ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Безпровідні мережі високої пропускної здатності»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 – Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Дмитро БЛАГОВІСНИЙ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-42
Дмитро БЛАГОВІСНИЙ
Ім'я, ПРІЗВИЩЕ

Керівник: Олександр ЗУБ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент:
інженерії
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 – Комп'ютерна інженерія

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Благовісний Дмитро Вікторович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Безпровідні мережі високої пропускної здатності
_____
керівник кваліфікаційної роботи Олександр ЗУБ,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025р. № 56
2. Строк подання кваліфікаційної роботи «5» червня 2024р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література; науково-технічна література;
протоколи стандартів IEEE 802.11ac, 802.11ax, 802.11be; хмарні технології: IaaS, SaaS, PaaS;
топологія мережі, логічна топологія (Layer 3), фізична топологія (Layer 2);
одноранговa мережа (P2P), клієнт-серверна мережа; IPv4/IPv6; технологія PoE; модулі SFP;
мережеві протоколи: TCP, UDP, DHCP.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
    1. Поняття безпровідної мережі високої пропускної здатності. Стандарти IEEE 802.11 та сучасні тренди
    2. Інфраструктура безпровідної мережі. Топологія, обладнання, технології доступу
    3. Розгортання, підтримка та безпека безпровідної мережі. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «24» лютого 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	26.04-25.03.2025	Виконано
2	Обробка матеріалу	24.04-06.04.2025	Виконано
3	Розробка теоретичної частини	08.04-12.04.2025	Виконано
4	Розробка моделі мережі	13.04-22.04.2025	Виконано
5	Висновки за результатами аналізу	22.04-07.05.2025	Виконано
6	Оформлення пояснювальної записки	09.05-10.05.2025	Виконано
7	Розробка презентації	12.05-18.05.2025	Виконано
8	Передзахист	27.05-29.05.2025	Виконано
9	Здача в деканат	02.05-05.06.2025	Виконано

Здобувач вищої освіти _____ Дмитро БЛАГОВІСНИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Олександр ЗУБ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 46 стор., 10 рис., 5 табл., 29 джерел.

Мета роботи – Дослідження безпровідних мереж високої пропускної здатності та аналіз сучасних технологій їх реалізації.

Об'єкт дослідження – Безпровідні мережі, орієнтовані на високу пропускну здатність у різних середовищах.

Предмет дослідження – Технології побудови, оптимізації та впровадження безпровідних мереж з акцентом на продуктивність.

Короткий зміст роботи: У роботі розглядаються сучасні підходи до створення бездротових мереж з високою пропускною здатністю, зокрема стандарти Wi-Fi 6/6E/7, технологія 5G та рішення SD-WAN. Проаналізовано технічні особливості кожної технології, включаючи OFDMA, MU-MIMO, Beamforming, BSS Coloring та інші механізми, які впливають на ефективність передачі даних. Значну увагу приділено питанням енергоефективності, адаптивного покриття, безпеки, підтримки роумінгу та надійності з'єднання.

Окремий розділ присвячений практичним аспектам проєктування мережі, таким як планування точок доступу, боротьба з інтерференцією, застосування IoT та приклади з реальних кейсів. У завершенні представлено узагальнені рекомендації щодо впровадження таких мереж у різних організаціях та середовищах, де критичними є стабільність та масштабованість з'єднання.

КЛЮЧОВІ СЛОВА: БЕЗПРОВІДНІ МЕРЕЖІ, ПРОПУСКНА ЗДАТНІСТЬ, Wi-Fi 6, 5G, SD-WAN, MU-MIMO, OFDMA, QoS, РОУМІНГ, IoT, ІНТЕРФЕРЕНЦІЯ, ПЛАНУВАННЯ МЕРЕЖІ, БЕЗПЕКА ДАНИХ, ЕНЕРГОЕФЕКТИВНІСТЬ.

ЗМІСТ

ВСТУП……...… 8
1 БЕЗПРОВІДНІ МЕРЕЖІ ТА ЇХ ТЕХНОЛОГІЇ……. 9
1.1 Класифікація безпровідних мереж ……..... 10
1.1.1 Класифікація та основні типи безпровідних мереж……..… 11
1.1.2 Класифікація за технологіями…… 12
1.1.3 Топологічна класифікація……... 13
1.1.4 Узагальнена таблиця класифікації……. 15
1.1.5 Класифікація за частотним діапазоном…….. 15
1.1.6 Переваги і недоліки окремих типів безпровідних мереж……. 17
1.2 Основні стандарти Wi-Fi, LTE, 5G …… 18
1.3 Технології підвищення пропускної здатності мереж ……..…… 22
1.4 Інтернет речей (IoT) у бездротових мережах…… 23
1.5 Вікімережі та Mesh-технології…… 25
2 ІНФРАСТРУКТУРА БЕЗДРОТОВОГО ЗВ'ЯЗКУ …… 27
2.1 Рівні моделі OSI в бездротовій інфраструктурі ……... 28
2.2 Компоненти мережевої інфраструктури бездротового доступу …… 31
2.3 Топологія та розміщення точок доступу і антен ……..… 34
2.4 Фактори, що впливають на якість бездротового зв'язку …… 36
2.5 Безпека та захист у бездротовій інфраструктурі…..……. 38
2.6 Енергозберігаючі рішення та екологічна відповідальність у сучасних бездротових мережах…… 39
3 ПРОЄКТУВАННЯ ТА АНАЛІЗ БЕЗДРОТОВОЇ МЕРЕЖІ …… 41
3.1 Вибір стандарту та мережевих технологій ……..... 42
3.2 Моделювання навантаження та пропускної здатності …… 44
3.3 Забезпечення безпеки та управління трафіком …… 46
3.4 Перевірка ефективності проєкту на практиці …….. 48
3.5 Інтеграція з існуючою інфраструктурою……... 50
ВИСНОВКИ…….. 53
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ…….. 55
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)……. 60

ВСТУП

У XXI столітті цифрові технології стрімко трансформують усі сфери діяльності людини — від особистого спілкування до складних індустріальних процесів. Одним із ключових напрямів цього розвитку є широке впровадження бездротових комунікаційних систем, які забезпечують передачу інформації без фізичного з'єднання між пристроями. Це створює нові можливості для мобільності, гнучкості та інтеграції уніфікованих інформаційних середовищ.

Інтенсивне зростання кількості пристроїв, підключених до мережі, розвиток Інтернету речей (IoT), «розумного» середовища (smart city, smart home) та підвищені вимоги до якості обслуговування (QoS) стимулюють потребу в мережах, здатних передавати великі обсяги даних із мінімальними затримками. У відповідь на це з’являються й активно впроваджуються технології нового покоління: Wi-Fi 6/6E, 5G NR, mmWave, Li-Fi, а також гібридні системи, які об’єднують різні канали зв’язку в єдину високошвидкісну інфраструктуру.

Актуальність теми зумовлена необхідністю глибокого аналізу сучасного стану бездротових технологій високої пропускної здатності, визначення їх ефективності в різних середовищах, виявлення переваг та обмежень, а також пошуку оптимальних рішень для перспективних застосувань. Оскільки бездротові мережі вже стали критично важливою складовою інформаційної інфраструктури, особливо у сфері освіти, медицини, оборони, логістики та розваг, їх розвиток та вдосконалення є важливим науково-практичним завданням.

Метою дослідження є систематизація знань про сучасні безпровідні технології передачі даних із високою пропускною здатністю, вивчення їх технічних параметрів, принципів функціонування, архітектурних особливостей, а також напрямів подальшої еволюції.

1 БЕЗПРОВІДНІ МЕРЕЖІ ТА ЇХ ТЕХНОЛОГІЇ

У сучасних умовах розвитку інформаційних технологій та невпинно зростаючої мобільності користувачів безпровідні мережі вийшли на перший план як надзвичайно гнучке й універсальне рішення для організації зв’язку. Замість обмежень, пов’язаних із фіксованою кабельною інфраструктурою, вони відкривають нові можливості для швидкого розгортання, оперативного перенесення робочих місць і адаптації до постійних змін внутрішнього простору офісів, навчальних закладів чи виробничих цехів.

Важливо зазначити, що безпровідні технології не просто «відрізняються від дротових» відсутністю кабелю — вони пропонують цілком інший підхід до побудови інформаційного середовища. Кожна з основних ліній розвитку — від традиційного Wi-Fi і Bluetooth до спеціалізованих рішень ZigBee чи LoRaWAN — виникла як відповідь на певні прикладні запити: швидке передавання об’ємних даних, енергоощадність у розподілених сенсорних мережах, безперервний зв’язок в умовах великого числа одночасно підключених пристроїв. А мережі четвертого та п’ятого покоління (4G/5G) поступово стають не просто засобом доступу до Інтернету, а надійним каналом для дистанційних консультацій, віддаленого керування промисловими роботами і навіть організації мобільних “гарячих точок” у полі під час проведення великих заходів.

