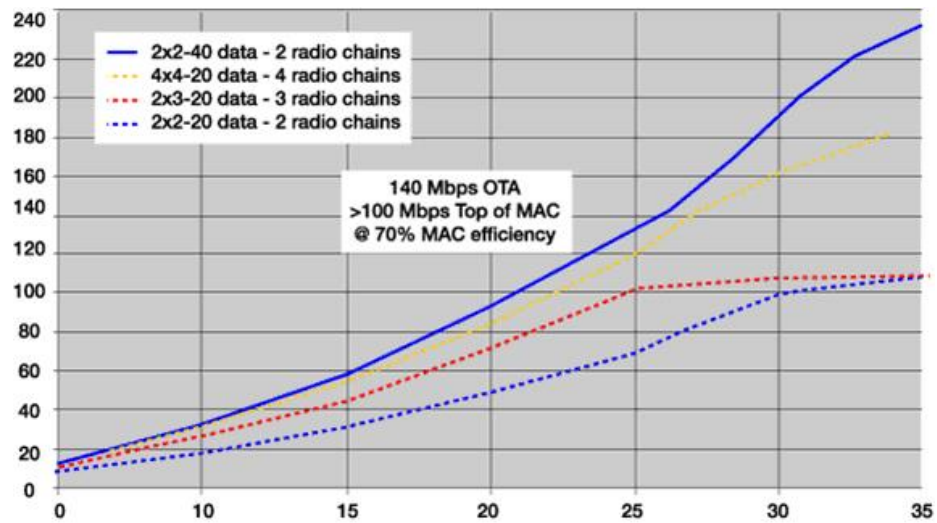


Рисунок 1.1 – Залежність теоретичної пропускної здатності від SNR, числа каналів і діапазонів

802.11n може працювати як на частоті 2,4 ГГц, так і на 5 ГГц, що дає гнучкість у виборі каналу та дозволяє уникнути перевантаженості. Швидкість передачі даних може досягати вражаючих 600 Мбіт/с завдяки використанню ширших каналів (40 МГц замість 20 МГц) та більш ефективних схем модуляції (рис. 1.2).

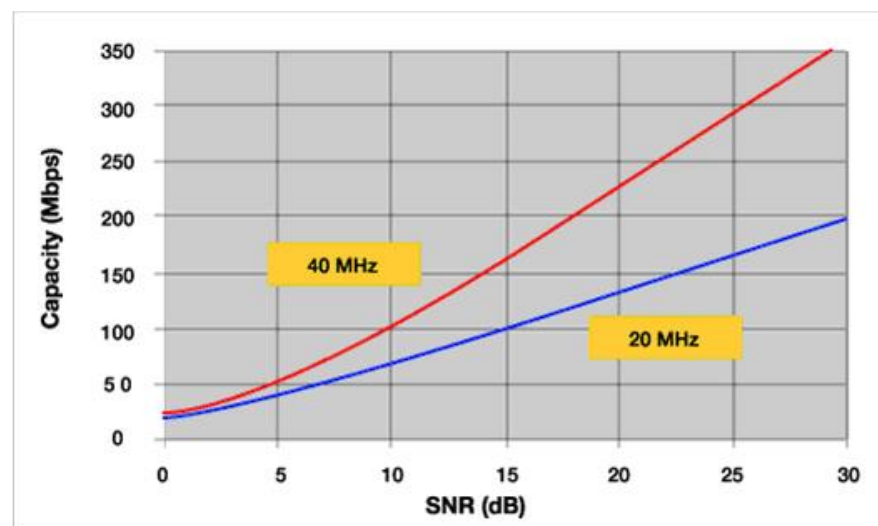


Рисунок 1.2 – Збільшення пропускної здатності каналу за рахунок розширення частотного діапазону

Щодо покриття, 802.11n демонструє покращені показники порівняно з

802.11a. У приміщеннях дальність може сягати 70 метрів при максимальній швидкості, а на відкритому просторі – до 250 метрів. Це досягається завдяки кращій обробці сигналів та використанню кількох антен.

1.2 Стандарти нового покоління Wi-Fi

Стандарт *802.11ac*, також відомий як Wi-Fi 5, вивів бездротові мережі на новий рівень, забезпечуючи гігабітні швидкості. Він працює виключно на частоті 5 ГГц, що дозволяє уникнути перешкод від пристроїв, що працюють на 2,4 ГГц [3].

Ключовою інновацією 802.11ac є використання технології MU-MIMO (Multi-User MIMO), яка дозволяє роутеру одночасно спілкуватися з кількома пристроями, а не послідовно. Це значно підвищує ефективність мережі, особливо в умовах високого навантаження [3].

Швидкість передачі даних у 802.11ac може сягати декількох гігабіт на секунду, що робить його ідеальним для потокового відео високої чіткості, онлайн-ігор та інших вимогливих до пропускної здатності завдань. Для досягнення таких швидкостей використовуються ширші канали (до 160 МГц) та більш складні схеми модуляції.

Дальність покриття 802.11ac на частоті 5 ГГц, як правило, дещо менша, ніж у стандартів, що працюють на 2,4 ГГц, через особливості поширення високочастотних хвиль. Однак, завдяки покращеній обробці сигналів та технології MU-MIMO, він забезпечує стабільний та швидкий зв'язок у межах свого радіусу дії.

Стандарт *802.11ax*, або Wi-Fi 6, зосереджений на підвищенні ефективності та продуктивності мережі, особливо в умовах високої щільності пристроїв. Він працює як на частоті 2,4 ГГц, так і на 5 ГГц, але його головна перевага – це покращена робота в умовах, де багато пристроїв одночасно підключені до мережі [3].

Wi-Fi 6 використовує нові технології, такі як OFDMA (Orthogonal Frequency Division Multiple Access), яка дозволяє розділяти канал на менші підканали для одночасної передачі даних різним пристроям. Це значно зменшує затримки та підвищує загальну пропускну здатність мережі. Також використовується покращена версія MIMO та більш ефективні схеми модуляції

[3].

Швидкість передачі даних у Wi-Fi 6 може бути вищою, ніж у 802.11ac, але головний акцент робиться на збільшенні загальної продуктивності мережі та зменшенні затримок для кожного окремого пристрою. Це робить його ідеальним для "розумних" будинків, офісів з великою кількістю підключених пристроїв та громадських місць [3].

Щодо покриття, Wi-Fi 6 забезпечує порівнянну або дещо кращу дальність порівняно з 802.11ac, завдяки покращеній обробці сигналів та ефективнішому використанню спектру. Він також включає функції, що покращують енергоефективність пристроїв, що підключаються, що важливо для пристроїв Інтернету речей (IoT).

Стандарт *802.11be*, відомий як Wi-Fi 7, є наступним поколінням бездротових технологій, що обіцяє ще більші швидкості та менші затримки. Він розробляється з акцентом на екстремально високу пропускну здатність (Extremely High Throughput - ЕНТ) та призначений для підтримки найвимогливіших додатків, таких як віртуальна та доповнена реальність (VR/AR), 8K-відео та хмарні ігри [3].

Wi-Fi 7 буде працювати у трьох діапазонах частот: 2,4 ГГц, 5 ГГц та новому діапазоні 6 ГГц. Використання діапазону 6 ГГц є ключовою особливістю, оскільки він пропонує значно більше неперекривних каналів, що дозволяє уникнути перевантаження та забезпечити максимальну швидкість [3].

Серед ключових інновацій Wi-Fi 7:

- ширші канали: підтримка каналів шириною до 320 МГц, що вдвічі більше, ніж у Wi-Fi 6;
- вища модуляція: використання 4096-QAM (Quadrature Amplitude Modulation), що дозволяє передавати більше даних за один цикл сигналу;
- технологія Multi-Link Operation (MLO): дозволяє пристроям одночасно використовувати кілька каналів у різних діапазонах частот для збільшення пропускну здатності та надійності. Наприклад, пристрій може одночасно передавати дані через 5 ГГц та 6 ГГц;
- покращений OFDMA та MU-MIMO: подальший етап вдосконалення цих технологій для ще ефективнішого використання спектру та підтримки більшої кількості пристроїв.

Очікується, що Wi-Fi 7 забезпечить пікові швидкості передачі даних, що

перевищують 30 Гбіт/с, що відкриє нові можливості для бездротових технологій. Хоча дальність покриття на 6 ГГц може бути дещо меншою, ніж на 2,4 ГГц, комбінація MLO та інших технологій дозволить забезпечити стабільний та надшвидкий зв'язок у межах зони покриття.

У табл. 1.1 приведено короткий опис та порівняння стандартів технології Wi-Fi.

Таблиця 1.1 – Порівняльна характеристика стандартів Wi-Fi:

Стандарт	Рік випуску	Частота (ГГц)	Макс. швидкість (Мбіт/с)	Технологія модуляції	Ключові особливості
802.11a	1999	5	54	OFDM	Висока швидкість, стійкість до перешкод, обмежена дальність у приміщеннях
802.11b	1999	2.4	11	DSSS	Низька швидкість, слабкий захист, більша дальність у приміщеннях
802.11g	2003	2.4	54	OFDM	Поєднання швидкості 802.11a та сумісності 802.11b
802.11n	2009	2.4, 5	600	OFDM, MIMO	Висока швидкість, покращене покриття, використання кількох антен
802.11ac (Wi-Fi 5)	2013	5	~3467 (теоретично)	OFDM, MU-MIMO	Гігабітні швидкості, робота на 5 ГГц, одночасне спілкування з кількома пристроями
802.11ax (Wi-Fi 6)	2019	2.4, 5	~9608 (теоретично)	OFDM, OFDMA, MU-MIMO	Ефективність у щільних мережах, зменшення затримок, покращена енергоефективність
802.11be (Wi-Fi 7)	Очікується	2.4, 5, 6	>30000 (теоретично)	OFDM, OFDMA, MU-MIMO, MLO	Екстремально висока пропускна здатність, робота на 6 ГГц, ширші канали, Multi-Link Operation

1.3 Класифікація Wi-Fi

За аналогією з тим, як ми класифікуємо дротові мережі, бездротові мережі також можна умовно розділити на категорії залежно від їхнього охоплення. Це персональні мережі (WPAN) з радіусом дії до 10 метрів, локальні мережі (WLAN) до 100 метрів, міські мережі (WMAN) з охопленням до 50 кілометрів, і, нарешті, глобальні мережі (WWAN), що покривають

відстані понад 50 кілометрів. При створенні мереж WPAN та WLAN застосовуються практично однакові технологічні рішення (рис. 1.3), головні відмінності між якими полягають у вибраних діапазонах частот та характеристиках радіоінтерфейсів. Обидві ці мережі функціонують у неліцензованих частотних діапазонах 2.4 ГГц або 5 ГГц. Це означає, що для їх розгортання не потрібне спеціальне частотне планування чи узгодження з іншими радіомережами, які працюють на тих самих частотах [4].

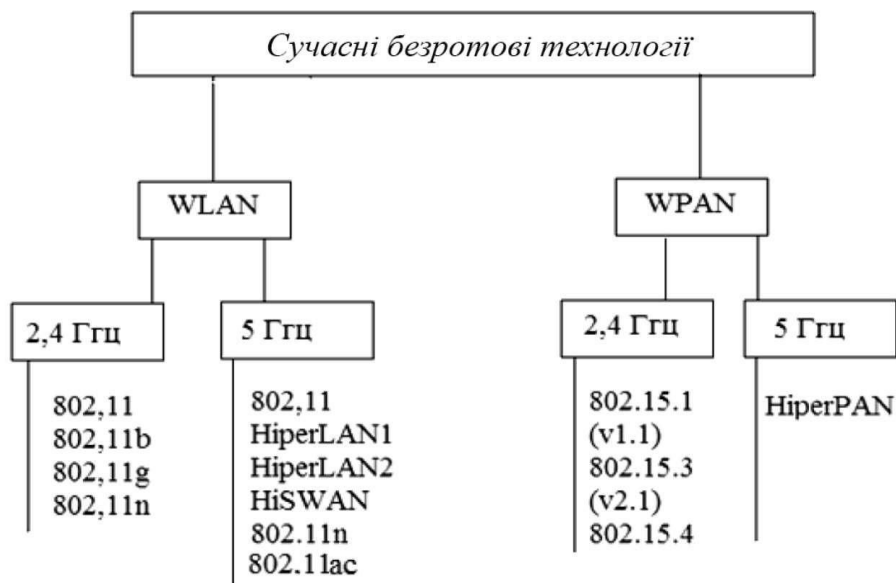


Рисунок 1.3 – Стандарти бездротових технологій

1.4 Архітектура безпроводових мереж

Виділяють 3 основних типи організації Wi-Fi мереж [4]:

- епізодична мережа (Ad-Hoc або IBSS – Independent Basic Service Set);
- основна зона обслуговування (BSS – Basic Service Set або Infrastructure Mode);
- розширена зона обслуговування ESS – Extended Service Set.

Режим *Ad-Hoc*, що має технічну назву Independent Basic Service Set (IBSS), являє собою найбазовішу схему побудови локальної мережі. У цій моделі взаємодія між клієнтськими пристроями, такими як комп'ютери та ноутбуки, відбувається напряму, без посередництва будь-якого центрального вузла (рис. 1.4) [4].



Рисунок 1.4 – Схема роботи обладнання Ad-Нос

Завдяки своїй здатності до самоорганізації, ця архітектура отримала назву "самоорганізована мережа", що влучно відображає її переваги для швидкого розгортання мережеских з'єднань. Для створення такої мережі достатньо, щоб кожен пристрій був обладнаний WLAN-адаптером.

У конфігурації BSS взаємодія між вузлами мережі реалізується не прямим з'єднанням, а через централізований компонент – точку доступу (Access Point). Точка доступу функціонує як міст для інтеграції з зовнішньою дротовою мережею та є основним комунікаційним хабом для всіх станцій BSS. Клієнтські станції не встановлюють прямих з'єднань між собою. Натомість, вони передають кадри до точки доступу, яка відповідає за їх маршрутизацію до станції-адресата. Наявність порту висхідного каналу (uplink port) дозволяє підключати BSS до дротової мережі (наприклад, Ethernet). З огляду на це, BSS іноді класифікують як інфраструктурний режим [4]. Типова топологія інфраструктури BSS проілюстрована на рис. 1.5.



Рисунок 1.5 – Схема роботи мережі в BSS

Режим ESS (Extended Service Set) призначений для створення єдиної бездротової мережі шляхом об'єднання декількох окремих точок доступу (які самі по собі формують мережі BSS, як показано на рис. 1.6). Це дозволяє точкам доступу взаємодіяти між собою. Розширений режим ESS особливо корисний, коли потрібно об'єднати велику кількість користувачів в одну мережу або інтегрувати кілька дротових та бездротових мереж в єдину систему [4].

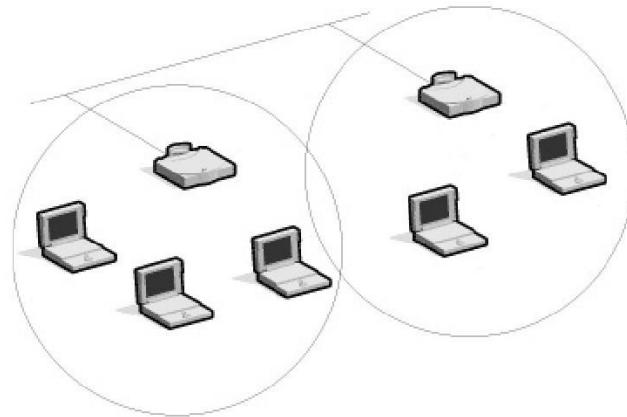


Рисунок 1.12 – Схема роботи обладнання у режимі ESS

Ключовим аспектом при побудові бездротових локальних мереж (WLAN) є забезпечення необхідної зони покриття. На цей параметр впливає низка факторів:

- використовувана частота: чим вища частота, тим менша дальність поширення радіохвиль;
- наявність перешкод: різні матеріали по-різному поглинають та відбивають сигнали, що впливає на їхню силу та дальність;
- режим роботи мережі: вибір між режимом Infrastructure (з точками доступу) та Ad Hoc (пряме з'єднання пристроїв) також впливає на покриття;
- потужність обладнання: потужність передавача та чутливість приймача безпосередньо визначають дальність зв'язку.