Неможливо обминути увагою й питання продуктивності: ключові метрики — пропускна здатність, час затримки, співвідношення сигнал/шум, стійкість до перешкод і обмеження за енергоспоживанням — тісно взаємопов’язані й вимагають ретельного балансування. Так, новий стандарт Wi-Fi 6 (IEEE 802.11ax) забезпечує не лише збільшення швидкості передачі даних, а й оптимізацію витрат енергії в клієнтських пристроях, можливість координованої роботи сотень гаджетів у єдиному просторі та зменшення мережевого “завалювання” під час пікових навантажень.

Завершуючи роздуми про технічні аспекти, слід підкреслити й соціальну значущість. Оскільки радіоефір є відкритим, надзвичайно важливою є багаторівнева система безпеки: від сучасних шифрів WPA3 до розмежування користувацьких груп і віртуальних локальних мереж, що дозволяє діставати доступ лише авторизованим пристроям, а також впровадження механізмів моніторингу й аналізу аномальної мережевої активності.

Таким чином, безпровідні мережі поєднують високий рівень мобільності, універсальності та надійності — і саме в цьому поєднанні полягає їхня ключова роль у створенні інтелектуальних екосистем майбутнього.

1.1 Класифікація безпровідних мереж

Безпровідні мережі являють собою телекомунікаційні системи, які забезпечують передавання інформації за допомогою радіохвиль або інших видів електромагнітного випромінювання, що дає змогу уникнути використання фізичних з’єднувальних кабелів. Ці мережі відіграють ключову роль у сучасних інформаційних технологіях, слугуючи основою для мобільного зв’язку, мереж Wi-Fi, супутникових комунікацій та інших сервісів. Класифікацію безпровідних мереж здійснюють за різними критеріями, зокрема за радіусом дії, способом організації та технологією передавання сигналу.



Рисунок 1.1 – Класифікація безпровідних мереж

1.1.1 Класифікація та основні типи безпровідних мереж

Сучасні безпровідні мережі класифікують за такими основними ознаками:

– Радіус дії (географічне покриття);

– Базова технологія;

– Тип топології;

– Швидкість передавання даних;

– Призначення (споживче, промислове, критичне) слугує одним із критеріїв класифікації безпровідних мереж за умовами експлуатації, рівнем надійності та вимогами до безпеки.

Таблиця 1.1.1 – Класифікація безпровідних мереж за масштабом покриття

Тип мережі	Абревіатура	Радіус дії	Приклад
Персональна мережа	WPAN	до 10 м	Bluetooth, ZigBee
Локальна мережа	WLAN	до 100 м	Wi-Fi (802.11n/ac/ax)
Міська мережа	WMAN	до кількох км	WiMAX (802.16)
Глобальна мережа	WWAN	десятки та сотні км	LTE, 5G, супутниковий зв’язок

1.1.2 Класифікація за технологіями

Згідно з класифікацією Fortinet, типові технології дозволяють поділити безпровідні мережі на кілька основних категорій, що базуються на їх функціональних можливостях, сфері застосування та типі реалізованої архітектури.

– Wi-Fi — найбільш розповсюджений стандарт для WLAN (IEEE 802.11);

– Bluetooth, ZigBee, Z-Wave — WPAN-протоколи з низьким енергоспоживанням;

– LoRa, SIGFOX, NB-IoT, LTE-M — LPWAN-мережі для IoT та віддаленого моніторингу;

– 5G, LTE, WiMAX — широкосмугові мережі для мобільного доступу.

Супутниковий зв’язок забезпечує глобальне покриття, що особливо важливо в умовах відсутності іншої телекомунікаційної інфраструктури (наприклад, у

віддалених або важкодоступних регіонах).Окремо виділяють так звані безпровідні спеціалізовані цифрові мережі (БСЦМ), які поділяють за:

а) Радіусом дії:

1) Великий (до 100 км): *SIGFOX*, *LoRa*;

2) Середній (до 10 км): *LTE-M*, *NB-IoT*, *openRTLS*;

3) Малий (до 30 м): *RFID, RuBee*.

б) Базовими технологіями:

1) UNB (Ultra Narrow Band) — SIGFOX;

2) IEEE 802.15.4 — LoRa, ZigBee;

3) 3GPP — LTE, LTE-M, NB-IoT.

«RFID (Radio Frequency Identification) використовується для передачі даних на короткі дистанції з метою ідентифікації об’єктів і належить до класу безпровідних мереж ближньої дії.» Ці мережі часто застосовуються у промисловості, логістиці, нафтогазовій галузі, «розумних» будівлях тощо.

1.1.3 Топологічна класифікація

За топологією — тобто конфігурацією фізичних або логічних зв’язків між вузлами мережі — безпровідні мережі поділяються на такі основні типи:

– *Топологія «Зірка» (Star).* Усі вузли мережі підключаються до центрального пристрою (точки доступу, маршрутизатора, базової станції). Такий підхід спрощує

керування мережею, однак центральний вузол є критичним елементом, і його відмова призводить до зупинки всієї мережі;

– *Топологія «Дерево» (Tree).* Являє собою ієрархічну структуру, яка складається з декількох з'єднаних між собою сегментів типу «зірка». Вона дозволяє масштабувати мережу та організувати розподіл навантаження за рівнями;

– *Топологія «Сітка» (Mesh).* Кожен вузол з'єднаний з кількома іншими, що забезпечує резервування маршрутів. Така топологія є надійною та гнучкою, особливо в умовах змінної доступності вузлів. Широко застосовується в мережах IoT, військових системах, аварійних мережах;

– *Топологія «Шина» (Bus).* Усі вузли підключені до спільного каналу передавання даних. У безпровідних мережах застосовується рідко через складність керування колізіями та обмежену масштабованість;

– *Топологія «Кільце» (Ring).* Кожен вузол має два сусіди, і дані передаються по кільцю. Через високі затримки та складність маршрутизації в безпровідних мережах використовується вкрай рідко;

– *Топологія «Точка-точка» (Point-to-Point).* Передбачає прямий зв'язок між двома пристроями. Приклади включають Wi-Fi Direct, Bluetooth, або безпровідні мости між будівлями;

– *Топологія «Точка–багатоточка» (Point-to-Multipoint).* Один центральний вузол з'єднаний із кількома периферійними пристроями. Ця схема характерна для стільникових мереж, супутникового зв'язку та фіксованих безпровідних систем;

Топологія визначає як фізичну організацію мережі, так і логіку передавання даних, що впливає на її продуктивність, масштабованість і стійкість до відмов.

1.1.4 Узагальнена таблиця класифікації

Для систематизації основних характеристик безпровідних мереж доцільно узагальнити класифікаційні ознаки, що впливають на їх проєктування, вибір технологій та сферу застосування. У таблиці 1.1.4 наведено основні параметри, за якими здійснюється класифікація безпровідних мереж: радіус дії, використовувані технології, тип топології, цільове призначення та частотний діапазон. Така узагальнена форма дозволяє швидко оцінити відповідність конкретної мережі вимогам до пропускної здатності, масштабованості та експлуатаційної ефективності.

Таблиця 1.1.4 – Узагальнена класифікація безпровідних мереж за основними ознаками

Ознака класифікації	Варіанти
Радіус дії	WPAN, WLAN, WMAN, WWAN
Технологія	Wi-Fi, Bluetooth, LTE, LoRa, ZigBee, NB-IoT
Топологія	Ad-hoc, Mesh, Star, Tree
Призначення	Споживчі, Промислові, IoT, Військові
Частотний діапазон	2.4 ГГц, 5 ГГц, 900 МГц, ліцензовані діапазони.

1.1.5 Класифікація за частотним діапазоном

Різні безпровідні технології функціонують у певних частотних діапазонах, які визначають їхні характеристики, сферу застосування та вимоги до ліцензування. Частотні смуги умовно поділяються на неліцензовані (вільні для загального користування) та ліцензовані (використання яких регламентується державними органами зв’язку). Неліцензовані діапазони:

2,4 ГГц — один із найпоширеніших частотних діапазонів для бездротових мереж. Використовується в таких технологіях, як Wi-Fi (стандарти 802.11b/g/n), Bluetooth, ZigBee та ін. Його перевагами є широке поширення пристроїв і сумісність, проте цей діапазон характеризується високим рівнем завад через перевантаження ефіру та обмежену кількість доступних каналів.

5 ГГц — забезпечує вищу швидкість передавання даних і менший рівень завад, оскільки використовується меншою кількістю пристроїв. Основним недоліком є зменшена дальність покриття, особливо в умовах наявності перешкод. Використовується у Wi-Fi стандартах 802.11a/n/ac/ax.

868 МГц / 915 МГц — ці діапазони застосовуються переважно для технологій вузькосмугового зв’язку, таких як LPWAN (наприклад, LoRa, Sigfox), що орієнтовані на довготривалу роботу пристроїв з низьким енергоспоживанням на великих відстанях. Завдяки здатності проходити крізь перешкоди, ці частоти використовуються в системах моніторингу, автоматизації та Інтернеті речей.