За відсутності перешкод, типова зона покриття однієї точки доступу становить: 150 метрів для мереж стандарту IEEE 802.11a/ac та близько 300 метрів для мереж стандартів 802.11b/g/n.

Шляхом додавання більшої кількості точок доступу в режимі ESS, можна ефективно розширювати зону покриття мережі, охоплюючи необхідну територію.

1.5 Безпека Wi-Fi мережі та способи захисту інформації

Основна проблема безпеки Wi-Fi полягає в її легкодоступності порівняно з дротовими мережами, такими як Ethernet. Для доступу до дротової мережі потрібно або фізично потрапити до будівлі, або подолати зовнішній брандмауер. Натомість, щоб підключитися до Wi-Fi, достатньо просто перебувати в зоні її дії. Більшість компаній прагнуть захистити свої конфіденційні дані, обмежуючи зовнішній доступ. Однак, використання бездротового підключення без належного шифрування значно знижує рівень безпеки [5].

Зловмисник, отримавши доступ до Wi-Fi маршрутизатора, може здійснити DNS-спуфінг-атаку, підміняючи відповіді DNS-сервера для інших користувачів мережі.

Старий стандарт шифрування WEP легко зламати, навіть якщо він налаштований правильно. Новіші стандарти WPA та WPA2, що з'явилися у 2003 році, були розроблені для вирішення цієї проблеми. Проте, часто точки доступу Wi-Fi за замовчуванням працюють без шифрування (у "відкритому" режимі). Це зручно для новачків, оскільки пристрій працює "з коробки", але не забезпечує жодного захисту, надаючи вільний доступ до локальної мережі. Щоб увімкнути безпеку, користувач повинен самостійно налаштувати пристрій, зазвичай через графічний інтерфейс. У незашифрованих мережах Wi-Fi підключені пристрої можуть бути об'єктом відстеження та запису даних, включаючи особисту інформацію. Такі мережі потребують додаткових засобів захисту, таких як VPN або HTTPS [5].

Зі зростанням кількості пристроїв, підключених до Wi-Fi, вкрай важливо впроваджувати стратегії безпеки, щоб мінімізувати ризики. Пристрої, підключені до Інтернету, можуть бути використані зловмисниками для збору особистої інформації, крадіжки особистих даних, компрометації фінансових даних, а також для прихованого прослуховування або спостереження за користувачами. Вжиття певних заходів безпеки під час налаштування та використання пристроїв може допомогти запобігти таким інцидентам.

Наразі можна виділити три основні загрози безпеці бездротових локальних мереж (WLAN):

- атаки типу "відмова в обслуговуванні" (DoS) - зловмисник

перевантажує мережу повідомленнями, що унеможлиблює доступ до мережевих ресурсів;

- спуфінг та захоплення сеансу - зловмисник отримує доступ до мережевих даних та ресурсів, видаючи себе за легітимного користувача;
- підслуховування - неавторизовані особи перехоплюють дані, що передаються захищеною мережею [6].

Ці загрози підкреслюють необхідність комплексного підходу до безпеки бездротових мереж. Окрім використання надійних протоколів шифрування, таких як WPA2 або новіший WPA3, користувачам слід регулярно оновлювати програмне забезпечення своїх маршрутизаторів та пристроїв, щоб усунути відомі вразливості. Також важливо використовувати складні та унікальні паролі для доступу до мережі Wi-Fi та адміністративної панелі маршрутизатора.

Для бізнес-середовищ, де безпека даних є критично важливою, рекомендується впровадження додаткових заходів, таких як сегментація мережі, використання віртуальних приватних мереж (VPN) для віддаленого доступу та впровадження систем виявлення та запобігання вторгненням (IDS/IPS). Регулярне проведення аудитів безпеки та навчання персоналу щодо правил безпечної поведінки в мережі також відіграють значну роль у мінімізації ризиків [6].

Крім того, слід пам'ятати про безпеку самих пристроїв, підключених до мережі. Це включає встановлення антивірусного програмного забезпечення, увімкнення брандмауерів на пристроях та обережність при підключенні до невідомих або незахищених мереж Wi-Fi, особливо в громадських місцях. Використання VPN при підключенні до публічних мереж є обов'язковим для захисту конфіденційної інформації.

Також, слід приділяти увагу безпеці IoT-пристроїв (Інтернету речей), які часто мають слабкі механізми захисту та можуть стати "слабкою ланкою" в загальній мережевій безпеці. Регулярна зміна паролів за замовчуванням на таких пристроях та оновлення їх програмного забезпечення є обов'язковими кроками.

Крім шифрування, для ускладнення доступу до вашої мережі стороннім особам, варто приховати ім'я мережі (SSID). Більшість Wi-Fi роутерів дозволяють це зробити. Якщо залишити SSID за замовчуванням, встановленим виробником, зловмисники зможуть легко визначити модель вашого роутера і, можливо, скористатися відомими його слабкими місцями.

Важливо мати брандмауер не тільки на рівні мережі (вбудований у роутер або модем), але й безпосередньо на ваших пристроях (так званий "брандмауер на основі хоста"). Це додасть додатковий рівень захисту, особливо якщо злоумисник зможе обійти мережевий брандмауер.

Сучасні бездротові системи вимагають гнучкості. Зростаючий попит на бездротову та дротову інфраструктуру означає необхідність балансування навантаження з високою пропускнуою здатністю. Це дозволяє системі автоматично перерозподіляти користувачів між точками доступу, коли одна з них перевантажена, забезпечуючи стабільну роботу [6].

Зі зростанням популярності бездротових пристроїв, мережі повинні бути здатні масштабуватися. Вони повинні дозволяти починати з малого, але легко розширюватися в плані покриття та пропускнуої здатності, без необхідності капітального ремонту або побудови нової мережі.

Створення надійної мережі – це не завдання одного компонента. Однак, мережевий брандмауер є ключовим елементом. Він забезпечує баланс між продуктивністю та безпекою, а також підтримує такі функції, як антивірусний захист, фільтрування спаму, глибока перевірка пакетів (DPI) та фільтрування додатків. [7].

Наприклад, можливість віддаленого керування маршрутизатором надає доступ до його налаштувань через мережу Інтернет. Функція WPS спрощує підключення нових пристроїв, дозволяючи ініціювати процес натисканням кнопки на маршрутизаторі, замість ручного введення пароля. Крім того, UPnP полегшує взаємодію пристроїв у локальній мережі, дозволяючи їм автоматично виявляти один одного. Хоча ці можливості можуть значно полегшити процес розширення мережі або надання доступу до Wi-Fi для гостей, вони потенційно можуть знизити рівень безпеки вашої мережі [8].

Ефективна стратегія безпеки бездротових мереж повинна бути багатошаровою і включати як технічні засоби захисту, так і організаційні заходи. Це забезпечить надійний захист від зростаючої кількості кіберзагроз у сучасному цифровому світі.

2 ОПИС СТАНДАРТУ 802.11AC

IEEE 802.11ac є наразі найпередовішим комерційним стандартом Wi-Fi, широко представленим на ринку. Хоча його часто асоціюють з п'ятим поколінням бездротових мереж, це визначення не є повністю коректним. Ключовими перевагами стандарту 802.11ac є суттєве збільшення пропускної здатності радіоканалу та вдосконалені механізми управління станом клієнтських пристроїв. Ці фактори призводять до значної економії енергоспоживання мобільних пристроїв.

Технологія 802.11ac функціонує виключно в діапазоні 5 ГГц. Тому двосмугові точки доступу часто продовжують використовувати стандарт 801.11n для роботи на частоті 2.4 ГГц. Однак, клієнтські пристрої з підтримкою 802.11ac отримують перевагу від роботи в менш завантаженому спектрі 5 ГГц [7].

Теоретичний максимум швидкості для 802.11ac становить близько 7 Гбіт/с, що досягається за рахунок конфігурації з 8 каналами по 160 МГц та модуляції 256-QAM, кожен з яких забезпечує 866.7 Мбіт/с. Ця висока швидкість також зумовлена впровадженням технології Multi User MIMO (MU-MIMO), яка дозволяє ефективно розподіляти просторові потоки та забезпечувати одночасну передачу даних кільком клієнтам [7].

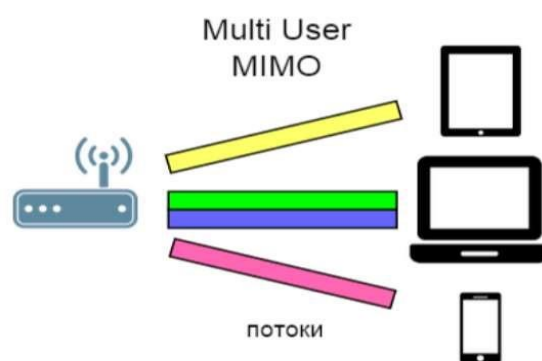


Рисунок 2.1 - Схема роботи технології MU-MIMO

Для реалізації цих можливостей був розроблений спеціальний формат кадру на фізичному рівні, що включає заголовок з інформацією про отримувачів. Варто зазначити, що швидкість передачі даних близько 900 МБ/с

перевищує можливості інтерфейсу SATA 3. Однак, в реальних умовах, через завантаженість ефіру та перешкоди, досягнення максимальної теоретичної швидкості є складним. Очікується, що реальна пропускна здатність буде в діапазоні 1.7-2.5 Гбіт/с, що значно перевершує теоретичний максимум стандарту 802.11n (600 Мбіт/с). [7].

2.1 Характеристики роботи стандарту в мережі IEEE 802.11ac

2.1.1 Частотні характеристики

Згідно з регуляціями FCC, діапазон частот UNII, що використовується стандартом 802.11ac, поділено на три окремі піддіапазони. Кожен з цих піддіапазонів має власні специфічні обмеження щодо максимальної потужності випромінювання. На відміну від попередніх версій стандарту IEEE 802.11, стандарт 802.11ac функціонує виключно в діапазоні 5 ГГц. Це призводить до суттєвих відмінностей у розподілі каналів порівняно з тим, що спостерігається у стандартах 802.11b/g/n (рис. 2.2) [5, 8].

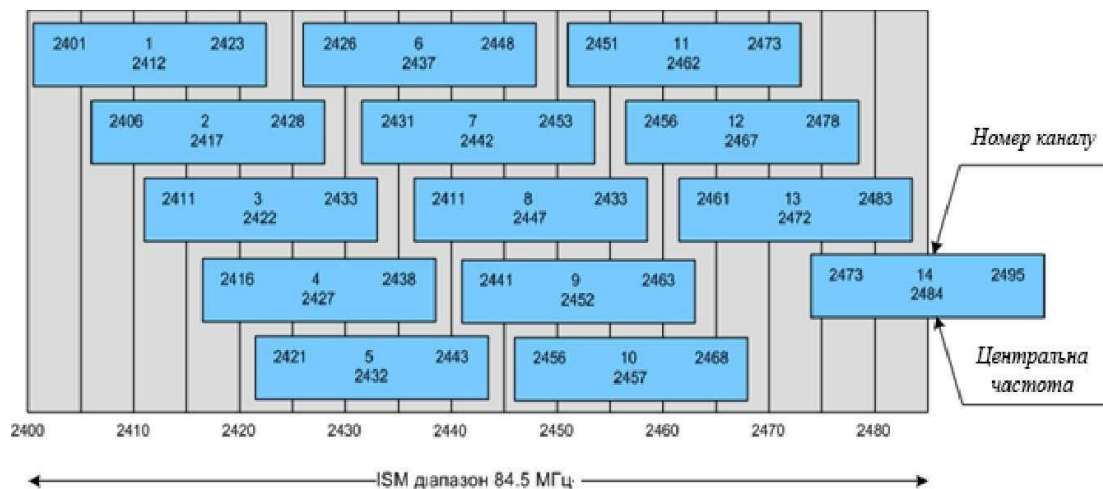


Рисунок 2.2 – Розподіл каналів для діапазону 2.4 ГГц

Діапазон частот розділено на три піддіапазони з відповідними обмеженнями потужності. Нижній піддіапазон (5170-5330 МГц) дозволяє використовувати потужність до 100 мВт. Середній піддіапазон (5470-5730 МГц) підтримує потужність до 250 мВт. Для верхнього піддіапазону (5715-5835 МГц) встановлено максимальну потужність 1 Вт [9]. Детальна схема розподілу частотних каналів представлена на рис. 2.3.

Нижній піддіапазон													
Канали	32	36	40	44	48	52	56	60	64				
Частоти	5160	5180	5200	5220	5240	5260	5280	5300	5320				
Середній піддіапазон													
Канали	96	100	104	108	112	116	120	124	128	132	136	140	144
Частоти	5480	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720
Верхній піддіапазон													
Канали	145	149	153	157	161	165							
Частоти	5725	5745	5765	5785	5805	5825							

Рисунок 2.3 – Розподіл каналів для діапазону 5 ГГц

Варто мати на увазі, що середній діапазон частот Wi-Fi може бути недоступний для деяких точок доступу. Це зумовлено тим, що використання певних частот регулюється залежно від регіону, для якого призначене обладнання, що позначається кодом країни (Country Code). Наприклад, європейські стандарти (ETSI) передбачають використання частот 5.18-5.32 та 5.48-5.72 ГГц. Для Сполучених Штатів та Канади спектр ширший: 5.16-5.32, 5.48-5.72 та 5.725-5.825 ГГц. У багатьох інших країнах діапазон може бути обмежений до 5.18-5.32 та 5.745-5.825 ГГц [10]. Тому при розробці Wi-Fi мереж та їх частотному плануванні необхідно враховувати ці регіональні особливості.

2.1.2 Фізичний рівень

Новий стандарт Wi-Fi 802.11ac був розроблений з урахуванням попередніх версій (802.11n та 802.11a). Це зроблено для того, щоб нові пристрої могли працювати зі старими, забезпечуючи безперебійну роботу мереж. Водночас, основна увага розробників була спрямована на значне збільшення швидкості передачі даних у стандарті 11ac [10].

На базовому, фізичному рівні, 11ac, як і його попередники 11a та 11n, використовує технологію OFDM (ортогональне частотне мультиплексування). Це дозволяє ефективно розділяти сигнал на багато менших частотних каналів для передачі даних. Принцип кодування та передачі бітів у 11ac схожий на той, що використовувався в 11n. Пристрої стандарту 11ac підтримують канали шириною 20, 40 та 80 МГц [10].

Щоб досягти значного приросту швидкості, у стандарті 802.11ac були додані нові можливості:

- більше просторових потоків: підтримка від 2 до 8 одночасних просторових каналів для передачі даних;
- розширені канали: можливість використання об'єднаних каналів шириною 80+80 МГц або суцільних каналів шириною 160 МГц;
- просторове кодування: застосування технології STBC (блочне кодування простір-час) для покращення надійності передачі;
- просунута модуляція: використання 256-QAM для більш щільного кодування даних;
- ефективне виправлення помилок: впровадження LDPC (контроль парності низької щільності) для зменшення кількості помилок при передачі;
- скорочений захисний інтервал: зменшення часу між пакетами даних до 400 нс для прискорення передачі;
- MIMO для кількох користувачів: технологія MU-MIMO дозволяє одночасно обслуговувати кілька пристроїв [11].

Таким чином пристрої, що відповідають базовим вимогам стандарту 802.11ac, можуть передавати дані зі швидкістю до 293 Мбіт/с. А пристрої, що використовують усі додаткові можливості, здатні досягати швидкості передачі даних, близької до 3,5 Гбіт/с.

Невикористовувані частотні піднесучі можуть бути встановлені на нуль. Це дозволяє пристрою передавати постійний сигнал або використовувати ці частоти як захисний інтервал. Канал шириною 80 МГц може бути розділений на дві суміжні смуги по 40 МГц, які не перекриваються. Канал шириною 160 МГц складається з двох частин по 80 МГц, які можуть бути як окремими, так і розташованими поруч. Технологія OFDM передбачає передачу даних по рівномірно розподілених піднесутих частотах, як показано в табл. 2.1 [12].

Щоб забезпечити зворотну сумісність з попередніми поколіннями 802.11, пристрої 802.11ac вставляють спеціальний заголовок у кожну 20 МГц підсмугу для синхронізації. Це призводить до підвищення PAPR (відношення пікової потужності до середньої), що знижує ефективність роботи підсилювачів. Для пом'якшення цього недоліку застосовується обертання сигналу в верхній 20 МГц підсмугі (табл. 2.2). Цей метод вже був реалізований у стандарті 802.11n для роботи з 40 МГц каналами.

Таблиця 2.1 - Розподіл піднесучих частот за половою у 802.11ac

Смуга частот, МГц	Кількість піднесучих частот	Піднесучі, де проходить передача сигналу, МГц
20	64	-28...-1, 1..28
40	128	-58...-2, 2..58
80	256	-122...-2, 2...122
160	512	-250...-130, -126...-6, 6...126, 130...250
80+80	256 на кожному каналі	-122...-2, 2...122

Таблиця 2.2 – поворот піднесучих частот

Смуга частот, МГц	Кількість повернутих піднесучих, МГц	Кут повороту
20	Відсутні	-
40	≥ 0	90° (j)
80	≥ -64	180° (-1)
160	-192...-1, ≥ 64	180° (-1)
80+80	Ті самі, що й для випадку в 80 МГц для кожної половини каналу	180° (-1)

Важливою відмінністю стандарту IEEE 802.11ac від попередніх є суттєво менший набір індексів MCS, які визначають методи модуляції. Як свідчить табл. 2.3, стандарт 802.11ac пропонує лише 10 таких індексів, тоді як у стандарті 802.11n їх налічується 77 [9].

Таблиця 2.3 – MCS-індекси стандарту IEEE 802.11ac [9]

MCS	Модуляція	Кодування	RCE
0	BPSK	1/2	-5
1	QPSK	1/2	-10
2	QPSK	3/4	-13
3	16QAM	1/2	-16
4	16QAM	3/4	-19
5	64QAM	2/3	-22
6	64QAM	3/4	-25
7	64QAM	5/6	-28
8	256QAM	3/4	-30
9	256QAM	5/6	-32

2.2 Формат пакетів в мережі 802.11ac

На рис. 2.4 представлена структура пакета, що використовується в стандарті 802.11ac. Перші три поля пакета – L-STF (коротка тестова послідовність), L-LTF (довга тестова послідовність) та L-SIG (сигнальне поле) – призначені для виявлення корисного сигналу та містять критично важливу інформацію. Ці тестові послідовності дозволяють пристрою оцінити зміщення частоти, тимчасову синхронізацію та інші необхідні налаштування. Префікс "L" у назвах цих полів означає "legacy", тобто вони успадкувалися від попередніх версій стандарту Wi-Fi. Це забезпечує сумісність із старішими пристроями. Поле L-SIG, окрім іншого, інформує про довжину всього пакета [9].

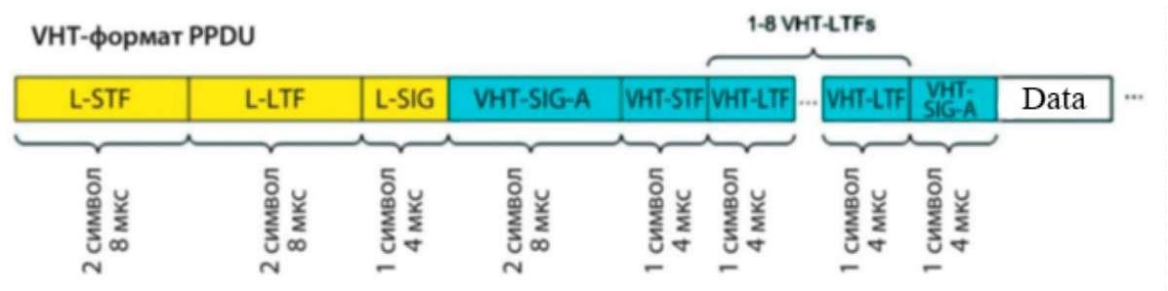


Рисунок 2.4 - Структура пакета 802.11ac

Стандарт 802.11ac запровадив нові поля, позначені як VHT (Very High Throughput), які відіграють ключову роль у забезпеченні високої швидкості передачі даних.

Поле VHT-SIGA складається з двох OFDM-символів:

- перший символ модулюється за допомогою BPSK. Його призначення – дозволити пристроям, що працюють за попереднім стандартом 11n, розпізнати пакет як такий, що відповідає формату 11a. Це забезпечує зворотну сумісність;

- другий символ модулюється за допомогою BPSK зі зсувом фази на 90 градусів. Це дозволяє пристроям, що підтримують VHT, ідентифікувати пакет як такий, що відповідає стандарту 11ac. Цей символ також містить важливу інформацію про параметри передачі, такі як ширина смуги пропускання, схема модуляції та кодування [9].

Важливо зазначити, що всі ці поля повторюються для кожних 20 МГц ширини смуги пропускання, що дозволяє ефективно використовувати доступний спектр.

Поле VHT-STF (VHT Short Training Field) призначене для автоматичного налаштування коефіцієнта посилення при передачі. Це особливо важливо в умовах багатопроменевості, коли сигнал може досягати приймача різними шляхами, що призводить до спотворень [9].

Наступні поля, VHT-LTF (VHT Long Training Field), використовуються пристроєм для точної оцінки стану каналу зв'язку MIMO (Multiple-Input Multiple-Output). На основі цієї інформації пристрій може здійснити підстроювання антени для оптимального прийому сигналу [9].

Останнє поле перед фактичними даними – це VHT-SIG-B. Воно модулюється за допомогою BPSK і містить наступну інформацію про довжину корисних даних у пакеті:

- для MU-MIMO (Multi-User MIMO) - у сценаріях одночасної передачі даних кільком користувачам, поле VHT-SIG-B також передає інформацію про схему кодування (MCS) та модуляції, що застосовується до кожного користувача;
- для одиничного користувача - у випадках передачі даних одному користувачеві, відповідна інформація про схему кодування та модуляції передається в полі VHT-SIG-A [9].

Подібно до VHT-SIG-A, до поля VHT-SIG-B також може застосовуватися обертання фази на кожній 20 МГц ділянці смуги пропускання для оптимізації передачі.

3 АНАЛІЗ ТА ВИБІР МЕТОДІВ ПОБУДОВИ КОРПОРАТИВНОЇ БЕЗДРОТОВОЇ МЕРЕЖІ

3.1 Визначення методів оптимізації бездротової мережі

Для досягнення максимальної продуктивності бездротової мережі під час її створення необхідно впроваджувати спеціальні оптимізаційні заходи. Це досягається шляхом застосування різноманітних методів оптимізації, які є ефективними інструментами для будь-якої науково-практичної роботи.

Зокрема, для оптимізації корпоративної Wi-Fi мережі рекомендується застосовувати наступні практичні методи:

- раціональне розміщення точок доступу - включає визначення оптимальної кількості точок, ефективний розподіл частотних каналів та правильне налаштування програмного забезпечення;
- використання діапазону 5 ГГц: активне застосування сучасних стандартів Wi-Fi (IEEE 802.11ac та IEEE 802.11n) дозволяє значно збільшити швидкість передачі даних та покращити покриття мережі;
- детальне радіопланування передбачає розрахунок зони покриття кожної точки доступу, візуалізацію на плані будівлі та визначення найвигіднішого розташування для максимального охоплення;
- забезпечення безшовного роумінгу дозволяє користувачам, які переміщуються, залишатися підключеними до мережі без помітних перерв та затримок;
- керування пріоритетами трафіку дозволяє встановлювати обмеження швидкості для кожного користувача та надавати пріоритет критично важливим мережевим сервісам [4].

У подальшому дослідженні будуть детально розглянуті саме ці методи, як найбільш ефективні та широко застосовувані на практиці.

3.2 Алгоритми оптимізації бездротової мережі

Процес оптимізації корпоративної бездротової мережі починається із формування чіткого алгоритму дій. Ключовим етапом є визначення основного

параметра, який буде орієнтиром для оптимізації. Далі необхідно проаналізувати такі критерії:

- оптимізація зони покриття;
- оптимізація швидкості передачі даних;
- оптимізація доступності мережевих ресурсів [4].

Для кожного з цих напрямів оптимізації розроблено відповідні алгоритми, ілюстровані блок-схемами рис. 3.1.

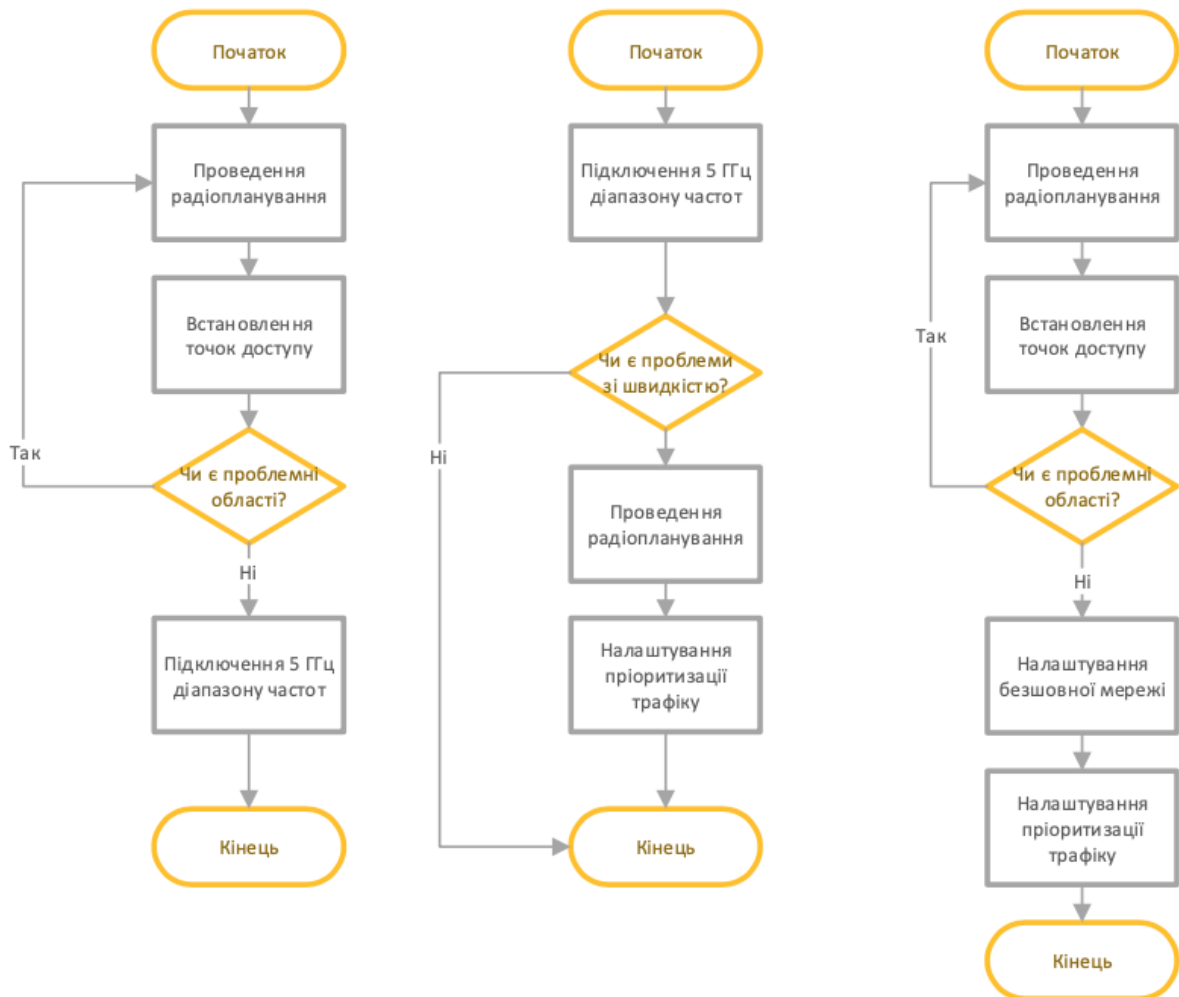


Рисунок 3.1 - Блок-схеми алгоритмів оптимізації покриття (ліворуч), швидкості (у центрі) та доступності мережі (праворуч)

Аналіз представленого зображення демонструє наявність універсальних компонентів у структурі алгоритмів. Це зумовлено критичною потребою в застосуванні певних оптимізаційних технік, які є практично невід'ємними при розробці будь-яких Wi-Fi мереж, незалежно від їхнього призначення – чи то домашнього, чи то корпоративного.

3.3 Особливості реалізації корпоративної бездротової мережі

Метою даної роботи є створення та перевірка методик і алгоритмів оптимізації бездротової частини локальної корпоративної мережі доступу. Для експериментальної платформи буде застосована бездротова мережа офісного центру, а також буде розроблений оптимальний порядок дій для підвищення ефективності її впровадження.

У приміщеннях є зони відведені під окремі офіси, також конференц-зали для проведення відеотренінгів, семінарів, «круглих столів» з онлайн трансляцією і ін.

Будинок триповерховий, у якому розташовано 42 робочих місця з дротовим підключенням. Окрім того, передбачено створення двох окремих бездротових гостьових підмереж, до яких зможуть підключатися відвідувачі трьох конференц-залів та кафе.

Інтернет-провайдер забезпечує пропускну здатність вхідного інтернет-каналу до 1000 Мбіт/с, проте реальна швидкість зазвичай виявляється меншою через багаторівневу обробку трафіку, втрати під час передачі та інші фактори. Результати тестування фактичної швидкості проводового інтернет-з'єднання наведені в таблиці 3.1. Тестування виконувалося з комп'ютера на базі процесора AMD Ryzen 5 1600X, за допомогою гігабітної мережевої карти, із застосуванням шести різних онлайн-сервісів у браузері Google Chrome.

Таблиця 3.1 – Результати тестування швидкості інтернету

Назва тесту	Швидкість завантаження по Україні, Мб/с	Швидкість передачі по Україні, Мб/с	Швидкість завантаження у світі, Мб/с	Швидкість передачі у світі, Мб/с
Speedtest by Ookla	823	760	312	201
speedtest.net.ua	570	682	72	45
Lurenet speedtest	860	726	197	380
Speedtest.su	880	677	418	317
Укртелеком Speedtest	507	365	-	-

Отже, ми можемо визначити максимальні швидкості для майбутніх бездротових мереж. Однак, при їх розробці важливо пам'ятати, що навіть за відсутності радіоперешкод та хорошого покриття сигналу, інші чинники можуть спричинити нестабільність мережі. Наприклад, некоректне встановлення обладнання може викликати проблему "прихованих вузлів", що призводить до збоїв зв'язку навіть у добре спланованих мережах. Крім того, сторонні джерела шуму на об'єкті можуть призводити до розривів з'єднання.

3.4 Недоліки існуючої мережі та розробка загальних вимог до оновлення обладнання

Наразі бездротова мережа установи функціонує на базі п'яти стандартних Wi-Fi маршрутизаторів, які підключені до головного маршрутизатора (шлюзу) через гігабітну мережу. Ця конфігурація є застарілою та має низку суттєвих недоліків:

- нерівномірне покриття: розташування маршрутизаторів не оптимізоване, що призводить до появи значних "мертвих зон", де сигнал Wi-Fi відсутній або дуже слабкий;
- проблеми зі стабільністю сигналу: спостерігається висока кількість конфліктів між пристроями (колізій) та негативний вплив зовнішніх електромагнітних завад, що знижує якість зв'язку;
- відсутність контролю доступу: немає механізмів для моніторингу та управління користувачами бездротової мережі;
- ризики безпеки через відсутність гостьової мережі: не виділено окремої підмережі для гостей. Це означає, що відвідувачі установи потенційно можуть отримати доступ до конфіденційної інформації та ресурсів корпоративної мережі;
- обмежені можливості створення гостьової мережі: через використання звичайних Wi-Fi маршрутизаторів замість спеціалізованих точок доступу, неможливо створити єдину, централізовано керовану гостьову підмережу. Кожен маршрутизатор створює власну ізольовану мережу;

- відсутність пріоритизації трафіку: немає можливості налаштувати пріоритет для різних типів трафіку (наприклад, для відеоконференцій або критично важливих додатків), що може призводити до уповільнення роботи;
- проблеми з роумінгом: користувачі, переміщуючись по території установи, змушені вручну перепідключатися до різних точок доступу, що незручно та перериває роботу;
- неефективне використання пропускну здатності: поточна мережа не використовує весь потенціал доступного каналу передачі даних [9].