Ліцензовані діапазони, зазвичай у межах 700 МГц – 3,5 ГГц і вище, застосовуються для стільникових мереж четвертого (LTE) та п’ятого (5G) поколінь. Їх використання вимагає отримання офіційних ліцензій. Ці частоти забезпечують високу пропускну здатність, стабільне з’єднання та підтримку значної кількості одночасних підключень. Вони активно використовуються в міських, приміських і промислових умовах.

Вибір частотного діапазону безпосередньо впливає на ефективність бездротової мережі. Частота визначає не лише швидкість і дальність зв’язку, а й тип антен, рівень енергоспоживання та стійкість до зовнішніх завад. Саме тому планування частотного ресурсу є важливим етапом при проектуванні сучасних безпровідних систем.

1.1.6 Переваги і недоліки окремих типів безпровідних мереж

У сучасних інформаційних системах безпровідні мережі відіграють ключову роль завдяки своїй гнучкості, мобільності та можливості забезпечення зв’язку в найрізноманітніших умовах. Проте, незважаючи на спільну мету — передавання даних без використання дротів, різні типи таких мереж мають суттєві відмінності. Їх розрізняють за зоною покриття, енергоспоживанням, швидкістю роботи та складністю розгортання.

Залежно від специфіки застосування — чи то персональні пристрої, промислові комплекси, транспортні системи або медичне обладнання — обирається той чи інший тип безпровідної мережі. Щоб краще орієнтуватися в їхніх особливостях, нижче наведено порівняльну таблицю, де узагальнено переваги й недоліки найбільш поширених типів таких мереж.

Таблиця 1.1.6 – Порівняння переваг і недоліків основних типів безпровідних мережі

Тип мережі	Переваги	Недоліки
WPAN	Низьке енергоспоживання, простота	Невеликий радіус дії
WLAN	Висока швидкість, доступність	Залежність від перешкод, зменшення сигналу через стіни
WMAN	Придатні для міських умов	Вимагають специфічного обладнання
WWAN	Велике покриття, мобільність	Висока вартість ліцензій та обладнання
LPWAN	Дуже низьке енергоспоживання, велика дальність	Обмежена швидкість передачі

Безпровідні мережі можуть бути орієнтовані на:

- Користувацьке використання — домашні роутери, смартфони, планшети;
- Промислові рішення (IoT) — сенсори, контроль виробництва, телеметрія;
- Медичні системи — передавання біомедичних даних у реальному часі;
- Військові та спеціальні завдання — захищені канали зв’язку, дрони, радіомаяки.

Транспортні системи — це безпровідні мережі типу V2V (vehicle-to-vehicle) та V2X (vehicle-to-everything), що забезпечують обмін даними між транспортними засобами та дорожньою інфраструктурою для підвищення безпеки та ефективності дорожнього руху.

Безпровідні мережі — це не лише технологія для зручного доступу до інтернету, а основа для побудови сучасних кіберфізичних систем, «розумних» міст, автономного транспорту та IoT. Їх класифікація дозволяє адаптувати технічні рішення до конкретних умов експлуатації, таких як відстань, швидкість, масштаб або енергоспоживання. З урахуванням швидкого розвитку нових стандартів (наприклад, Wi-Fi 7, 5G Advanced, 6G), поділ безпровідних мереж за різними ознаками є важливим як для практичної реалізації, так і для досліджень.

1.2 Основні стандарти Wi-Fi, LTE, 5G

Wi-Fi — це набір стандартів бездротової локальної мережі (WLAN), розроблений Інститутом інженерів електротехніки та електроніки (IEEE). Основні стандарти Wi-Fi включають:

- 802.11 — базовий стандарт з низькою швидкістю передачі;
- 802.11b — працює на частоті 2,4 GHz, до 11 Мбіт/с;
- 802.11a — частота 5 GHz, до 54 Мбіт/с;
- 802.11g — поєднує переваги b та a, до 54 Мбіт/с;
- 802.11n — до 600 Мбіт/с, підтримує технологію MIMO;
- 802.11ac — підвищення пропускної здатності до 1 Гбіт/с.

802.11ax (Wi-Fi 6) забезпечує на 37 % вищу швидкість, удвічі меншу затримку та в чотири рази більшу пропускну здатність порівняно з 802.11ac. Завдяки підтримці MU-MIMO та OFDMA він оптимізований для ефективної роботи в умовах високої щільності підключень, що робить його придатним для

офісів, стадіонів, «розумних» будівель і промислових об’єктів з великою кількістю IoT-пристроїв.Wi-Fi 6 орієнтований також на розвантаження мобільних мереж LTE/5G та підтримку IoT-пристроїв, забезпечуючи вищу щільність підключень, знижену затримку, кращу енергоефективність і стабільну передачу даних у середовищах з великою кількістю одночасних користувачів.

LTE (Long-Term Evolution) це стандарт мобільного широкосмугового зв’язку, затверджений консорціумом 3GPP. Забезпечує високошвидкісний мобільний доступ до Інтернету — до 100 Мбіт/с під час руху та до 300 Мбіт/с у стаціонарному режимі. Має низьку затримку (менше 10 мс), що є критично важливим для потокового відео, VoIP, онлайн-ігор та інших сервісів реального часу. Підтримує гнучке управління радіоресурсами, адаптивну модуляцію та агрегацію частотних каналів.

Завдяки архітектурі EPC (Evolved Packet Core), LTE повністю базується на IP, що спрощує інтеграцію з іншими IP-сервісами й технологіями, зокрема Wi-Fi та 5G.Удосконалення, такі як LTE-Advanced, дозволяють агрегацію носіїв (carrier aggregation), використання технології MIMO, а також впровадження механізмів покращеного модуляційного кодування та динамічного розподілу ресурсів, що суттєво підвищує швидкість передачі даних, спектральну ефективність і стабільність з'єднання навіть за високого навантаження мережі.

LTE також активно інтегрується з Wi-Fi, щоб розвантажувати мережі доступу та ефективно використовувати радіоресурси обох технологій, забезпечуючи безшовний хендовер, покращене покриття в густонаселених районах і підвищення загальної пропускної здатності мережі завдяки агрегації каналів та спільному управлінню трафіком.

5G є не просто наступником LTE, а представляє собою нову парадигму в розвитку телекомунікаційних систем, орієнтовану на задоволення вимог цифрового суспільства майбутнього. Основні стандарти формуються Міжнародним союзом електрозв’язку (ITU) в межах IMT-2020, а також консорціумом 3GPP (починаючи з Release 15).

Ключові характеристики 5G:

– Швидкість завантаження — до 10 Гбіт/с, що суттєво перевищує можливості попередніх поколінь;

– Наднизька затримка — менше 1 мс, що критично для сервісів реального часу;

– Масове підключення пристроїв — до 1 мільйона на 1 км², що дозволяє обслуговувати великі IoT-мережі;

– Надійність, масштабованість та енергоефективність — ключові вимоги для інфраструктури майбутнього;

– Нова радіотехнологія (NR) працює в діапазоні частот до 100 ГГц, зокрема в mmWave-смугах;

– Інтеграція технологій OFDMA, massive MIMO, beamforming, network slicing, які забезпечують адаптивність, гнучкість і високу ефективність використання радіочастотного спектра;

– 5G відіграє важливу роль у таких сферах, як автоматизоване виробництво, автономний транспорт, доповнена/віртуальна реальність (AR/VR), розумні міста та інтернет речей (IoT).

Таблиця 1.2 – Порівняльна характеристика стандартів Wi-Fi 6, LTE та 5G

Характеристика	Wi-Fi 6 (802.11ax)	LTE / LTE-Advanced	5G (NR – New Radio)
Частотний діапазон	2.4 / 5 GHz	< 6 GHz	<6 GHz (Sub-6) та >24 GHz (mmWave)
Пропускна здатність	До 9.6 Гбіт/с	До 1 Гбіт/с	До 10 Гбіт/с і більше
Затримка	~20-30 мс	~10 мс	<1 мс
Масштабування	Для локального покриття	Широкомасштабне	Масове підключення (IoT, URLLC, eMBB)
Мобільність	Обмежена	Висока	Дуже висока
Архітектура	Децентралізована (локальна)	Централізована	Хмарна, віртуалізована
Сфери застосування	Домашні, офісні, кампуси	Мобільний зв’язок	Вся цифрова інфраструктура

Сучасний розвиток бездротових технологій демонструє тенденцію до інтеграції та доповнення, а не конкуренції між стандартами Wi-Fi та мобільного зв’язку. У межах концепції гетерогенних мереж (HetNets) передбачається використання Wi-Fi 6 для високошвидкісного доступу в межах локальних зон

(LAN), тоді як 5G забезпечує надійний зв’язок у мобільних сценаріях або при масовому підключенні пристроїв у межах розширених зон покриття.

Технологія LTE-Advanced (стандарти 3GPP Release 10–13) відіграла ключову роль у підготовці інфраструктури до вимог 5G. Зокрема, були впроваджені:

- агрегація носіїв (carrier aggregation);
- покращені схеми модуляції;
- розширені механізми MIMO;
- підтримка handover між Wi-Fi і мобільною мережею.