Зважаючи на виявлені недоліки, для забезпечення стабільної та ефективної роботи бездротової мережі установи необхідно встановити нове обладнання. Зокрема, потрібна певна кількість потужних дводіапазонних точок доступу, які підтримують сучасний стандарт Wi-Fi 802.11ac. Важливою функцією є Multiple SSID, що дозволить створити окрему, безпечну підмережу для гостей.

Крім того, необхідний окремий Wi-Fi маршрутизатор, який буде виконувати роль бездротового контролера. Такий пристрій повинен мати розширені можливості для управління трафіком та централізованого керування всіма точками доступу.

Також для підвищення мобільності користувачів стаціонарних комп'ютерів та зменшення витрат на прокладання кабелів, пропонується підключити деякі ПК до нової бездротової мережі. Це можна реалізувати за допомогою компактних Wi-Fi USB адаптерів, які підключатимуться до комп'ютерів як зовнішні модулі.

4 РОЗРОБКА ТА ОПТИМІЗАЦІЯ БЕЗДРОТОВОЇ МЕРЕЖІ ДОСТУПУ ОФІСНОГО ЦЕНТРУ

4.1 Розрахунок кількості точок доступу

Після етапу формування вимог до корпоративної бездротової мережі, здійснюється розрахунок її навантажувальних характеристик. Цей розрахунок, як правило, дозволяє визначити необхідну кількість точок доступу. Першочергово проводиться збір відомостей щодо профілю користувацьких пристроїв. У випадку створення мережі для офісного середовища, що є актуальним для даного проекту, здійснюється аналіз характеристик абонентських станцій, які вже експлуатуються або будуть введені в експлуатацію. Якщо визначення типу пристроїв заздалегідь неможливе, наприклад, при розгортанні мережі Wi-Fi у місцях з високою щільністю відвідувачів, для проведення розрахунків застосовуються усереднені дані з типовими характеристиками (табл. 4.1) [4].

Таблиця 4.1 – Типові характеристики основних Wi-Fi пристроїв

Тип пристрою	Тип радіомодуля	Підтримка каналів	Ширина каналу, МГц	Потужність передавача, дБм	Максимальна швидкість передачі даних, Мбіт/с
Смартфон	802.11g/n	1-13	20	11	54
Потужний смартфон	802.11n/ac 1 x 1:1	1-13, 36-64	20/40	11-14	65-72
Планшет	802.11n/ac 1 x 1:1	1-13, 36-64	20/40	11-14	65-72
Бюджетний ноутбук	802.11n 2 x 3:2	1-13, 36-64	20/40	17-20	144/300
Ноутбук	802.11n/ac 3 x 3:3	1-13, 36-64	20/40	17-20	216/450

Щоб визначити, наскільки завантажена бездротова мережа, можна застосувати метод, який базується на аналізі часу, протягом якого пристрої використовують радіоканал (так званий "airtime"). На цьому етапі ключову роль

відіграють не самі точки доступу, а характеристики пристроїв користувачів, оскільки саме вони створюють основне навантаження. Для подальших розрахунків потрібно врахувати такі параметри: стандарт Wi-Fi (наприклад, 802.11g/n/ac), конфігурацію MIMO (кількість антен, наприклад: 1x1, 2x2 і т.д.), доступні радіочастотні діапазони та канали, ширину каналу (20, 40 МГц), потужність передавача та максимальну швидкість на фізичному рівні. Після цього необхідно проаналізувати, які програми використовуватимуть користувачі, і для кожного типу використання визначити необхідну швидкість передачі даних (табл. 4.2).

Таблиця 4.2 – Середні показники необхідної пропускної здатності [8]

Тип використання	Необхідна пропускна здатність, Мбіт/с
Веб-брузинг/пошта/соц. мережі	0.5-1
Відео-конференції	0.5-1
SD відео	1-1.5
HD відео	2-5
4K відео	25-30
Передача файлів	5-20
Інтернет-телефонія	0.03-0.1

Стає можливим розрахувати необхідну кількість радіомодулів (і, відповідно, точок доступу) для забезпечення обслуговування абонентських станцій певного типу, які використовують задану програму. Процес починається з визначення числа абонентських станцій, що функціонують у діапазоні 2,4 ГГц (4.1), а потім переходить до визначення числа станцій у діапазоні 5 ГГц (4.2).

$$Q_{2,4} = Q \cdot k_{2,4}, \quad (4.1)$$

$$Q_5 = Q \cdot k_5, \quad (4.2)$$

де $k_{2,4}/k_5$ - це коефіцієнти використання діапазонів 2,4/5 ГГц відповідно. Тобто, при $k_{2,4}=0,6$, в діапазоні 2,4 ГГц буде працювати 60% відсотків абонентів, а в діапазоні 5 ГГц - буде 40%;

Q - загальне число абонентських станцій, які повинна обслуговувати мережа Wi-Fi. Відповідно:

$$Q_{2,4} = 200 \cdot 0.6 = 120$$

$$Q_5 = 200 \cdot 0.4 = 80$$

Подальший етап передбачає визначення відсотка часу активності радіоканалу, зумовленої передачею певного виду трафіку пристроєм A_t .

$$A_t = (V_{app}/V_{max}) \cdot 100\%, \quad (4.3)$$

де V_{app} - необхідна швидкість передачі даних, V_{max} - максимальна швидкість передачі даних, на якій може працювати абонентська станція. Тобто:

$$V_{max} = V_{maxPHY} \cdot c = 300 \cdot 0,067 = 200,$$

де c - коефіцієнт втрати пропускної здатності, що знаходиться в діапазоні $[0,4-0,6]$. Даний коефіцієнт відображає ступінь зниження ефективної швидкості передачі даних на транспортному рівні (наприклад, TCP або UDP) відносно теоретичного максимуму на фізичному рівні (табл. 4.1). При коефіцієнті 0,4, максимальна швидкість передачі даних обмежується 40% від максимальної. Цей консервативний прогноз є доцільним для проектування високопродуктивних Wi-Fi мереж, що передбачають значне навантаження та велику кількість одночасних підключень. При коефіцієнті 0,6, максимальна швидкість передачі даних може сягати 60% від максимальної. Цей оптимістичний прогноз може бути застосований для офісних середовищ з низькою щільністю користувачів. Тобто:

$$A_t = (20/200) \cdot 100\% = 10\%.$$

Далі здійснюється розрахунок загальної відсоткової частки використання радіоканалу всіма абонентськими станціями для кожного з відповідних діапазонів

$$A_{\Sigma 2.4} = Q_{2.4} \cdot A_{t2.4} \quad (4.4)$$

$$A_{\Sigma 5} = Q_5 \cdot A_{t5} \quad (4.5)$$

Проведемо розрахунок:

$$A_{\Sigma 2.4} = 80 \cdot 4\% = 320\%$$

$$A_{\Sigma 5} = 120 \cdot 6\% = 720\%$$

Підсумовуючи, ми визначаємо, скільки радіомодулів кожного типу нам потрібно, щоб усі пристрої, які користуються певними програмами, мали стабільний зв'язок.

$$R_{2.4} = \frac{A_{\Sigma 2.4}}{80\%} = \frac{320}{80} = 4$$

$$R_5 = \frac{A_{\Sigma 5}}{80\%} = \frac{720}{80} = 9$$

Згідно з розрахунками $R_{2.4}$ та R_5 , прийнято, що кожен радіомодуль ефективно використовується для обробки корисного трафіку лише 80% часу, тоді як решта 20% відводиться на службовий та керуючий трафік [10].

При наявності в мережі різних типів станцій або різноманітних додатків користувачів, відповідні вимоги підсумовуються. Після визначення необхідної кількості радіомодулів, можна розрахувати число точок доступу. Для цього необхідно обрати постачальника обладнання (наприклад, Cisco, Aruba Networks, Ruckus Wireless) та конкретну модель точки доступу. Виробники пропонують широкий вибір точок доступу з різними характеристиками радіомодулів, включаючи моделі з одним радіомодулем (працює в діапазоні 2,4 або 5 ГГц) та з двома радіомодулями (одночасно в обох діапазонах). Ця різноманітність дозволяє оптимізувати вибір з точки зору співвідношення ціни та продуктивності.

4.2 Аналіз виробників обладнання

Ruckus Wireless

Компанія Ruckus Wireless пропонує гнучкі рішення для побудови бездротових мереж, що відповідають потребам як невеликих, так і масштабних організацій.

Для невеликих мереж (до 50 точок доступу, до 1000 клієнтів) Ruckus Unleashed – це просте та ефективне рішення, яке не потребує окремого контролера. Функції керування вбудовані в одну з точок доступу. Це забезпечує надійність та високу швидкість роботи, хоча й дещо обмежує продуктивність самої точки, що виконує роль контролера [11].

Для великих та корпоративних мереж (понад 50 точок доступу, понад 1000 клієнтів) ZoneDirector або SmartZone – це потужні апаратні або програмні контролери, які дозволяють створювати практично необмежені за масштабом мережі. Вони підтримують до 30 000 точок доступу та 300 000 клієнтів, що з запасом покриває потреби будь-якого бізнесу, муніципалітету чи державної установи [11].

Ключові переваги Ruckus:

- висока продуктивність та надійність: обладнання Ruckus відоме своєю стабільністю та здатністю працювати без збоїв протягом тривалого часу (кілька років безперервної роботи – це норма). Воно легко справляється з високою щільністю клієнтів, що робить його ідеальним для місць масового скупчення людей (стадіони, конференц-зали, виставки), а також для вимогливих завдань, таких як відеоспостереження та VR;
- сучасні технології: Ruckus підтримує найновіші стандарти Wi-Fi (802.11g/n/ac та новіші), забезпечуючи високу швидкість та ефективність;
- інтелектуальне керування сигналом (BeamFlex): унікальна технологія BeamFlex робить антени точок доступу "розумними". Вони динамічно спрямовують сигнал туди, де знаходяться клієнти, і уникають випромінювання в порожні зони. Це значно покращує якість зв'язку та зменшує перешкоди;
- оптимізація для мобільних пристроїв: кожна точка доступу може створювати до 4000 унікальних діаграм спрямованості сигналу, адаптуючись до постійного руху мобільних пристроїв користувачів у реальному часі;
- безшовний роумінг: підтримка протоколів IEEE 802.11r/k/v забезпечує плавне перемикання між точками доступу без втрати зв'язку;
- висока якість виготовлення: обладнання Ruckus відрізняється надійністю та довговічністю;
- підтримка сучасних стандартів: впроваджені актуальні технології, такі як Beamforming, Airtime Fairness, Band Steering, MU-MIMO, WMM, для максимальної ефективності мережі;

- відмовостійкість: рішення Ruckus включають технології для забезпечення безперервної роботи, такі як дублювання компонентів;
- максимальна безпека: забезпечується найсучаснішими методами шифрування, виявлення та запобігання атакам;
- сервісна підтримка: можливість покриття обладнання сервісними контрактами, що гарантують швидку заміну несправного пристрою протягом одного робочого дня.

Ruckus Wireless пропонує комплексні рішення для побудови бездротових мереж, які відзначаються високою продуктивністю, надійністю та масштабованістю. Від простих рішень для малого бізнесу до потужних систем для великих підприємств та громадських установ, Ruckus забезпечує стабільний та швидкий доступ до мережі, використовуючи передові технології для оптимізації роботи та безпеки.

MikroTik

Компанія MikroTik (Mikrotikls Ltd), що базується в Латвії, є значним гравцем на ринку мережевого обладнання. Вона займається повним циклом розробки та виробництва інноваційних рішень для мережевої інфраструктури, включаючи маршрутизатори, комутатори, бездротові пристрої та точки доступу. Фундаментальною перевагою продукції MikroTik є інтегрована операційна система RouterOS, розроблена самою компанією. Ця ОС надає обладнанню розширений функціонал та відкриває широкі можливості для конфігурації. Більшість маршрутизаторів та точок доступу MikroTik підтримують технологію живлення Power over Ethernet (PoE). Однією з ключових конкурентних переваг є значно нижча вартість обладнання порівняно з аналогами, при цьому функціональні можливості залишаються на високому рівні. Процес налаштування спрощується завдяки наявності великої кількості готових скриптів. Компанія пропонує широкий вибір високопродуктивних маршрутизаторів з різним ціновим діапазоном. Навіть найбюджетніші моделі вирізняються багатофункціональністю, практичністю, компактним дизайном, доступністю та легкістю впровадження [12].

Типово, маршрутизатори MikroTik оснащуються високоякісними процесорами та значним обсягом оперативної пам'яті, що робить їх універсальними рішеннями для будь-яких мережевих сценаріїв.

Важливою перевагою є включення в комплект ліцензії RouterOS різних рівнів, що дозволяє навіть найпростішим маршрутизаторам отримати функціонал рівня Enterprise. Серед підтримуваних технологій варто виділити: динамічну маршрутизацію (Dynamic routing), функціонал Hotspot, потужний міжмережевий екран (Firewall), MPLS, VPN, розширені можливості управління якістю обслуговування (QoS), балансування навантаження та моніторинг мережевих параметрів у реальному часі. Деякі бездротові моделі додатково оснащені роз'ємами MiniPCI та USB, що розширює можливості для побудови складних та високопродуктивних Wi-Fi мереж. Маршрутизатори MikroTik відзначаються високою надійністю та стабільністю роботи, що робить їх придатними для створення відмовостійких рішень у корпоративному секторі [12].

Ключові характеристики рішень MikroTik:

- підтримка актуальних стандартів Wi-Fi для забезпечення високої пропускної здатності;
- власні розробки для реалізації безшовного роумінгу між точками доступу;
- гарантована стабільність функціонування;
- високий рівень кібербезпеки, що досягається завдяки підтримці сучасних протоколів шифрування та механізмів виявлення й запобігання атакам;
- можливості інтеграції з існуючими системами моніторингу мережевої інфраструктури;
- економічна ефективність, що проявляється у низькій вартості обладнання.

Ubiquiti

Компанія Ubiquiti приділяє значну увагу дизайну на всіх етапах – від упаковки до інтерфейсів управління. Їхня продукція вирізняється привабливим співвідношенням ціни та якості, пропонуючи високу продуктивність за помірну вартість [11].

Однак, варто зазначити, що Ubiquiti не забезпечує справжній безшовний роумінг Wi-Fi згідно зі стандартами IEEE. Натомість вони пропонують власну реалізацію цієї функції. Тому для критично важливих завдань, де потрібна бездоганна робота роумінгу клієнтів, рішення від Ubiquiti можуть не підійти.

Крім того, в Україні відсутні офіційний сервіс та представництво компанії, що може бути суттєвим недоліком [11].

Незважаючи на певні недоліки, Ubiquiti залишається одним із лідерів ринку бездротових рішень завдяки потужній компонентній базі, широкому асортименту обладнання та ефективній маркетинговій стратегії. Головною перевагою є їхня екосистема UniFi. Вона охоплює не лише Wi-Fi обладнання, але й комутатори, маршрутизатори, системи відеоспостереження, IP-телефонію та навіть компоненти для "розумного будинку". Управління всією системою здійснюється через зручне програмне забезпечення, включаючи мобільний додаток, що інтегрується з хмарними сервісами Ubiquiti [11].

Ключові особливості рішень Ubiquiti:

- розширена екосистема UniFi: Комплексні рішення, що включають комутатори, маршрутизатори, точки доступу, IP-телефони та камери відеоспостереження.
- висока швидкість: підтримка найсучасніших стандартів Wi-Fi для гігабітних швидкостей передачі даних;
- власний роумінг: запатентована технологія для забезпечення роумінгу, хоча й не повністю стандартизована;
- сучасні технології: підтримка актуальних стандартів, таких як Beamforming, Airtime Fairness, Band Steering;
- мобільне управління: можливість керувати та моніторити мережу через мобільний додаток;
- привабливий дизайн: сучасний та естетичний вигляд як обладнання, так і програмного забезпечення;
- технічна підтримка: цілодобова онлайн-підтримка англійською мовою;
- доступна ціна: одні з найнижчих цін на ринку при високій якості.

Загалом, Ubiquiti пропонує привабливі рішення для побудови мереж, особливо для тих, хто цінує інтегровані системи, сучасний дизайн та доступну вартість, але потребує уважного ставлення до питань стандартизованого роумінгу та офіційної підтримки в Україні.

TP-LINK

Для початку слід розуміти, що бренд TP-LINK насправді включає в себе два напрямки. Один з них займається виробництвом недорогих домашніх

роутерів і пластикових комутаторів, а інший спеціалізується на продуктах корпоративного рівня – корпоративних Wi-Fi системах, серії комутаторів Smart та відповідних аксесуарах. По суті, це дві різні компанії, оскільки між цими сегментами немає спільних розробок чи виробничих процесів. Причому корпоративний TP-LINK відрізняється значно вищою якістю [13].

У лінійці TP-LINK представлена серія Auronet CAP, яка наразі перебуває у дещо забутому стані, хоча це тимчасово. Це рішення розраховане на управління до 500 точок доступу і до 10 000 бездротових клієнтів. Контролери доступні лише у вигляді апаратних пристроїв з підтримкою 50 або 500 точок доступу. Точки доступу мають доволі застарілий дизайн, але підтримують повноцінний безшовний роумінг згідно зі стандартами 802.11k/v, а також функції Beamforming, Band Steering і Airtime Fairness – тобто набір якостей тут дуже повний [13].

Інша екосистема TP-LINK – Omada, яка включає точки доступу серії EAP. Контролер Omada існує у вигляді апаратного пристрою з обмеженням до 50 точок у мережі, а також у програмній версії, яку можна встановити на сервер під керуванням Windows або Linux [13].

Рішення TP-LINK відзначаються такими характеристиками:

- підтримка новітніх Wi-Fi стандартів із забезпеченням гігабітних швидкостей передачі даних;
- висока продуктивність, здатність витримувати суттєві навантаження (понад 50 користувачів на одну точку доступу);
- підтримка протоколів безшовного роумінгу 802.11r/k/v;
- якісне виготовлення та стабільність роботи;
- підтримка сучасних технологій, зокрема Beamforming, Airtime Fairness, Band Steering, WMM, MU-MIMO;
- наявність механізмів відмовостійкості, зокрема дублювання ключових компонентів;
- забезпечення високого рівня інформаційної безпеки за рахунок підтримки сучасних стандартів шифрування, виявлення та запобігання атакам;
- інтеграція із системами моніторингу.

Після ретельного аналізу вимог організації, порівняння сильних та слабких сторін мережеских рішень від різних виробників, а також врахування фінансових обмежень, було прийнято обґрунтоване рішення на користь

системи безпроводового роумінгу від MikroTik. Такий вибір дозволить повністю покрити потреби установи в корпоративній бездротовій мережі та забезпечить бездоганну інтеграцію з основною локальною мережею, яка вже побудована на обладнанні MikroTik.

4.3 Вибір обладнання для бездротової мережі

На даний момент ринок мережевого обладнання представлений широким спектром пристроїв, що відповідають останнім стандартам. Однак, значні цінові розбіжності між пропозиціями від провідних виробників ускладнюють вибір оптимального рішення. Враховуючи обмежений бюджет, виділений для державної установи, процес підбору необхідного устаткування стає ще більш викликом.

4.3.1 Вибір маршрутизатора Wi-Fi

Першим кроком у побудові нашої бездротової мережі є вибір Wi-Fi маршрутизатора, який буде виконувати роль центрального контролера. Компанія MikroTik має в своєму арсеналі кілька пристроїв, що ідеально підходять для цієї задачі. Вони відповідають таким критеріям: підтримка сучасного стандарту IEEE 802.11ac, достатня продуктивність для одночасної роботи з 200 користувачами, наявність гігабітних LAN-портів та інтегровані Wi-Fi антени. Серед рекомендованих моделей – Mikrotik hAP ac (випущений у 2016 році), а також Mikrotik hAP ac2 та Mikrotik RB4011iGS+5HacQ2HnD-IN, які з'явилися на ринку у 2018 році. Всі ці маршрутизатори є цілком придатними для створення надійної бездротової мережі [14].

Особливу увагу варто приділити моделі Mikrotik RB4011iGS+5HacQ2HnD-IN (рис. 4.1). Цей пристрій є найпродуктивнішим серед запропонованих, забезпечує повну підтримку технології MU-MIMO та обіцяє вражаючу пропускну здатність до 1733 Мбіт/с на частоті 5 ГГц [14].

З основними технічними характеристиками маршрутизатора можна ознайомитись у табл. 4.3.



Рисунок 4.1 – бездротовий дводіапазонний маршрутизатор Mikrotik RB4011iGS+5HacQ2HnD-IN

Таблиця 4.3 – технічні характеристики Mikrotik RB4011iGS+5HacQ2HnD-IN [14]

Операційна система	RouterOS Layer 5
Процесор	AL21400, 1.4 ГГц (4 ядра)
Оперативна пам'ять	1 Гб
Постійна пам'ять	512 МБ
Тип інтерфейсу WAN/LAN	10/100/1000 BASE-TX Ethernet з підтримкою POE, SFP порт
Кількість Ethernet інтерфейсів	10
Кількість зовнішніх антен	4
Кількість внутрішніх антен	2
Безпроводові інтерфейси	802.11 a/b/g/n (до 300 Мбіт/с), 802.11ac (до 1777 Мбіт/с);
Підтримка протоколів	DHCP, PPPoE, IPsec, L2TP, PPTP
функції VPN	OpenVPN / PPTP VPN
Режими шифрування	64/128-бітний WEP, WPA/WPA2, WPA-PSK/ WPA2-PSK

На основі цих міркувань, ми обираємо бездротовий маршрутизатор, що гарантовано задовольнить вимоги установи та створить основу для подальшого розвитку мережевої інфраструктури.

4.3.1 Вибір точки доступу

Наступним кроком є вибір настінних точок доступу, які не тільки розширяють покриття нашої Wi-Fi мережі, але й забезпечать ефективну роботу в режимі кількох SSID. Для побудови надійної мережі, здатної обслуговувати до ста одночасних клієнтів, необхідне відповідне обладнання.

MikroTik пропонує диференційований підхід до своїх точок доступу. Серед усіх доступних моделей, Mikrotik cAP ac (RbсAPGi-5acD2nD), представлена навесні 2018 року, є оптимальним вибором для наших потреб [15].

Ця модель (рис. 4.2) підтримує роботу в діапазонах 2.4 ГГц та 5 ГГц, має чотири вбудовані антени та ідеально підходить для настінного або стельового монтажу. Живлення пристрою може здійснюватися за допомогою технології PoE (IEEE802.3af). Завдяки підтримці 3x3:3 MIMO, Mikrotik cAP ac дозволяє створювати до восьми незалежних SSID на кожному з частотних діапазонів. Це надає широкі можливості для побудови багаторівневих підмереж, зокрема для ізольованого доступу гостей [15].



Рисунок 4.2 – Бездротова дводіпазонна точка доступу Mikrotik cAP ac

Технічні характеристики точки доступу представлені у табл. 4.4.

Таблиця 4.4 – технічні характеристики Mikrotik cAP ac

Операційна система	RouterOS
Процесор	IPQ-4018, 0.716 ГГц (4 ядра)
Оперативна пам'ять	128 МБ
Постійна пам'ять	16 МБ
Тип інтерфейсу Ethernet	10/100/1000 BASE-TX Ethernet з підтримкою PoE, SFP порт
Кількість Ethernet інтерфейсів	2
Кількість внутрішніх антен	4
Бездротові інтерфейси	802.11 a/b/g/n (до 300 Мбіт/с), 802.11ac (до 867 Мбіт/с);
Кількість multiple SSID	16
Підтримка протоколів	DHCP, PPPoE, IPsec, L2TP, PPTP
Режими шифрування	64/128-бітний WEP, WPA/WPA2, WPA-PSK/WPA2-PSK

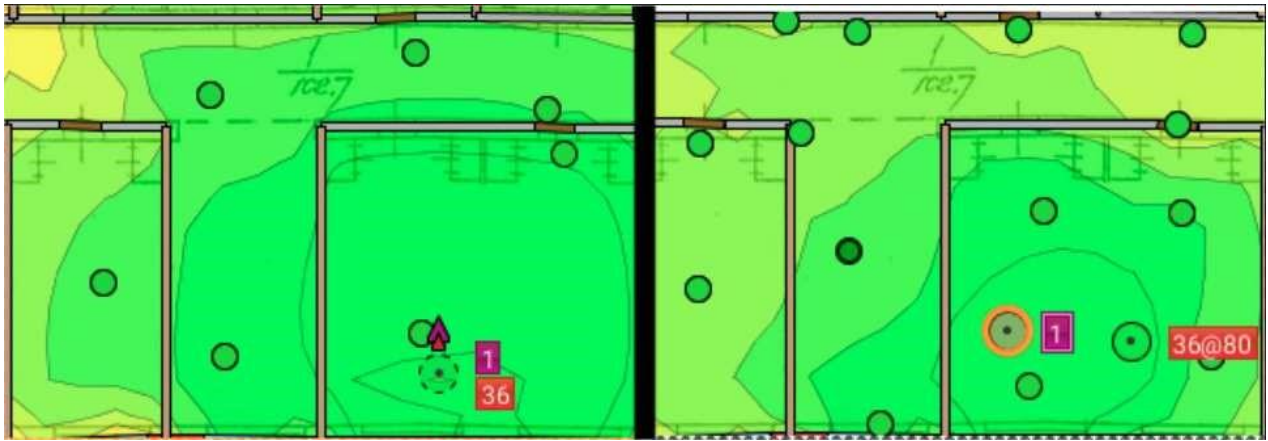
4.4 Радіопланування і установка точок доступу

Для визначення оптимального розташування точок доступу Wi-Fi, першочерговим завданням є проведення радіопланування для кожного поверху. Існує два основних підходи до планування Wi-Fi мереж: емпіричний метод, що полягає у використанні однієї тестової точки доступу для вимірювання рівня сигналу з подальшим її переміщенням та повторними вимірами, та більш сучасний метод, що передбачає створення віртуальної моделі. Останній метод реалізується за допомогою спеціалізованого програмного забезпечення, яке часто містить термін "Site Survey" у своїй назві. Серед найпоширеніших програм для таких завдань виділяються Tamograph Site Survey від Tamosoft та Ekahau Site Survey від Ekahau. Після аналізу функціоналу було обрано Ekahau Site Survey версії 9.0.3.221, як найбільш актуальну на даний момент, що підтримує сучасні технології побудови моделей радіомереж [11]. Для планування трьох поверхів офісу буде достатньо демонстраційної версії програми, яка має незначні обмеження. Вхідні параметри для програми будуть отримані з офіційних специфікацій пристроїв MikroTik RB4011iGS+5HacQ2HnD-IN та Mikrotik cAP ac. Дані будуть занесені до табл. 4.5.

Таблиця 4.5 – Характеристики радіомодулю MikroTik RB4011iGS+5HacQ2HnD-IN та cAP ac

Пристрій	RB4011iGS+5HacQ2HnD-IN	cAP ac
Максимальна потужність передавача	33 dBm	26 dBm
Коефіцієнт підсилення в діапазоні 2,4 ГГц	3 dBi	2 dBi
Коефіцієнт підсилення в діапазоні 5 ГГц	3 dBi	2.5 dBi

Для верифікації надійності та достовірності результатів, що генеруються програмним забезпеченням, потрібно провести тестування його функціональності на ізолюваному тестовому стенді. В рамках цього підходу буде розроблено репрезентативну комп'ютерну модель приміщення, а також застосовано метод "точка доступу на палиці" (рис. 4.3)



а) теоретична модель

б) результат дослідження

Рисунок 4.3 – Графічне відображення зони покриття

Аналіз показав наявність відхилення між теоретичною зоною покриття та фактичними вимірними показниками. Слід зазначити, що при формуванні моделі приміщення не було враховано його наповненість, зокрема, наявність стаціонарних об'єктів, таких як шафи та столи. Ці об'єкти можуть створювати перешкоди для поширення радіосигналу, що призводить до певних неточностей при зіставленні даних. Окрім графічного представлення радіопокриття, EkaHau Site Survey забезпечує можливість прогнозування конкретного рівня сигналу в будь-якій локації приміщення. З огляду на це, буде проведена модернізація моделі та повторне дослідження з внесенням отриманих замірів до табл. 4.6

Таблиця 4.6 – Порівняння замірів рівня сигналу

Номер точки заміру	Рівень сигналу під час експерименту	Рівень сигналу в моделі EkaHau Site Survey
1	-69	-71
2	-47	-49
3	-54	-50
4	-47	-43
5	-53	-57
6	-57	-55
7	-59	-57
8	-58	-59
9	-60	-60
10	-53	-52

Аналіз даних демонструє наявність відмінностей у результатах, проте ці відмінності є несуттєвими. Отже, Ekaau Site Survey може бути успішно використаний для подальшого етапу планування. Всі наступні проектні рішення будуть орієнтовані на стандарт IEEE 802.11ac, що передбачає використання частотного діапазону 5 ГГц.

4.4.1 Радіопланування на першому поверсі

Схема першого поверху представлена на рис. 4.4.

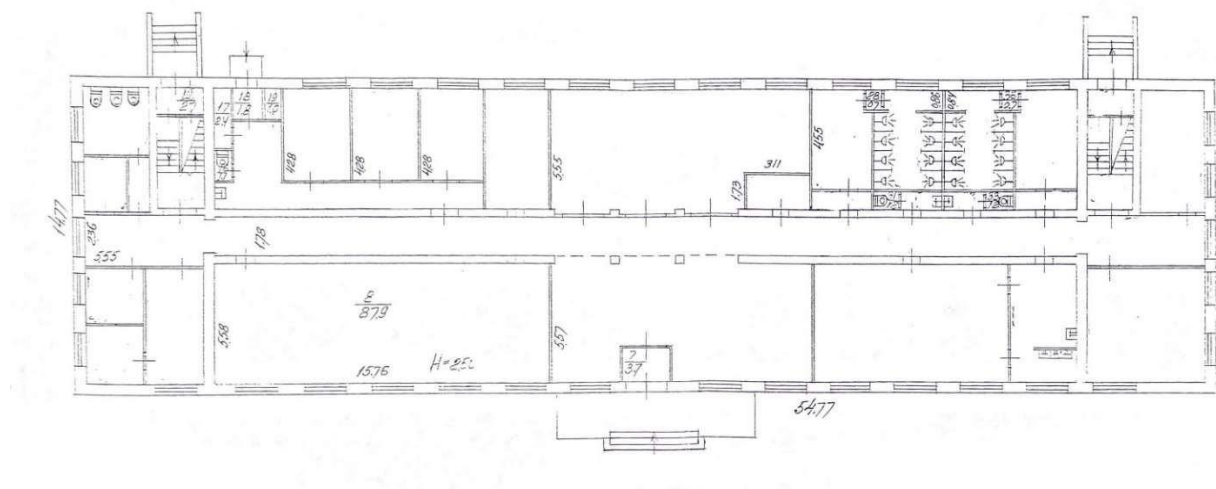


Рисунок 4.4 - План першого поверху офісного центру

На першому поверсі будівлі розміщено два конференц-зали, які є зонами з високою пропускнуою здатністю для користувачів, що потребують підключення до гостьової Wi-Fi мережі. Робочі станції в цих приміщеннях не передбачені. Натомість, кожен зал оснащений комп'ютером, який виконує роль контролера для інтерактивної презентаційної дошки та забезпечує відеовиведення на проектор. З огляду на необхідність підключення цих презентаційних комп'ютерів до основної Wi-Fi мережі, рекомендованим рішенням є застосування точок доступу Mikrotik cAP ac. Ці пристрої мають можливість створення до 16 незалежних SSID (ідентифікаторів мережі) з гнучкими налаштуваннями прав доступу. Крім того, на першому поверсі розташоване кафе, яке також потребує забезпечення Wi-Fi покриття. Для подальшого моделювання мережі буде виконано експорт плану будівлі в

програмне забезпечення EkaHau Site Survey з подальшим нанесенням елементів конструкції, таких як стіни, вікна та перегородки (рис. 4.5).