Ці можливості забезпечили плавний перехід до архітектури 5G та її сервісів.

У межах концепції 5G Beyond (очікується після 2030 року) прогнозується інтеграція передових підходів: використання штучного інтелекту для динамічної оптимізації мережевих процесів, застосування терогенного спектру — поєднання традиційних і нових діапазонів, включаючи терагерцові частоти, розгортання адаптивних мереж зі свідомою реакцією на навколишнє середовище, поява нових типів зв’язку, зокрема видимого світлового зв’язку (Visible Light Communications, VLC) та терехвильових каналів зв’язку. Ці технології відкривають шлях до створення маштабних , і енергоефективних мереж нового покоління.

Wi-Fi орієнтований насамперед на забезпечення високої швидкості передавання даних у локальних мережах, що робить його оптимальним для використання в домашніх умовах, офісах, навчальних і комерційних приміщеннях.

LTE забезпечує стабільний мобільний доступ до Інтернету, однак має обмеження у контексті масового підключення пристроїв, що знижує його ефективність для машинного зв’язку та IoT-сценаріїв великого масштабу.

5G виступає як універсальна комунікаційна платформа, що поєднує переваги високої швидкості, низької затримки та масової масштабованості. Вона надає гнучке та адаптивне середовище для широкого спектра застосувань — від персонального мобільного зв’язку до індустріального Інтернету речей (IIoT), автономного транспорту, розумних міст і навіть віддаленої медицини.

1.3 Технології підвищення пропускної здатності мереж

У наш час бездротові мережі переживають справжній бум: стрімко зростає число під’єднаних пристроїв, а разом із тим — обсяги мультимедійного трафіку, спричинені відеоконференціями, потоковим відео та «розумними» датчиками Інтернету речей. Класичне визначення пропускної здатності як кількості мегабіт за секунду вже не охоплює всіх викликів: сьогодні важливо, щоб мережа не просто передавала якомога більше даних, а й добре справлялася з раптовими стрибками навантаження, в умовах радіоперешкод і навіть за руху користувачів. На старті часто вистачає оптимального налаштування існуючого обладнання — правильне розташування точок доступу для покриття «сліпих» зон і автоматичний вибір каналів з найменшим рівнем конкуренції можуть знизити перешкоди й підвищити середню швидкість на 20–30 % без жодних додаткових витрат. Водночас у великих системах (промислових мережах, міському IoT, розподілених сенсорних платформах) застосовують агрегацію й стиснення даних на периферії, відправляючи в ядро лише статистику — так вдається звільнити канал для найбільш критичних повідомлень і зменшити енергоспоживання сенсорних вузлів.

Наступний крок — впровадження сучасних Wi-Fi-стандартів. 802.11ac (Wi-Fi 5) приніс гігабітні швидкості в домашніх мережах, а 802.11ax (Wi-Fi 6) додав OFDMA для обслуговування кількох пристроїв одним кадром, MU-MIMO для одночасного зв’язку з великою кількістю клієнтів і Target Wake Time для енергозбереження IoT-датчиків. Це не просто «вищі цифри в характеристиках», а реальні інструменти підвищення ефективності й економії енергії в умовах великого навантаження.

Паралельно розвиваються просунуті технології: мережеве кодування дозволяє «зшивати» кілька пакетів у лінійні комбінації (наприклад, $A \oplus B$), знижуючи число трансляцій і підвищуючи стійкість до втрат, що особливо цінно в мобільних сценаріях із часто змінюваними маршрутами. У великій інфраструктурі

застосовують multipath-маршрутизацію та динамічний роутинг, щоб об’їжджати перевантажені ділянки мережі або перешкоди.

Найсучасніші рішення — на базі штучного інтелекту: алгоритми навчання з підкріпленням у режимі реального часу підбирають найкращі частоти та шляхи, глибинні нейронні мережі прогнозують піки трафіку за історією використання, федеративне навчання дає змогу пристроям обмінюватися лише узагальненими моделями (щоб зменшити обсяг переданих даних і підвищити конфіденційність), а edge-обчислення виконують попередній аналіз і фільтрацію безпосередньо на периферії. У результаті мережі стають справжніми самоорганізованими системами (SON), які без втручання адміністратора вчаться, адаптуються й тонко налаштовуються: затримки падають до –30 %, а реальна пропускна здатність росте на 10–15 % без додаткового обладнання. У підсумку сучасні бездротові мережі — це не просто набір точок доступу, а інтелектуальні, саморегульовані системи, які поєднують класичні технічні методи й алгоритми ШІ, щоб бути одночасно швидкими, надійними та гнучкими.

1.4 Інтернет речей (IoT) у бездротових мережах

Інтернет речей (IoT) уособлює ідею повсюдного підключення різноманітних пристроїв до однієї глобальної мережі, де вони самостійно збирають, обробляють і передають дані без участі людини. Зростання кількості таких «розумних» об’єктів вже найближчим часом може досягти сотень мільярдів, що ставить перед бездротовою інфраструктурою нові вимоги: вона має бути надзвичайно масштабованою, енергоефективною та вкрай надійною.

У невеликих просторах — вдома чи в офісі — ідеальним рішенням стають протоколи короткого радіусу дії: Bluetooth Low Energy, ZigBee або Wi-Fi HaLow. Вони добре працюють на обмежених відстанях, споживаючи мінімум енергії та

забезпечуючи стабільний зв’язок між датчиками, побутовою технікою й іншими переносними пристроями.

Якщо ж мова йде про покриття великих територій або про сценарії, коли заміна батарей практично неможлива, на виручку приходять LPWA-мережі (LoRaWAN, Sigfox, NB-IoT та LTE-M). Ці технології дозволяють сенсорам десятки кілометрів передавати невеликі пакети даних, працюючи від одного заряду роками. Вони знайшли застосування у розумному фермерстві, екологічному моніторингу, «розумних» містах та інфраструктурних системах.

У складних проєктах, де паралельно треба керувати сотнями тисяч пристроїв із гарантованою якістю обслуговування, використовують мобільні мережі — від класичного GSM/UMTS/LTE до їх спеціалізованих версій NB-IoT і LTE-M. Інтеграція в існуючу стільникову інфраструктуру дозволяє централізовано керувати величезними IoT-парками, легко масштабувати рішення та швидко реагувати на зміни навантаження.

Коли у міських умовах радіочастоти переповнені через високу щільність підключень, на допомогу приходять технології багатоканального доступу та MIMO, які ефективно розподіляють спектр між тисячами пристроїв і знижують рівень перешкод. Це критично важливо, щоб уникнути затримок і втрат пакетів у «розумних» промислових або транспортних мережах.

Оскільки більшість IoT-пристроїв працюють від батарей, розробники приділяють велику увагу економії енергії: у протоколах передбачені глибокі режими сну, поштовхові пробудження та адаптивне планування передачі даних.

Не менш важливим є питання безпеки — як захистити дані та сама мережу. Обчислення на периферії (edge computing) зменшують затримки, але розширюють площу атаки, тож для захисту впроваджують шифрування, взаємну автентифікацію пристроїв і регулярні оновлення прошивок.

Ще одне випробування IoT — це гетерогенність стандартів у різних пристроях і платформах. Щоб зробити «розумний» дім або місто дійсно інтегрованим, використовують мультипротокольні шлюзи та універсальні хмарні платформи, які підтримують одночасно десятки технологій.

Таким чином, розвиток Інтернету речей тримається на трьох китах: технологіях короткого радіусу для персональних і побутових систем, LPWA-мережах для довготривалого моніторингу на великих відстанях і мобільних стандартах для корпоративних рішень із високими вимогами до надійності та керованості.

1.5 Вікімережі та Mesh-технології

Mesh-мережі будуються з рівноправних вузлів, кожен із яких водночас передає й приймає дані, а маршрути для пакунків формуються динамічно. Після увімкнення вузол самостійно знаходить сусідів, визначає якість каналу й оновлює свої маршрути, тож навіть якщо хтось із них виходить із ладу, весь потік автоматично переформатується іншим шляхом (рис. 1.3). Така гнучкість значно підвищує стійкість мережі та знижує потребу в ручному налаштуванні — вузли самі обмінюються інформацією про обставини навколо себе й адаптують свої налаштування.

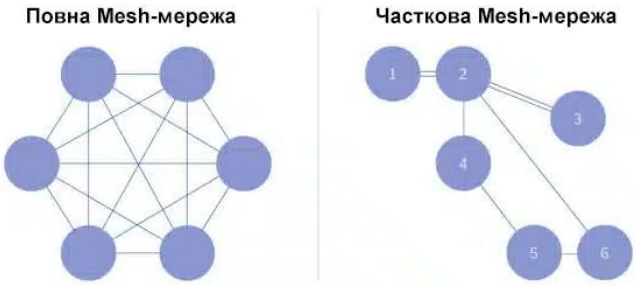


Рисунок 1.2 –Повна Mesh-мережа та часткова Mesh-мережі

У «розумних» містах mesh-мережі дозволяють об’єднати сотні й тисячі точок Wi-Fi, датчиків повітря та освітлення в єдину самоконфігуровану систему. Наприклад, сенсори якості повітря на вуличних ліхтарях збирають дані в реальному часі та передають їх через сусідні вузли до центру управління. Якщо в районі проводяться планові ремонти або трапляються раптові відключення, мережа сама вибудовує обхідні маршрути, щоб інформація надходила безперебійно.