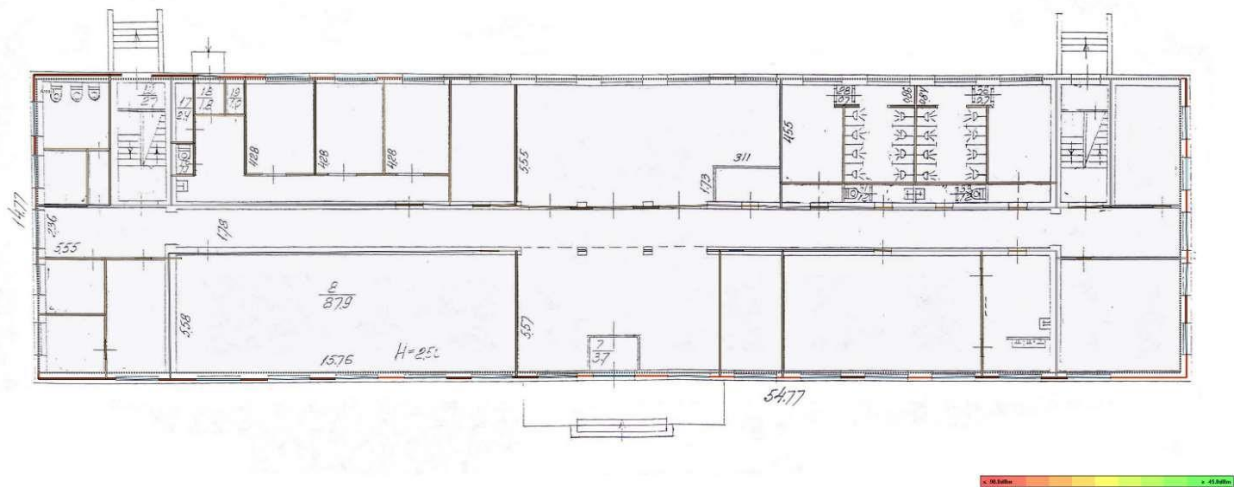


Рисунок 4.5 - Вигляд проекту в EkaHau Site Survey після внесення структурних елементів

Оптимальне розміщення точок доступу Mikrotik sAP ac для створення максимально ефективної зони покриття з мінімальним числом пристроїв було визначено тестуванням. Виявлено, що для повного покриття поверху достатньо трьох точок доступу. Після їх встановлення та виключення із зони покриття технічних приміщень та санвузлів, готова схема розміщення (рис. 4.6).



Рисунок 4.6 - Розміщення точок доступу

Зважаючи на те, що основна маса користувачів буде знаходитись у приміщеннях конференц-залів та кафе, оптимальним рішенням є розміщення точок доступу з внутрішнього боку цих зон. Фінальна схема радіопланування представлена на рис. 4.7. Для забезпечення ефективної роботи та мінімізації інтерференції, кожна точка доступу функціонує на виділеному каналі, частотний діапазон якого не перетинається з іншими.



Рисунок 4.7 - Результат радіопланування першого поверху

Таким чином, вдалося сформувавши раціональний план розташування точок доступу в межах першого поверху установи.

4.4.2 Радіопланування на другому поверсі

План другого поверху офісного центру наведено на рис. 4.8. Оскільки тут розташована більшість офісів, важливо відразу вказати місцезнаходження всіх робочих місць.

Для забезпечення ефективної роботи на другому поверсі, де розміщено 33 робочі станції, планується створення єдиної бездротової мережі. Ця мережа має охопити як стаціонарні робочі місця, так і персональні мобільні пристрої співробітників. Оскільки конференц-зал на поверсі призначений виключно для внутрішніх зустрічей, створення окремої гостьової підмережі не є необхідним. Першим кроком у радіоплануванні буде нанесення на план усіх структурних елементів, таких як стіни, вікна, двері та перегородки (рис. 4.9). Крім того, будуть виділені ділянки, які не потребують Wi-Fi покриття.

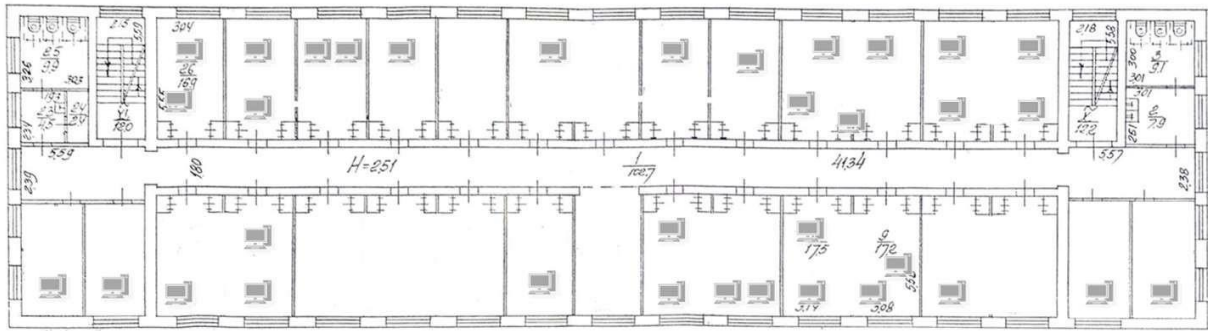


Рисунок 4.8 – План другого поверху з розташуванням дротового підключення робочих станцій

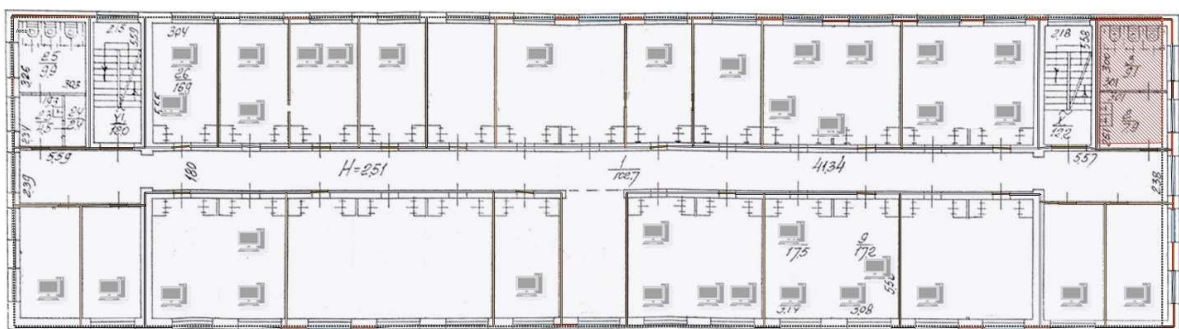


Рисунок 4.9 – Вигляд проекту в EkaHau Site Survey після внесення структурних елементів

Для забезпечення максимальної щільності покриття бездротової мережі, точки доступу будуть встановлені всередині робочих приміщень. Результати моделювання мережі, виконаного за допомогою EkaHau Site Survey, свідчать про необхідність розгортання чотирьох точок доступу на другому поверсі для досягнення оптимального рівня бездротового доступу. Після аналізу різних конфігурацій, було прийнято рішення про розміщення маршрутизаторів згідно зі схемою, представленою на рис. 4.10.

Після видалення графічного представлення надлишкових зон та внесення необхідних коригувань буде представлено фінальний варіант радіопланування другого поверху (рис. 4.11).



Рисунок 4.10 – Розміщення маршрутизаторів на другому поверсі



Рисунок 4.11 – Результат радіопланування другого поверху

Аналіз покриття демонструє, що всі робочі станції розташовані в зоні досяжності сигналу. Мінімальний зафіксований рівень сигналу становить -67 dBm, що класифікується як "прийнятний". Для забезпечення оптимальної продуктивності та уникнення інтерференції, кожна точка доступу функціонує на виділеному каналі, що унеможливорює конфлікти з сусідніми точками на першому та другому поверхах.

4.4.3 Радіопланування на третьому поверсі

План приміщень на третьому поверсі представлено на рис. 4.12.

Поверх містить конференц-зал, який використовується для проведення конференцій та нарад. Це зумовлює необхідність створення окремої гостьової підмережі. Частина поверху не задіяна співробітниками, тому розгортання мережевого покриття в цій зоні є нераціональним. Інша частина поверху

обладнана десятьма робочими станціями та комп'ютером, що забезпечує роботу обладнання конференц-залу. На плані відображено нефункціональні зони, технічні приміщення та основні конструктивні елементи: стіни, вікна та перегородки (рис. 4.13).

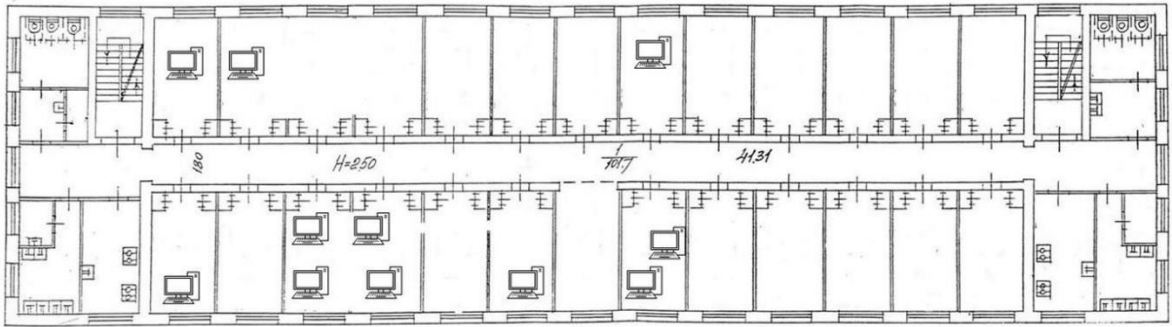


Рисунок 4.12 – План третього поверху з урахуванням робочих станцій

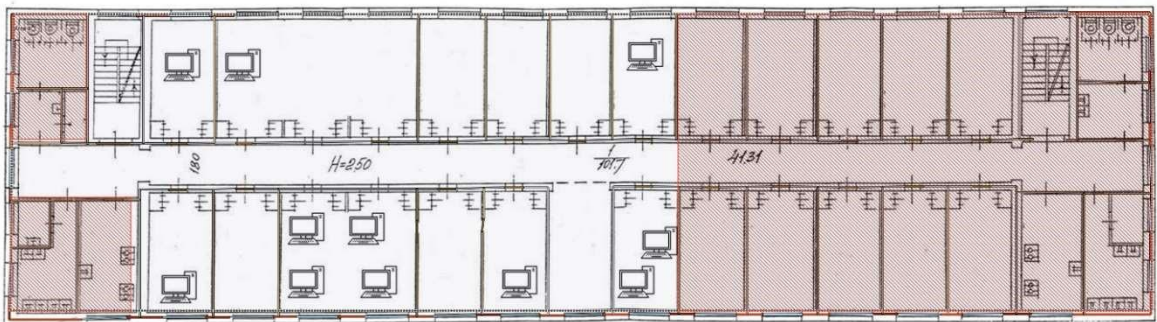


Рисунок 4.13 – Структурна схема третього поверху

Розміщення точок доступу здійснюватиметься з урахуванням специфічної вимоги: для гостьової мережі зарезервовано точку доступу Mikrotik cAP ac, призначену для встановлення у конференц-залі. Після інтеграції всіх заданих параметрів в Ekahau Site Survey візуалізація зони покриття поверху буде представлена на рис. 4.14.



Рисунок 4.14 – Розміщення точок доступу на третьому поверсі

Для забезпечення достатнього покриття Wi-Fi мережі, як правило, достатньо двох точок доступу. Однак у зв'язку з наявністю конференц-залу виникає необхідність збільшення їх кількості до трьох на даному поверсі. Це рішення, незважаючи на супутнє збільшення витрат на обладнання, є обґрунтованим. Виключивши з початкової схеми зони з обмеженнями, ми отримуємо фінальну схему радіопланування третього поверху (рис. 4.15).

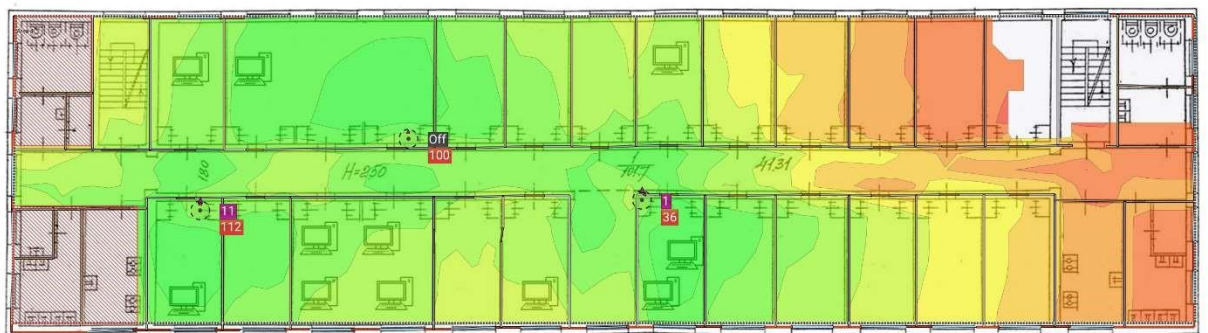


Рисунок 4.15 – Схема радіопланування третього поверху

На окремих ділянках поверху спостерігається недостатнє покриття мережі. Рівень сигналу в цих зонах сягає приблизно -90 dBm, що забезпечує стабільне з'єднання при переміщенні через невикористовувану зону третього поверху.

4.4.4 Тривимірне відображення планованої мережі

Зважаючи на тривимірну природу поширення радіосигналів, важливо усвідомлювати, що окремі поверхи будівлі не функціонують як ізольовані системи. Програмне забезпечення Ekahau Site Survey надає можливість

створення детальної віртуальної моделі споруди, яка враховує всі потенційні фактори. Це дозволяє точно оцінити взаємний вплив точок доступу, розташованих на різних рівнях. Для побудови такої моделі необхідно об'єднати дані про три поверхи та визначити характеристики міжповерхових перекриттів, такі як товщина та щільність (рис. 4.16) [11].

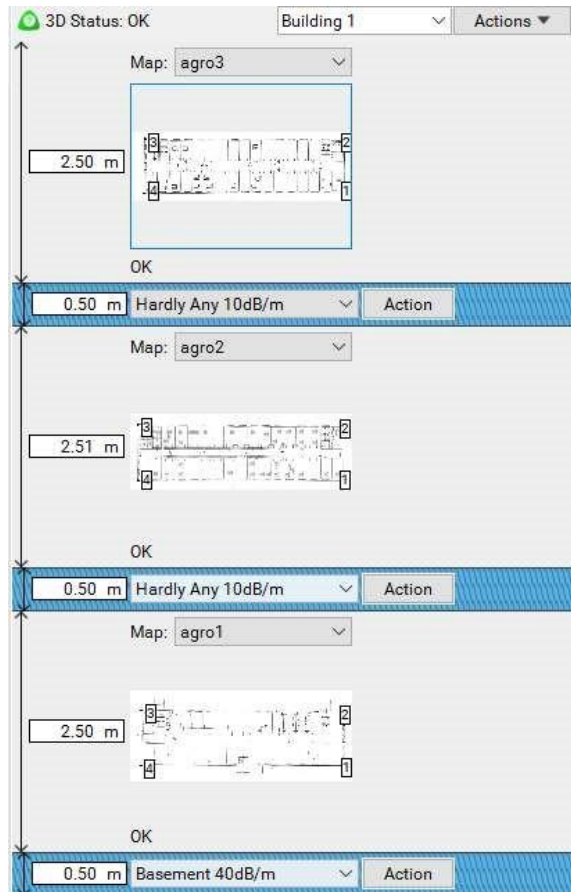


Рисунок 4.16 – Схематичне відображення будівлі установи

Програмне забезпечення автоматично розрахує зони покриття Wi-Fi, враховуючи задані параметри, та візуалізує кінцевий проект, як це проілюстровано на рис. 4.17.

Радіопланування будівлі завершено. Тепер можна переходити до налаштування обладнання.

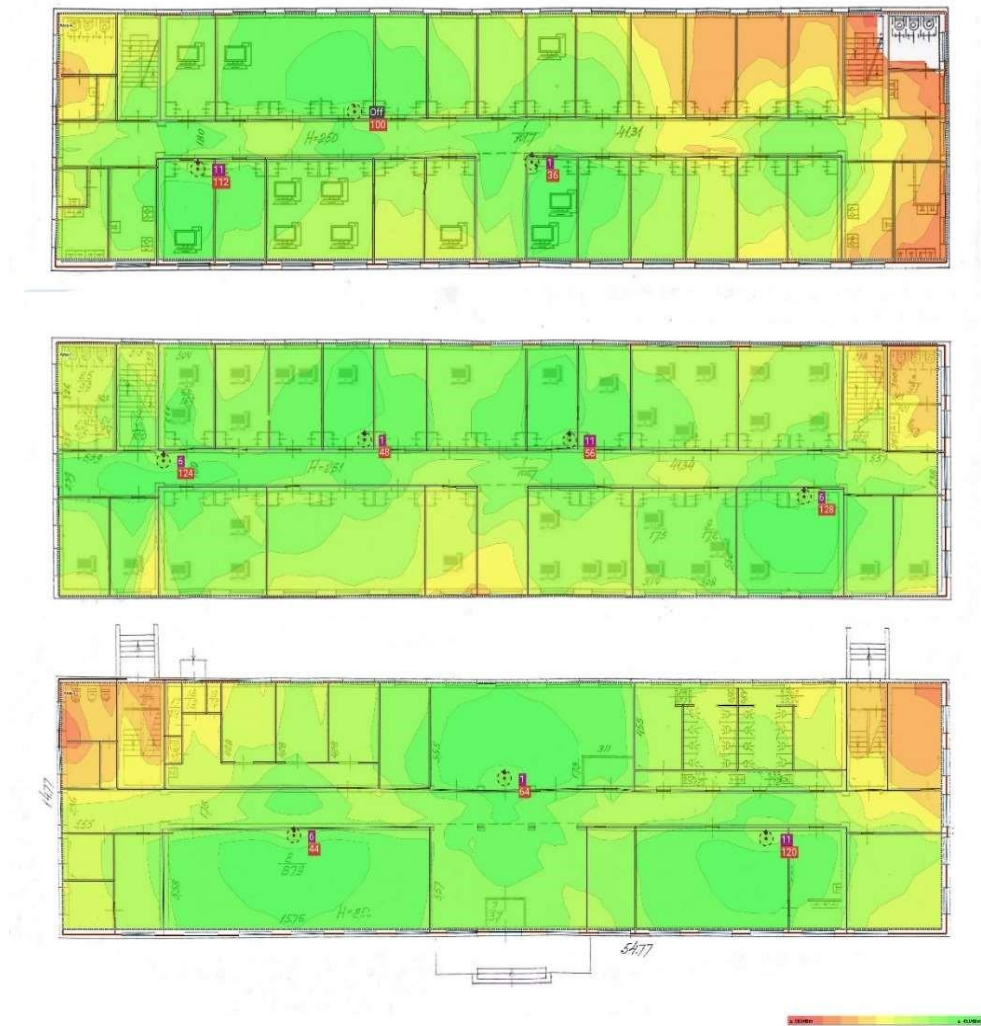


Рисунок 4.17 – Кінцева схема радіопланування трьох поверхів офісного центру

4.5 Налаштування «безшовної» мережі Wi-Fi

Обладнання MikroTik виділяється на тлі конкурентів завдяки інтегрованому менеджеру управління Wi-Fi мережами Capsman. Цей компонент функціонує як централізований контролер, що зберігає конфігурацію для всіх підключених точок доступу. Водночас, сам маршрутизатор відповідає за ефективну обробку мережевих пакетів. Для початку роботи з пристроями, необхідно встановити програмне забезпечення Winbox, яке слугує для адміністрування як точок доступу, так і маршрутизатора. Початкові налаштування будуть здійснені за допомогою цього інструменту. Візуальне ознайомлення з інтерфейсом програми доступне на рис. 4.18 [14].

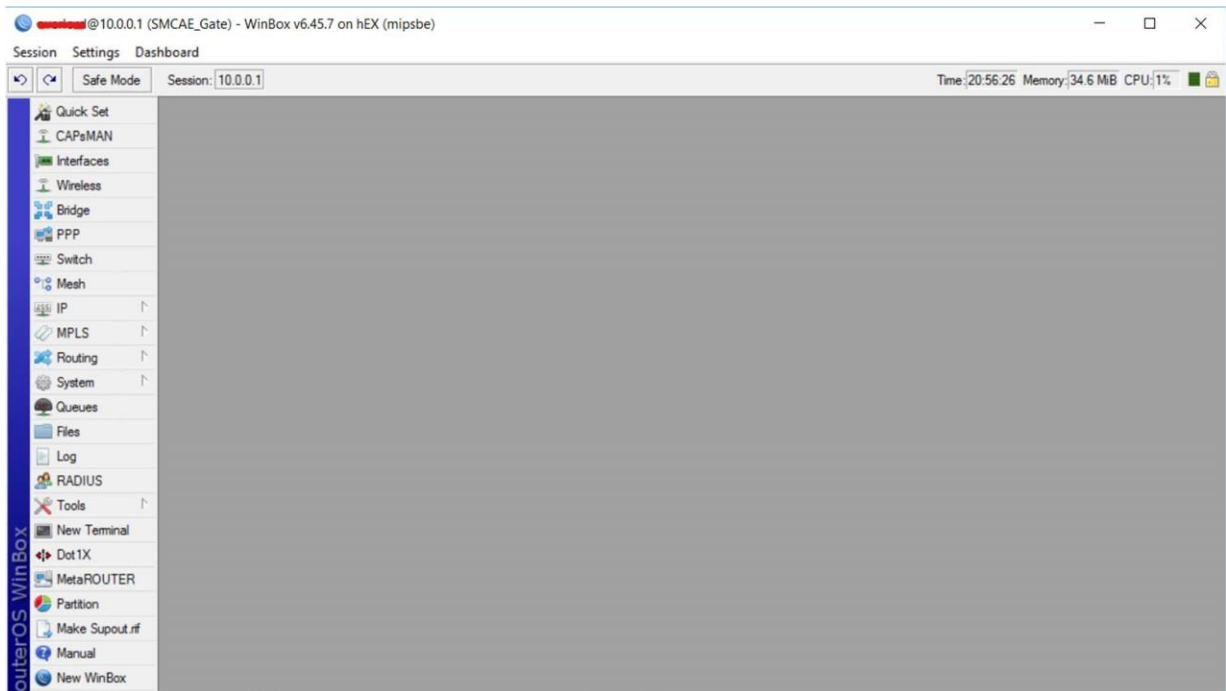


Рисунок 4.18 – Інтерфейс MikroTik Winbox

Додамо до нашої мережі частотні канали. Налаштування знаходяться у меню CAPsMAN->Channels. Для цього вводимо наступні команди:

```
/caps-man channel add band=2ghz-b/g/n name=channel-24
/caps-man channel add band=5ghz-a/n/ac name=channel5
/caps-man datapath add bridge=bridge-1 client-to-client-forwarding=yes
name=\datapath
```

Local Forwarding – трафік, що надходить від клієнта, буде оброблятися або контролером Capsman (якщо відповідний чекбокс не активований), або безпосередньо самою точкою доступу (за умови увімкнення цього чекбокса). Ця опція допомагає знизити навантаження на центральний маршрутизатор, проте необхідно враховувати продуктивність Wi-Fi точки доступу та її здатність обробляти великі обсяги трафіку, а також розташування мережного екрану (Firewall) [14].

Client To Client Forwarding – встановлює дозвіл на обмін трафіком між клієнтами мережі. Наприклад, у гостьовій мережі бажано заборонити цей обмін, в той час як у локальній мережі його варто дозволити [14].

Тепер перейдемо до розділу CAPsMAN->Security Cfg для налаштування параметрів безпеки. Для цього використаємо команду:

```
/caps-man security add authentication-types=wpa2-psk encryption=aes-ccm
\group-key-update=1h name=security passphrase=123456678
```

У вкладці CAPsMAN->Configurations знаходяться параметри загальної конфігурації. Виконаємо наступні команди:

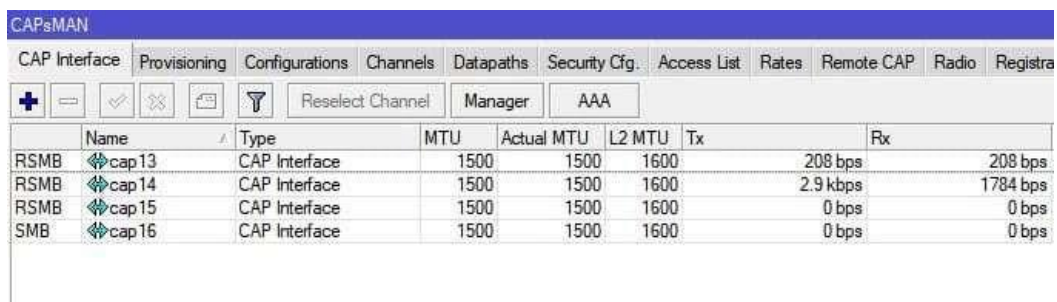
```
/caps-man configuration add channel=channel-24 datapath=datapath mode=ap
name=\cfg-24 rx-chains=0,1,2,3 security=security \ssid=MikrotikConfigUkr
txchains=0,1,2,3
```

```
/caps-man provisioning add action=create-enabled hw-supported-modes=an,ac
\master-configuration=cfg-5
```

Після завершення всіх конфігураційних процедур, необхідно перейти до налаштування безпосередньо точки доступу. Інтерфейс пристрою Mikrotik cAP має схожість з інтерфейсом моделі Mikrotik RB4011iGS+5HacQ2HnD-IN, оскільки обидва базуються на операційній системі RouterOS. Для підключення до точки доступу скористаємося утилітою Winbox у розділі Wireless -> WiFi Interfaces. Далі виконаємо наступні команди:

```
/interface wireless cap set bridge=bridge caps-man-addresses=127.0.0.1
enabled=yes interfaces=\wlan1,wlan2
```

Під час виконання дії "Provisioning Action" з параметром "create dynamic enabled" відбувається автоматичне створення віртуальних інтерфейсів на всіх конфігурованих точках доступу. Результат цього процесу представлено на рис. 4.19.



Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx
cap13	CAP Interface	1500	1500	1600	208 bps	208 bps
cap14	CAP Interface	1500	1500	1600	2.9 kbps	1784 bps
cap15	CAP Interface	1500	1500	1600	0 bps	0 bps
cap16	CAP Interface	1500	1500	1600	0 bps	0 bps

Рисунок 4.19 – Список налаштованих точок доступу у Winbox

Відтепер у нашій установі функціонує повноцінна система безшовного роумінгу. Це означає, що користувачі можуть вільно переміщуватися по території, не відчуваючи перебоїв у зв'язку, спричинених необхідністю перепідключення пристроїв.

4.6 Налаштування Wi-Fi адаптерів користувачів

Більшість сучасних мобільних пристроїв для користувачів вже мають вбудовану підтримку стандарту бездротового зв'язку IEEE 802.11ac. Якщо ж ви використовуєте старіше обладнання, воно все ще може підключатися до мережеских точок доступу, використовуючи стандарти 802.11a/b/g/n. Для комп'ютерів, які не мають вбудованого Wi-Fi, але потребують бездротового підключення, доступні USB Wi-Fi адаптери. У даному випадку, ми встановили адаптер TP-Link Archer T4U на комп'ютер під керуванням Windows 10. Після успішного встановлення драйверів, пристрій можна підключати до бездротової мережі (рис. 4.20) [4].

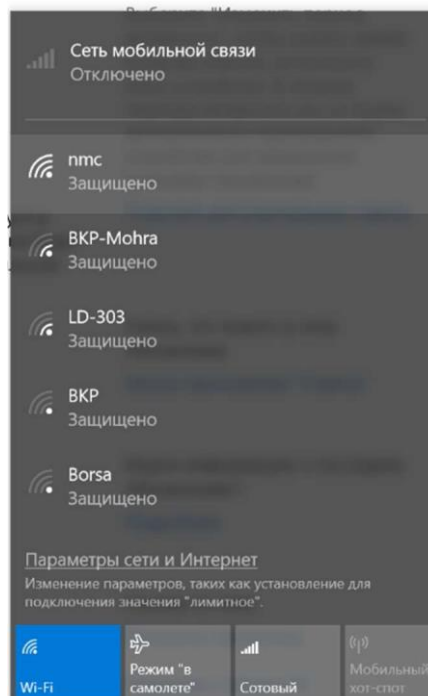


Рисунок 4.20 – Налаштування бездротових підключень в операційній системі Windows 10

Базове тестування підтвердило повну сумісність адаптера з ОС Windows 10, що встановлена на всіх комп'ютерах установи.

Недостатня пропускна здатність точок доступу може спричинити їх некоректну роботу. Тому критично важливо оцінити рівень трафіку в місцях з найбільшою концентрацією користувачів, зокрема в конференц-залах. Саме там одночасне використання мережі великою кількістю людей може призвести до збоїв. Оскільки кількість одночасних підключень до точки доступу безпосередньо пов'язана з обсягом даних, які передають користувачі (тобто з їхніми завданнями), доцільно встановити обмеження швидкості для гостьової підмережі на рівні 5-10 Мбіт/с. Це дозволить мінімізувати потенційні проблеми та розвантажити точки доступу.

4.7 Налаштування захисту бездротової мережі

Безпека залишається однією з найгостріших проблем для бездротових мереж. Зловмисники можуть легко підключитися до корпоративної мережі, використовуючи власний ноутбук, при цьому залишаючись непоміченими. Виявити факт прослуховування такої мережі надзвичайно складно, і традиційні засоби захисту, як-от файрволи, тут безсилі.

Саме тому шифрування даних у Wi-Fi мережах стало необхідністю. Раніше використовуваний протокол WEP з 128-бітним ключем вже не забезпечує достатнього рівня захисту. Тому варто звернути увагу на протоколи WPA та його покращену версію – WPA2 [5].

Протоколи шифрування та перевірки цілісності:

- TKIP (Temporal Key Integrity Protocol) використовує динамічні ключі шифрування довжиною 128 біт. Ці ключі генеруються за складним алгоритмом і часто змінюються, що робить їх стійкими до зламу. Однак, сьогодні існує більш ефективна альтернатива – AES (Advanced Encryption Standard).

- MIC (Message Integrity Check) відповідає за перевірку цілісності даних. Цей протокол допомагає відсіювати пакети, які були незаконно вставлені в мережевий трафік сторонніми особами [5].

Важливо розуміти, що жодна зі схем захисту бездротових мереж не є абсолютно досконалою. Сучасні зловмисники постійно шукають нові вразливості, іноді успішно їх експлуатуючи.

Зважаючи на всі ці фактори, для забезпечення надійного захисту даних у бездротових мережах було обрано комбінацію протоколу WPA2-PSK з алгоритмом шифрування AES. Ця конфігурація вважається найбільш ефективним методом шифрування на сьогоднішній день.

4.8 Визначення результатів оптимізації

Проектування корпоративної бездротової мережі для офісного центру базувалося на ретельному дотриманні принципів побудови та оптимізації.

В результаті оптимізації, бездротова мережа доступу WLAN отримала низку суттєвих переваг:

- значно зросла швидкість передачі даних;
- зведено до мінімуму кількість "мертвих" зон, забезпечуючи стабільне покриття;
- завдяки впровадженню безшовного Wi-Fi, перепідключення до мережі відбувається практично миттєво;
- підвищено рівень безпеки та розширено функціональність шляхом створення окремої гостьової підмережі;
- досягнуто повного використання потенціалу бездротової передачі даних.

Крім того, оптимізація дозволила усунути раніше виявлені недоліки, а саме:

- низький рівень захищеності даних;
- значний вплив зовнішнього середовища на поширення радіохвиль;
- проблеми взаємного впливу точок доступу.

Щоб переконатися в стабільній роботі бездротової мережі після її оптимізації, необхідно провести тестування. Це допоможе виявити будь-які приховані недоліки, що можуть вплинути на передачу даних між клієнтами. Як тестовий пристрій було обрано планшет з операційною системою Windows 10 та мережевим адаптером 802.11ac Wireless PCIe. Для створення реалістичного навантаження на точку доступу було задіяно ще 10 бездротових пристроїв. Процес тестування реалізовано за допомогою програмного забезпечення LAN Speed Test (рис. 4.21).