У сенсорних мережах, де кожен прилад працює від батарей або енергоємного живлення, mesh-архітектура допомагає зберігати ресурси. Сенсори обирають найкоротші шляхи до збору даних, зменшуючи кількість «передавань» і, отже, економлячи заряд. Крім того, нові прилади додаються в мережу без складної конфігурації — вони просто під’єднуються до найсильнішого сигналу, і вся система інтегрує їх у наявну топологію.

У результаті mesh-мережі поєднують у собі відмовостійкість та самостійність розгортання. Вони ідеально підходять для масштабних проєктів «Інтернету речей», де важлива безперервність обміну даними, та для міських інфраструктур, що потребують оперативного моніторингу та керування. Їхня здатність самоорганізовуватися робить проєкти простішими у впровадженні й надійнішими в експлуатації. Водночас сучасні стандарти шифрування та аутентифікації на рівні мережевих протоколів забезпечують захищеність переданих даних, що особливо важливо для критичних застосувань.

складної конфігурації — вони просто під’єднуються до найсильнішого сигналу, і вся система інтегрує їх у наявну топологію.

У результаті mesh-мережі поєднують у собі відмовостійкість та самостійність розгортання. Вони ідеально підходять для масштабних проєктів «Інтернету речей», де важлива безперервність обміну даними, та для міських інфраструктур, що потребують оперативного моніторингу та керування. Їхня здатність самоорганізовуватися робить проєкти простішими у впровадженні й надійнішими в експлуатації. Водночас сучасні стандарти шифрування та аутентифікації на рівні мережевих протоколів забезпечують захищеність переданих даних, що особливо важливо для критичних застосувань.

2 ІНФРАСТРУКТУРА БЕЗДРОТОВОГО ЗВ’ЯЗКУ

Інфраструктура бездротового зв’язку — це сукупність апаратних та програмних засобів, що забезпечують організацію, керування і підтримку обміну даними між мобільними або стаціонарними пристроями без використання фізичних кабельних з’єднань. У сучасному цифровому середовищі така інфраструктура відіграє ключову роль у забезпеченні мобільності, гнучкості доступу до ресурсів та масштабованості систем зв’язку. Склад інфраструктури бездротової мережі, як правило, включає:

– базові станції (наприклад, стільникові вишки або точки доступу Wi-Fi);

– мережеве обладнання (маршрутизатори, комутатори, шлюзи);

– транспортувальні магістралі (оптоволоконні, супутникові або мікрохвильові канали);

– центри обробки даних та хмарні платформи, які обробляють, зберігають та розподіляють інформацію;

– системи керування мережею, що забезпечують моніторинг, конфігурацію та балансування навантаження.



Рисунок 2.1 – Структура інфраструктури бездротового зв’язку

Успішна реалізація бездротових мереж залежить від оптимального розміщення передавальних пунктів (точок доступу), вибору частотного спектра, типу протоколів зв’язку, як-от Wi-Fi, LTE, 5G, та використання відповідного програмного забезпечення для керування трафіком і безпекою.

Сучасні архітектури передбачають інтеграцію розподілених обчислень, віртуалізації функцій мережі (NFV), інтелектуального аналізу трафіку та механізмів самовідновлення, що дозволяє забезпечити високий рівень якості обслуговування (QoS) навіть у динамічному середовищі з непередбачуваним навантаженням.

Крім того, інфраструктура має враховувати: енергетичну ефективність, особливо в розгортанні мереж у важкодоступних або ізольованих регіонах; захищеність від несанкціонованого доступу чи атак, зокрема шляхом використання шифрування, автентифікації, ідентифікації користувачів; адаптивність до зростання кількості IoT-пристроїв, які постійно змінюють вимоги до пропускної здатності.

Розвиток технологій, таких як Wi-Fi 6/6E, 5G та майбутній 6G, вимагає від інфраструктури підтримки наднизьких затримок, високої щільності підключень і обробки величезного обсягу даних. Це зумовлює інтеграцію зі штучним інтелектом та машинним навчанням для оптимізації використання ресурсів.

Таким чином, інфраструктура бездротового зв’язку є критично важливою ланкою сучасних інформаційно-комунікаційних систем і вимагає системного підходу до її проєктування, підтримки та модернізації.

2.1 Рівні моделі OSI в бездротовій інфраструктурі

У сучасних бездротових мережах семирівнева модель OSI слугує універсальним каркасом для опису процесів передачі даних. Вона дозволяє чітко розділити функції від фізичної передачі сигналу до прикладного інтерфейсу, що

спрощує проєктування й аналіз мережевих систем. Нижче подано стислий виклад кожного рівня моделі OSI в контексті бездротових технологій.



Рисунок 2.2 – Рівні моделі OSI та їхні функції

Фізичний рівень відповідає за передачу двійкових сигналів у вигляді електромагнітних хвиль. У бездротових мережах його реалізація передбачає вибір радіочастотного діапазону, методів модуляції (OFDM, DSSS тощо), налаштування потужності передавача та ширини каналу. До основних завдань цього рівня належить забезпечення оптимального співвідношення між дальністю передавання та рівнем втрат, підвищення стійкості сигналу в умовах перешкод, а також підтримка технологій MIMO, DFS і канал-бондингу для збільшення пропускної здатності та надійності зв’язку.

Канальний рівень формує кадри даних, контролює їхню цілісність і координує доступ пристроїв до спільного середовища. У сучасних стандартах Wi-Fi застосовується механізм CSMA/CA, який запобігає колізіям у радіоефірі шляхом перевірки вільності каналу перед передаванням кадру. Крім того, на цьому рівні реалізуються процедури виявлення помилок (CRC) та протоколи

автоматичного повторного запитування втрачених кадрів (ARQ), а також механізми пріоритезації трафіку (QoS) для забезпечення необхідного рівня обслуговування мультимедійних та голосових сервісів.

Мережевий рівень відповідає за логічну адресацію пристроїв і визначення маршрутів передачі пакетів від джерела до одержувача. В умовах мобільності застосовуються IPv6 та Mobile IP, які дозволяють підтримувати стійке з'єднання під час переходу між точками доступу без зміни логічної адреси. У ad-hoc та mesh-мережах використовуються протоколи динамічної маршрутизації (OLSR, AODV), що автоматично будують оптимальні шляхи з урахуванням затримки та якості радіозв'язку

Транспортний рівень гарантує доставку даних у повному обсязі та в правильному порядку. Протокол TCP здійснює сегментацію, контроль цілісності (контрольні суми) і керування рухом (flow control), а протокол UDP забезпечує мінімальні затримки за рахунок відмови від перевірок порядку та повторних передач. У бездротовому середовищі падіння пакетів може бути викликане не тільки завантаженістю мережі, а й радіоперешкодами, тому стандарт TCP доповнюють алгоритмами селективного підтвердження (Selective ACK) або використовують сучасні транспортні протоколи (QUIC), які адаптуються до режимів втрат і затримок.

Сеансовий рівень встановлює й координує взаємодію між кінцевими вузлами протягом однієї логічної сесії. Він обробляє процедури встановлення, підтримки та завершення сеансу, а також відновлення зв'язку після тимчасових перерв. Це особливо актуально для тривалих трансляцій або відеоконференцій, де необхідне збереження контексту обміну даними без повторної аутентифікації та налаштування параметрів зв'язку.

Представницький рівень забезпечує уніфікацію форматів даних: кодування (UTF-8, ASCII), стиснення (gzip, JPEG) та шифрування (TLS, AES). Він відповідає за перетворення структур даних так, щоб клієнт і сервер сприймали їх однаково, та за захист інформації від несанкціонованого доступу під час передавання по відкритому середовищу.

Прикладний рівень надає інтерфейс для кінцевих сервісів: веб-браузерів, поштових клієнтів, хмарних та мультимедійних додатків. У бездротових мережах він виконує додаткові функції адаптації сервісів до змінної пропускної здатності та затримок, наприклад, динамічне коригування якості відеопотоку, керування буферизацією та вибір протоколів (HTTP/2, QUIC) для забезпечення безперебійного користувацького досвіду.

2.2 Компоненти мережевої інфраструктури бездротового доступу

Високошвидкісні бездротові мережі сьогодні є критично важливою складовою IT-інфраструктури, що забезпечує мобільність, гнучкість і масштабованість сучасних сервісів. Надійність і продуктивність таких мереж залежать від чіткої взаємодії кількох ключових компонентів, кожен із яких виконує свою специфічну роль у загальній архітектурі.