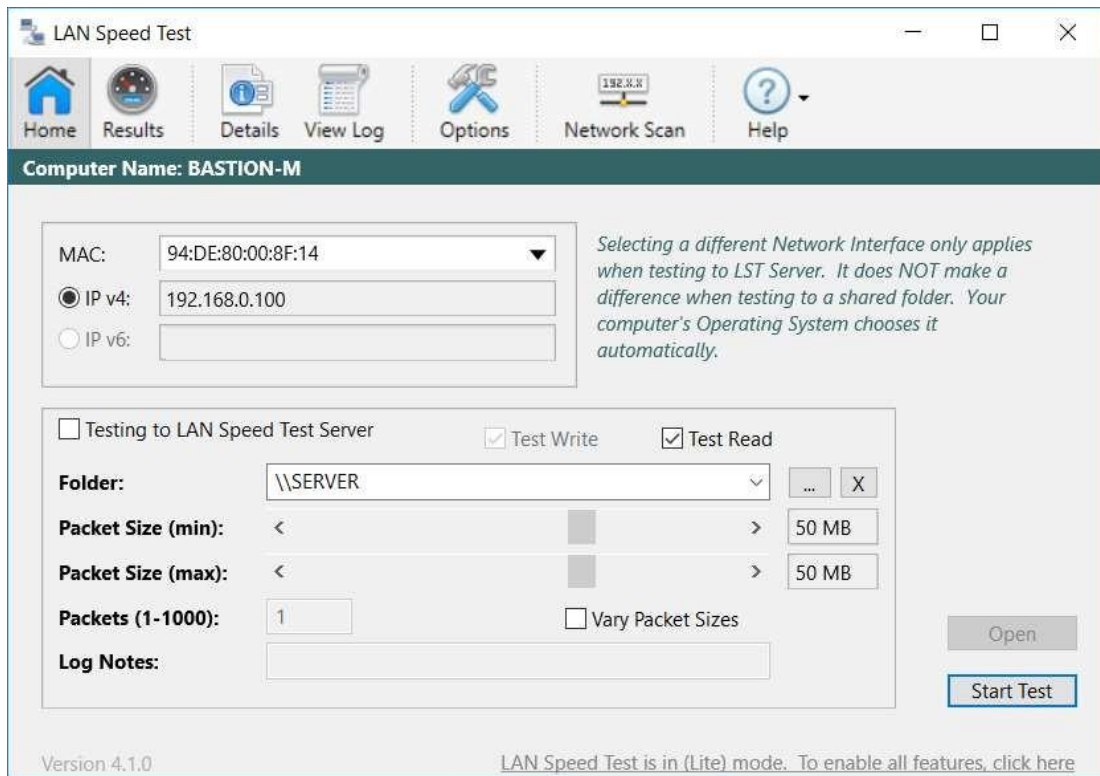


Рисунок 4.21 – Головне вікно LAN Speed Test

Для оцінки ефективності локальної мережі використовується програма LAN Speed Test. Цей синтетичний тест імітує реальний мережевий трафік, надаючи можливість детально вивчити різноманітні аспекти продуктивності. З його допомогою можна визначити максимальну швидкість передачі та прийому даних мережним адаптером, а також оцінити швидкість обробки пакетів, кількість операцій введення-виводу та ступінь завантаження центрального процесора. Оскільки пріоритетом для цієї мережі є взаємодія між локальними пристроями, тестування здійснюватиметься пінгуванням високопродуктивного файлового сервера. Оптимальний розмір пакета для всіх тестів встановлено в 50 Мб [8]. Візуальне подання схеми тестування наведено рис. 4.22.

Для аналізу впливу числа підключених пристроїв на обсяг мережного трафіку, що проходить через точку доступу, було застосовано таку методику: кількість активних пристроїв поетапно збільшувалася від одного до десяти. Кожен доданий пристрій переводився в режим активної передачі даних шляхом надсилання ping-запитів на сервер, що імітувало максимальне навантаження. Дослідження проводилися в умовах, близьких до ідеальних, з відстанню до точки доступу не більше 5 метрів. Зібрані під час тестування дані відображені у табл. 4.7.

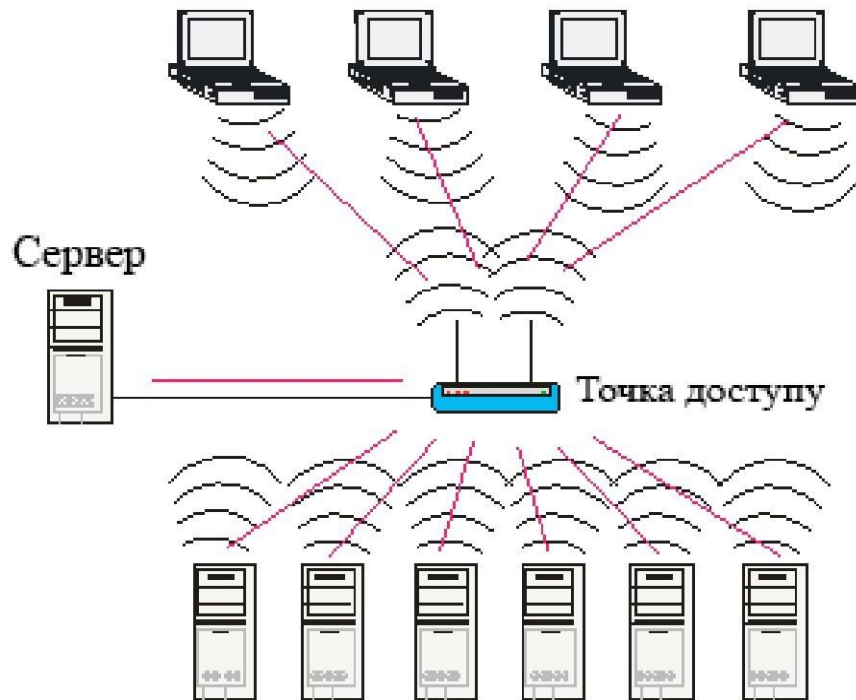


Рисунок 4.22 – Схема тестування бездротової мережі

Таблиця 4.7 – Результати тестування мережі у режимі «всі клієнти активні»

Кількість клієнтських пристроїв у мережі	1	2	3	4	5	6	7	8	9	10
Середня швидкість прийому, Мбіт/с	321,7	120,5	80,9	60,1	55,8	41,5	32,2	21,5	20,8	20,2
Середня швидкість віддачі, Мбіт/с	298,1	210	120,6	80,2	56,1	45,4	38,5	31	28,2	15,3

Проведемо аналіз взаємозв'язку між швидкістю передачі даних та числом одночасних активних користувачів у мережі, візуалізувавши його у вигляді графіків (рис. 4.23).

Згідно з графіком, спостерігається значне падіння швидкості мережі зі збільшенням кількості одночасно підключених пристроїв. Тим не менш, навіть при десяти активних пристроях, швидкість тримається на стабільному рівні 20 Мбіт/с.

Для більш точного розуміння роботи мережі в типових умовах, ми проведемо тестування, імітуючи сценарій з одним домінуючим клієнтом, який використовує всю доступну пропускну здатність. Решта абонентів будуть

генерувати фоновий трафік, включаючи обмін повідомленнями, перевірку пошти та завантаження веб-сторінок. Кількість таких фонових абонентів буде поступово збільшуватися від одного до дев'яти. Дані тестування наведені в табл. 4.8.

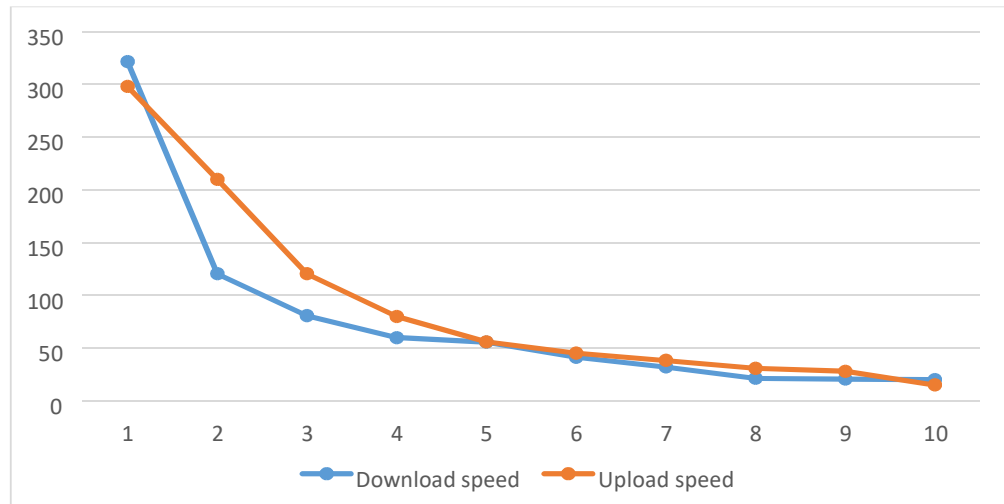


Рисунок 4.23 – Графік залежності швидкості передачі даних від кількості активних клієнтів у мережі

Таблиця 4.8 – Результати тестування мережі у режимі «спокійна активність»

Кількість фонових пристроїв у мережі	0	1	2	3	4	5	6	7	8	9
Середня швидкість прийому на активному клієнті, Мбіт/с	325,1	313,5	305,1	302,2	301,8	300,3	292,4	295,2	284,9	281,1
Середня швидкість віддачі на активному клієнті, Мбіт/с	308,2	299,6	295,3	282,8	286,1	271,2	266,7	258,8	269,5	254,2

Побудуємо графік залежності швидкості передачі від числа фонових користувачів у мережі (рис. 4.24).

Згідно з графіком, швидкість передачі даних у мережі демонструє високу стабільність, залишаючись у діапазоні 250-300 Мбіт/с навіть при значному навантаженні. Цей показник є цілком достатнім для задоволення всіх операційних потреб офісної установи.

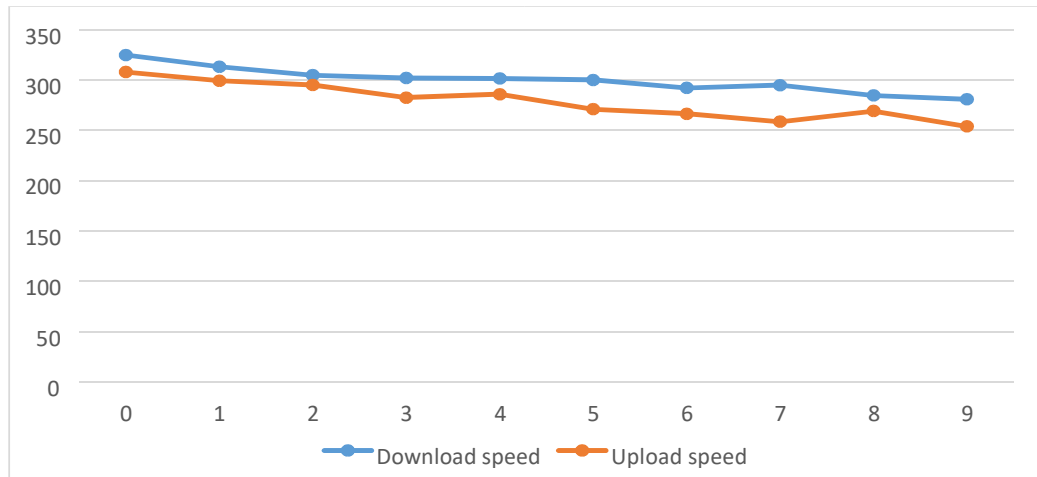


Рисунок 4.24 – Графік залежності швидкості передачі даних від кількості фонових клієнтів у мережі

У рамках польових випробувань було проведено тестування точки доступу в умовах інтенсивного використання, зокрема, під час конференції, де одночасно перебувало близько 80 осіб. Середня кількість підключених пристроїв склала 20. Зафіксовано, що приблизно 40% користувачів автоматично обрали 5 ГГц мережу, з яких половина використовувала стандарт 802.11ac.

ВИСНОВКИ

У рамках кваліфікаційної роботи було здійснено повний цикл робіт: проектування, побудову та оптимізацію високошвидкісної бездротової мережі доступу для офісного центру, застосувавши авторський алгоритм оптимізації. Вибір теми був продиктований перевагами бездротових технологій та нагальною потребою в оптимізації існуючої бездротової інфраструктури установи.

Детальний аналіз сучасних мережевих стандартів (зокрема, стандартів бездротового зв'язку та безпеки) дозволив обрати найбільш ефективне рішення для проектування мережі доступу.

Для забезпечення якісного покриття було проведено радіопланування трьох поверхів будівлі, що дозволило визначити оптимальний тип та кількість мережевого обладнання. Результати дослідження показали, що для побудови повноцінної Wi-Fi мережі за стандартом 802.11ac достатньо десяти точок доступу, розташованих з урахуванням особливостей приміщень. Мережа побудована на базі сучасного обладнання, яке відповідає всім технічним вимогам для надання високоякісних послуг зв'язку на частотах 2.4 ГГц та 5 ГГц, а також відрізняється високою надійністю. Проведений аналіз отриманої бездротової мережі виявив її сильні та слабкі сторони.

Тестування Wi-Fi мережі підтвердило її повну працездатність та відповідність поставленим вимогам. Створена в процесі виконання дипломного проекту модель побудови бездротової мережі, завдяки своїй гнучкості та адаптивності, може бути успішно реалізована і ефективно застосована на практиці в інших подібних установах після незначної адаптації до специфічних умов.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Характеристики та принцип роботи Wi-Fi. URL: <https://www.briz.ua/help/princip-raboty-wi-fi> (Дата звернення 09.11.2025).
2. Wi-Fi - розвиток і основні принципи найпоширенішого стандарту бездротових мереж. URL: <https://ua.gecid.com/netlan/wi-fi - razvitie i osnovnyee prinjipy samogo rasprostranennogo standartarta besprovodn yeh seteyi/> (Дата звернення 19.11.2025)
3. Стандарти бездротового доступу до мережі Wi-Fi. URL: <https://triolan.net/wiki/knowledgebase.php?article=35> (Дата звернення 29.11.2025).
4. Засоби моделювання Wi-Fi мережі. URL: <https://uk.clccomputers.com/8-best-wifi-analyzer> (Дата звернення 12.11.2025).
5. Tanenbaum A., D. Wetherall Комп'ютерні мережі. – Новий Джерсі, Пірсон, 2012. 959 с.
6. Стрельников, А. Ю., С. А. Страмоусова. Технологія бездротової передачі даних Wi-Fi. Молодий вчений. - 2016.- №9-4 (113). - С. 67-69.
7. Чистяков, Б. Є. Миктибаєв, А. Б. Жанбеков. Аналіз технологій бездротової передачі даних. Журнал наукових і прикладних досліджень. - 2016. - №1. - С. 166-169.
8. Verenkoff B. Understanding and Optimizing 802.11n. Brian Verenkoff // Buffalo Technology – URL: https://www.lmi.net/wp-content/uploads/Optimizing_802.11n.pdf (Дата звернення 16.11.2025).
9. А.А. Максимова, В.М. Кострова, А.А. Андросов. Оптимізація бездротових мереж зв'язку на основі методів штучного інтелекту. Моделювання, оптимізація та інформаційні технології. 2016. №2. С.185-190.
10. Channel Selection in Uncoordinated IEEE 802.11 Networks Using Graph Coloring [Електронний ресурс] / [J. M. Gimenez-Guzman, M. Ivan, H. Enrique та ін.] // MDPI. – 2023. – Режим доступу до ресурсу: <https://www.mdpi.com/1424-8220/23/13/5932>.
11. Diaz J. WiFi Best Practice – WiFi Channels allocation and configuration. [Електронний ресурс] / Jorge Diaz // JD Tech Solution. – 2022. – Режим доступу до ресурсу: <http://jdtechsolutions.net/wifi-best-practice-wifi-channels-allocation-and-configuration/>.

12. Geier E. How to configure Wi-Fi channels for top network performance [Электронный ресурс] / Eric Geier // Computerworld. – 2015. – Режим доступа до ресурсу: <https://www.wifisurveyors.com/configure-wi-fi-channels-network-pe>.

13. Deep reinforcement learning based interference optimization for coordinated beamforming in ultra-dense Wi-Fi networks / Jamshid Bacha та ін. Computer Communications. 2025. С. 1–5.