Інфраструктура високошвидкісної бездротової мережі доступу починається з точок доступу (Access Point, AP) — радіомодулів із вбудованим Ethernet-інтерфейсом, які транслюють бездротовий сигнал і приймають підключення кінцевих пристроїв. Сучасні AP підтримують стандарти 802.11ac/ax, технології MIMO, OFDMA й beamforming, що забезпечує високу швидкість, надійність зв’язку та обслуговування великої кількості користувачів.

Централізоване управління точками доступу здійснює контролер (Wireless LAN Controller, WLC). Він автоматично конфігурує та оновлює прошивку AP, балансує навантаження між ними, реалізує автентифікацію за стандартом 802.1X та шифрування трафіку, а також забезпечує швидкий роумінг (fast handoff) у межах мережі.

Для агрегації Ethernet-з’єднань від AP використовують мережеві комутатори рівня L2/L3, які підтримують PoE (Power over Ethernet) для живлення точок

доступу, VLAN-ізоляцію трафіку різних SSID, а також маркування QoS (DSCP/CoS) для пріоритезації пакетів із голосом чи відео.

Між бездротовою інфраструктурою та зовнішніми мережами (Internet, MPLS) розташовується маршрутизатор або мережевий шлюз, який виконує функції NAT, VPN-концентратора для віддаленого доступу, міжмережевого екрана (stateful-firewall) і політики маршрутизації (BGP, OSPF).

Інтеграція з AAA-системою (RADIUS або TACACS+) забезпечує централізовану автентифікацію, авторизацію та облік підключень. Сервер перевіряє облікові дані користувачів або пристроїв, призначає ролі й політики доступу та фіксує статистику використання мережі.

Ключову роль у плануванні покриття відіграють антени — панельні, секторні або всенаправлені — та якісні коаксіальні кабелі з низькими втратами. Вони формують потрібну спрямованість і забезпечують оптимальний радіоплан із урахуванням інтерференції та перешкод.

Для передачі трафіку від комутаторів і контролерів до ядра мережі або провайдера використовується бек-хол — дротовий (оптоволоконний, Ethernet) або бездротовий (міліметровий радіозв’язок). У мережах високої пропускної здатності він проєктується з розрахунку на ємність 10 Gbps+ і мінімальну затримку.

Мережева безпека реалізується за допомогою IDS/IPS для Wi-Fi, систем WIPS (Wireless IPS) та NAC (Network Access Control). Ці рішення виявляють підозрілі точки доступу (rogue AP), блокують атаки «Evil Twin» і сегментують гостьовий трафік у виділені VLAN.

Централізований моніторинг і управління всією інфраструктурою забезпечує NMS/EMS. Воно збирає метрики (завантаження AP, рівні сигналу, помилки), будує карти покриття, відправляє сповіщення про збої та допомагає планувати розширення мережі на основі аналітики трендів.

Нарешті, для безперебійної роботи всіх компонентів важливі джерела резервного живлення (UPS) та система охолодження серверної кімнати. Вони захищають обладнання від перепадів напруги, збільшують час автономної роботи під час аварій і підтримують оптимальний температурний режим.



Рисунок 2.3 – Архітектура бездротової мережі

Принципи роботи:

Покриття. Точки доступу з відповідними антенами формують суцільну клітинну структуру, що забезпечує безперервний зв’язок;

Агрегація. PoE-комутатори живлять AP і передають їхній трафік до контролера або ядра мережі;

Контроль. WLC централізує політики безпеки, налаштування радіо й здійснює швидкий роумінг;

Доступ. AAA-сервер перевіряє облікові дані кожного пристрою, забезпечуючи авторизований вхід і облік використаних ресурсів;

Прохід. Маршрутизатор/VPN-шлюз шифрує й передає трафік до зовнішніх мереж із застосуванням міжмережевого екрана;

Управління. NMS/EMS моніторить стан мережі, аналізує тренди й оперативно сповіщає про відмови.

Таким чином, багаторівнева архітектура гарантує, що бездротова мережа високої пропускної здатності буде не лише швидкою, а й керованою, безпечною та готовою до майбутнього розширення.

2.3 Топологія та розміщення точок доступу і антен

Ефективність функціонування бездротової мережі значною мірою визначається правильністю проєктування топології та вибором місць встановлення точок доступу (AP) і антен. Саме від фізичного розташування компонентів залежить рівномірність покриття, стійкість радіосигналу й загальна пропускна здатність системи.

Однією з важливих передумов якісного покриття є орієнтація на реальні маршрути й сценарії пересування користувачів. Якщо точка доступу змонтована в коридорі чи технічному приміщенні — де пристрої практично не використовуються — це призводить до зниження інтенсивності сигналу при проходженні крізь стіни, меблі та інші перешкоди. Внаслідок цього падає швидкість передачі даних або з’являються “сліпі” зони без зв’язку.

Ускладнює ситуацію й перекриття каналів, особливо за високої густоти AP в офісних кластерах. При роботі сусідніх точок на однакових частотах зростає рівень колізій, збільшуються затримки передачі й зменшується ефективна пропускна здатність мережі.

Ще одним критичним чинником є висота та орієнтація антен. Для забезпечення оптимального покриття найчастіше застосовують монтаж AP під стелею або безпосередньо на стелі, спрямовуючи антени вниз. Така схема гарантує рівномірне охоплення робочих місць і рухомих користувачів. У довгих коридорах доцільно використовувати спрямовані антени, тоді як у відкритих просторах — всеспрямовані.

Для об’єктів із складною геометрією або високою щільністю клієнтів рекомендується вдатися до алгоритмічних методів розрахунку покриття. Зокрема застосування генетичних алгоритмів чи симуляційного аналізу дає змогу змоделювати RF-середовище й автоматично підібрати оптимальні позиції AP з урахуванням завад, відбиттів і зон перекриття. Практика показує, що такі підходи дозволяють підвищити якість покриття до 20 % без додаткових витрат на

обладнання. У практичному проєктуванні слід уникати типових помилок, характерних навіть для досвідчених інсталяцій:

– розміщення АР у коридорах або технічних зонах замість пріоритетних робочих зон користувачів;

– нехтування характеристиками будівельних матеріалів та внутрішніми перешкодами (металеві перегородки, електроніка);

– робота сусідніх АР на однакових каналах без адаптивного керування частотами;

– невідповідний вибір діаграми спрямованості антен для конкретної конфігурації приміщення;

– відсутність попереднього RF-планування із застосуванням профільного програмного забезпечення.

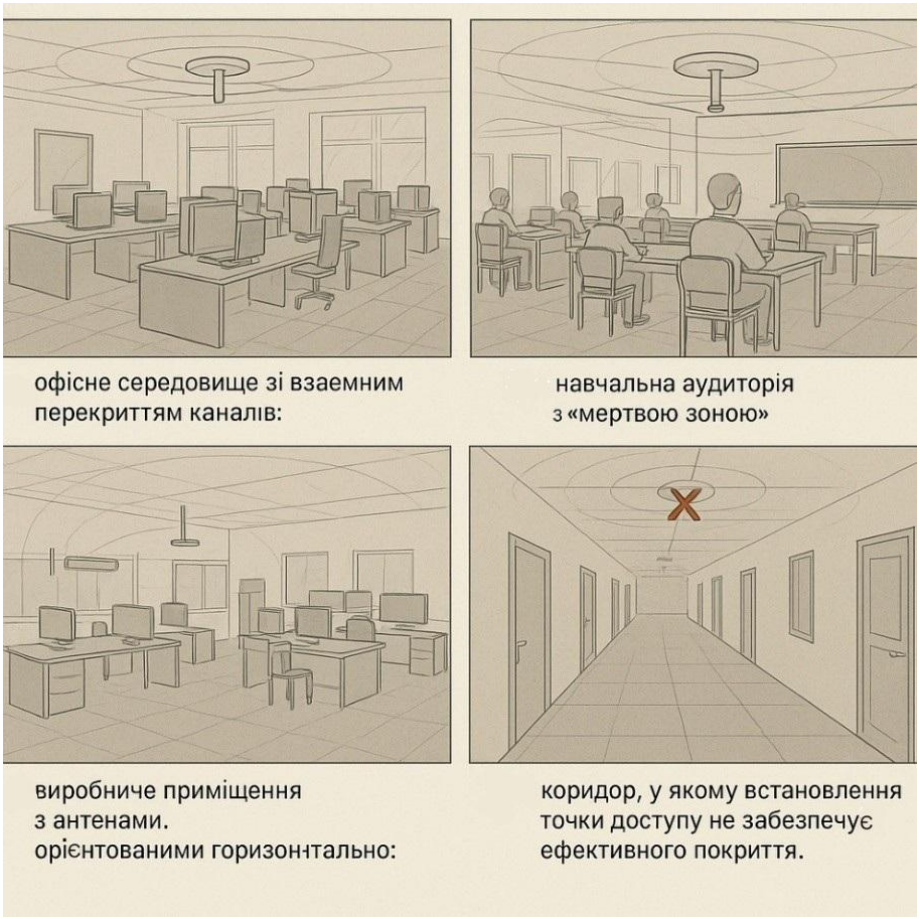


Рисунок 2.4 — Приклади невдалого розміщення точок доступу у типових приміщеннях

Якісне розміщення точок доступу — це інтегрований процес, який охоплює архітектуру приміщення, аналіз поведінкових патернів користувачів, характеристики джерел інтерференції та вимоги до майбутнього масштабування мережі. Такий підхід забезпечує високу продуктивність і надійність бездротової інфраструктури без зайвих витрат.

2.4 Фактори, що впливають на якість бездротового зв’язку

Якість бездротового зв’язку виникає як наслідок гармонійної взаємодії апаратних можливостей мережевого обладнання та умов реального середовища, у якому ці можливості реалізуються. Насамперед ключовим завданням проєктувальника є визначення оптимальних точок розміщення АР у тих ділянках, де зосереджена основна маса користувачів. Якщо встановити точку доступу в коридорі чи за стіною технічного приміщення, замість того щоб врахувати маршрути руху та зони перебування людей, сигнал невблаганно затухатиме, долаючи залізобетон і металеві конструкції, залишаючи за собою «мертві зони», де пристрої просто не бачать мережі.

Одночасно варто пам’ятати про будівельні матеріали: арматура в бетоні, сталеві перегородки та товсті цегляні стіни поводяться зі радіохвилями як дзеркала або губка — вони або відкидають їх, або поглинають. Тому в проєкті необхідно закласти поправочні коефіцієнти втрат для кожного типу перешкоди, щоб у підсумку забезпечити заданий рівень прийому та пропускну здатність мережі навіть у найскладніших умовах.

Наступний вимір — антенна підсистема. У просторих приміщеннях із вільним плануванням офісу доцільно використовувати всеспрямовані антени під стелею, що розгортають сигнал навколо себе у всіх напрямках, забезпечуючи однорідне покриття без «провалів». Натомість у довгих, вузьких коридорах або виробничих цехах, де потрібно «тягнути» сигнал вздовж одного коридору,

ефективнішими будуть спрямовані антени, які підсилюють випромінювання саме в напрямку осі проходу, зменшуючи енерговитрати й покращуючи стійкість зв’язку.

Якщо перейти до частотного планування, слід зазначити: кілька десятків точок доступу, встановлених без урахування канальної синхронізації, починають конкурувати за вузький спектр смуги. Результат — взаємна інтерференція, колізії пакетів і зріст затримок, від чого страждає кінцевий користувач. Щоб упередити подібні проблеми, сучасні контролери динамічно регулюють потужність передавання та автоматично обирають вільні частоти в реальному часі, зводячи до мінімуму людський фактор у налаштуваннях і підтримуючи стабільність мережі за мінливих умов.

Нарешті, коли мова йде про складні за конфігурацією простори або великі скупчення одночасних підключень — гостьові зони, конференц-зали, промислові цехи — на арену виходять алгоритмічні методи. Симуляційне моделювання, генетичні, евристичні алгоритми й аналіз «що-якщо» дають змогу змоделювати тисячі варіантів розміщення і звести до мінімуму ризики утворення «мертвих» зон. За допомогою таких інструментів ми не просто спрощуємо проєкт, а створюємо адаптивну, «розумну» мережу, готову автоматично пристосовуватися до змін у навантаженні й зовнішніх перешкодах.

Узгоджене застосування всіх цих заходів — від грамотного розташування АР і вибору антен до автоматичного керування параметрами та просунутих алгоритмів оптимізації — забезпечує високу надійність, стабільність і максимальну пропускну здатність бездротового зв’язку, якої потребують сучасні підприємства та організації.

2.5 Безпека та захист у бездротовій інфраструктурі

Безпровідна інфраструктура вимагає узгодженого поєднання інженерних розрахунків та операційних заходів безпеки, починаючи з докладного радіо-планування. На цьому етапі виконують вимірювання параметрів каналу (RSSI, SNR, затримки) за допомогою спеціалізованих сканерів спектру, складають link budget для кожної зони й моделюють покриття з урахуванням будівельних матеріалів і розташування антен. Такий підхід дозволяє обрати оптимальні параметри потужності, спрямованості антени та частотних каналів, мінімізуючи інтерференцію й «мертві зони».

Щоб гарантувати, що до мережі потрапляють лише довірені пристрої, впроваджують централізовану автентифікацію за IEEE 802.1X із сертифікатами X.509 і протоколами EAP-TLS (для максимальної безпеки) або EAP-PEAP (для зручності інтеграції з існуючими Active Directory). Одночасно мережу сегментують на віртуальні LAN (VLAN) із чітко визначеними політиками: корпоративний сегмент із суворими ACL, гостьовий сегмент із обмеженим доступом до ресурсів і окремі віртуальні мережі для IoT-пристроїв, кожна з яких має власний профіль доступу та таймаути сесій.

Шифрування трафіку на канальному рівні реалізується через WPA3-SAE із 192-бітним AES-CCMP-шифруванням і обов’язковою ротацією ключів на кожній сесії. Додатковим захистом служить тунелювання на транспортному рівні за допомогою IPsec VPN або TLS 1.3, що створює ізольований тунель для критичних даних. При цьому важливо відмовитися від застарілих алгоритмів (WEP, TKIP) і впроваджувати механізми перевірки списків відкликаних сертифікатів (CRL) або OCSP.

Нарешті, безперервний моніторинг і підтримка — це запорука стійкості. Системи WIDS/WIPS виконують аналіз радіоспектра 24/7, виявляючи індикатори атак (rogue AP, deauth flood, beacon spam) і передаючи події в SIEM для кореляції з іншими журналами. Регулярні автоматизовані оновлення прошивок і щоквартальні

пен-тести дозволяють вчасно закривати нові вразливості, а документовані процедури управління змінами гарантують відновлення працездатності мережі після будь-яких модифікацій конфігурацій. Такий життєвий цикл безпеки забезпечує безперервне дотримання політик і високу надійність безпровідної інфраструктури.

2.6 Енергозберігаючі рішення та екологічна відповідальність у сучасних бездротових мережах

В останні роки оптимізація енергоспоживання стала однією з основних задач для розробників і операторів бездротових мереж. Щорічне зростання кількості підключених пристроїв, поява IoT-платформ і збільшення площі покриття напряму впливають на загальні витрати електроенергії та експлуатаційні витрати. У багатьох випадках достатньо впровадити прості кроки: наприклад, у корпоративних Wi-Fi-мережах ефективний розподіл навантаження між точками доступу дозволяє знизити середню потужність передавачів на 20–25 %, а правильне планування графіка роботи IoT-сенсорів допомагає відправляти лише важливі повідомлення, залишаючи другорядні пристрої в режимі очікування.

Нові стандарти, такі як Wi-Fi 6, Wi-Fi 6E та 5G NR, інтегрують енергоощадні функції безпосередньо у протокол. Target Wake Time дозволяє IoT-пристроям погоджувати розклад з точкою доступу: сенсори температури, камери, або датчики вологості прокидаються тільки на короткий час для передачі інформації, решту часу залишаючись у сплячому режимі. MU-MIMO й OFDMA зменшують потребу в повторних трансляціях і розділяють канал на багато незалежних потоків, що важливо для офісів, де працює кілька сотень користувачів і десятки автоматизованих систем.

Окрема увага приділяється використанню «зелених» джерел живлення для базових станцій і обладнання. У віддалених районах дедалі частіше застосовують

сонячні панелі або невеликі вітрові електростанції, а в конструкції самих точок доступу використовують перероблені матеріали. В дата-центрах трафік оптимізують, щоб скоротити кількість операцій читання й запису, що напряму впливає на споживання енергії.

У великих корпоративних або кампусних мережах енергозбереження організовують на кількох рівнях: автоматичне перемикання точок доступу в нічний або вихідний час у режим зниженої потужності, використання адаптивних контролерів для балансування клієнтів і підтримка інтеграції з системами керування будівлею. Наприклад, у типовому офісному центрі Wi-Fi 6E дозволяє кожному пристрою самостійно обирати найближчу точку доступу з оптимальним рівнем сигналу та мінімальним навантаженням, а BMS автоматично вимикає підсвітку й клімат-контроль у неактивних зонах.

Результати таких підходів — зниження витрат електроенергії до 30 % у порівнянні з традиційними схемами та збільшення терміну служби автономних пристроїв. У підсумку мережа отримує не тільки стабільне покриття та високу швидкість, але й можливість відповідати сучасним стандартам енергоефективності.

3 ПРОЄКТУВАННЯ ТА АНАЛІЗ БЕЗДРОТОВОЇ МЕРЕЖІ

Проєктування бездротової мережі — це створення невидимої інфраструктури для одночасного обслуговування сотень кінцевих пристроїв: робочих станцій, IP-телефонів, систем відеоконференцій і «розумних» сенсорів. Кожна точка доступу, кожен канал зв'язку та рівень безпеки повинні бути налаштовані так, щоб гарантувати високу пропускну здатність, мінімальну затримку й безшовний роумінг у будь-якій зоні будівлі — від конференц-зали до серверної. Таке завдання неможливо вирішити простим «повісити кілька точок» — адже середовище диктує свої правила. Далі — головні виклики, які доведеться розв'язати:



Рисунок 3.1 — Основні аспекти проєктування бездротової мережі

Покриття. Сигнал повинен проникати через бетон, скло й металеві перегородки, щоб дійти до кожного робочого місця;

Пропускна здатність. У години пік відеодзвінків, хмарних синхронізацій та IoT-трафіку мережа має рівномірно розподіляти навантаження між точками доступу.

Інтерференція. Сторонні Wi-Fi, Bluetooth-периферія або індустріальні радіомодеми створюють «радіошум» — планування каналів і потужності передачі стає критичним;

Безпека. Сегментація трафіку, сучасні протоколи шифрування (WPA3), окремі SSID для гостей і IoT-пристроїв — щоб запобігти несанкціонованому доступу;

Роумінг і плинність. Мобільні пристрої мають безшовно переходити від однієї точки доступу до іншої без «провисань» зв’язку й повторної аутентифікації.

Моніторинг і аналітика. Після запуску мережа потребує постійного контролю: збір метрик RSSI, MCS, пінгів і навантаження CPU точок, а також автоматичне регулювання (RRM, airtime fairness) для стабільної роботи.

Сучасні бездротові мережі також потребують постійного оновлення прошивок і оперативного реагування на нові уразливості, щоб не допустити витоку даних чи зовнішніх атак. Важливо враховувати й резервування основних компонентів — це дозволяє уникнути простоїв у разі збою обладнання чи оновлення програмного забезпечення. Ефективне проєктування передбачає гнучкість до майбутніх змін: з розрахунком на зростання кількості пристроїв, підвищення вимог до пропускної здатності та підтримку нових технологічних стандартів. Саме такий підхід дозволяє мережі залишатися стабільною, надійною та готовою до викликів майбутнього.

3.1 Вибір стандарту та мережевих технологій

У виборі технології для побудови бездротової мережі високої пропускної здатності першочергово слід звернути увагу на три рішення: Wi-Fi 6 (IEEE 802.11ax), 5G (IMT-2020) та SD-WAN. Wi-Fi 6, або IEEE 802.11ax, оптимізовано для середовищ із високою щільністю користувачів — офісів, кампусів чи складів — завдяки впровадженню OFDMA та MU-MIMO, які значно

підвищують ефективність використання радіочастот та дозволяють одночасно обслуговувати численні пристрої без суттєвого зниження швидкості. Окрім цього, стандарт передбачає механізми енергозбереження для пристроїв Інтернету речей, що важливо для довготривалої роботи сенсорів і датчиків .

5G за концепцією IMT-2020 формує нову архітектуру мобільного зв'язку з можливістю обслуговувати понад мільйон пристроїв на квадратний кілометр, забезпечуючи затримки нижче ніж 1 мс і пікові швидкості передачі до 20 Гбіт/с. Така конфігурація ідеально підходить для міських інфраструктур, мереж «розумного міста» та мобільних сценаріїв, де критичною є стабільність і швидкість на великих територіях .

SD-WAN (Software-Defined WAN) не є телекомстандартом, але дозволяє централізовано керувати маршрутами між філіями, хмарними середовищами та дата-центрами, автоматично обираючи найоптимальніший канал (MPLS, LTE, широкосмуговий інтернет тощо). Завдяки Cisco Catalyst SD-WAN організації можуть гнучко реагувати на зміну навантаження, знижувати витрати на мережеву інфраструктуру і забезпечувати високу доступність сервісів незалежно від типу транспорту.

Таблиця 3.1 – Порівняння ключових характеристик технологій Wi-Fi 6 (IEEE 802.11ax), 5G (IMT-2020) та SD-WAN

Характеристика	Wi-Fi 6 (IEEE 802.11ax)	5G / IMT-2020	SD-WAN
Пропускна здатність	до 9,6 Гбіт/с	до 20 Гбіт/с	залежить від обраного каналу
Радіус дії	до 100 м (локально)	до кількох км	не залежить від радіуса (WAN-транспорт)
Затримка	≈ 10 мс	< 1 мс	оптимізується програмно, залежить від WAN
Орієнтація	внутрішні мережі, кампуси	мобільність, широка зона	централізоване керування розподіленою мережею
Ідеальний сценарій	офіси, Wi-Fi IoT, навчальні заклади	Smart City, транспорт	корпоративна WAN-інфраструктура

У підсумку, Wi-Fi 6 найкраще підходить для внутрішніх просторів із багатьма пристроями, 5G — для широкомасштабного покриття й мобільних застосунків із критично низькими затримками, а SD-WAN — для гнучкого й ефективного управління розподіленим корпоративним трафіком. Водночас вибір конкретного рішення повинен базуватися на аналізі економічної доцільності, вимог до безпеки й наявної інфраструктури. Часто оптимальним виявляється комбінований підхід: наприклад, використання SD-WAN для магістрального з'єднання між філіями та 5G або Wi-Fi 6 для останньої милі. Інтеграція цих технологій у єдину платформу дозволяє централізовано моніторити роботу мережі, швидко масштабувати сервіси й оперативно реагувати на відмови. Нарешті, варто передбачити можливості майбутнього оновлення стандартів, щоб мережа залишалася стійкою до технологічних викликів наступного десятиліття.

3.2 Моделювання навантаження та пропускної здатності

У задачі моделювання навантаження перш за все потрібно визначити склад і характеристику трафіку, який доведеться пропускати через мережу. У нашій моделі розглядають три основні типи потоків: атмосферні (або «елементарні») з постійною швидкістю — наприклад, VoIP або передача телеметричних даних IoT, потоки зі змінною інтенсивністю (відеостріми HD/4K, відеоконференції) та епізодичні «пікові» передачі (завантаження великих файлів, резервні синхронізації).

$$R_{in} = \sum_{\{i=1\}}^{N} \lambda_i \cdot L_{\{p,i\}} \cdot 8 \qquad (3.1)$$

Середня інтенсивність потоку λ_i визначає кількість пакетів, які надходять у секунду для потоку з номером i. Середній розмір пакета цього потоку позначається як $L_p(i)$ і подається в байтах. Щоб перевести цей розмір у біти, використовується множник 8, оскільки один байт містить 8 біт. Загальна кількість типів потоків

(наприклад, атмосферні, з змінною інтенсивністю, пікові тощо) позначається як N. Сукупне навантаження, яке створюється всіма потоками разом, позначається як R_{in} і вимірюється у бітах за секунду. Воно обчислюється за формулою:

$$C_{eff} = C_{max} \cdot \eta \tag{3.2}$$

Дана формула описує ефективну пропускну здатність каналу зв'язку. Тут $C_e$ff — це дійсна (ефективна) пропускна здатність, яку можна використати для передачі корисних даних; C_{max} — максимальна теоретично можлива пропускна здатність каналу; η — коефіцієнт ефективності передачі, який враховує витрати на службову інформацію, повторні передачі, затримки тощо. Цей коефіцієнт завжди менший або дорівнює одиниці.

$$C_{eff} \geq R_{in} \cdot (1 + P_a) \tag{3.3}$$

Продемонстрована формула визначає умову, за якої ефективна пропускна здатність каналу є достатньою для забезпечення передавання всіх потоків даних з урахуванням ймовірності повторної передачі. Тут $C_e$ff — ефективна пропускна здатність каналу; R_{in} — загальна швидкість вхідного трафіку; P_a — ймовірність повторної передачі пакетів. Чим вища ця ймовірність, тим більшу пропускну здатність потрібно мати, щоб уникнути перевантаження каналу.

Це дозволяє не тільки передбачати необхідну пропускну здатність для заданого набору сервісів і кількості користувачів, а й оцінити запас ємності на випадок непередбачуваних стрибків трафіку.

У результаті такого моделювання можна визначити кількість одночасно активних пристроїв і сервіси, які мережа зможе забезпечити без втрати продуктивності, спланувати обсяг резервної смуги та розрахувати економічно обґрунтовану конфігурацію обладнання для Wi-Fi 6, 5G чи SD-WAN. Завдяки цим розрахункам адміністратор отримує змогу заздалегідь побачити, де виникне «інцидент», і точно налаштувати параметри QoS, щоб підтримати ключові сервіси зі стабільною затримкою та мінімальними втратами пакетів.

3.3 Забезпечення безпеки та управління трафіком

У сучасному цифровому світі швидкість передачі даних – не самоціль. Справжня цінність мережі полягає в її здатності надійно захищати інформацію, гнучко керувати трафіком та оперативно адаптуватися до нових загроз і пікових навантажень. Якщо просто «прокачати» канал без механізмів контролю, отримаємо блискавичну, але вразливу мережу: за першої ж атаки або раптового сплеску трафіку вона вийде з ладу, розкриє корпоративні секрети або погіршить досвід користувачів.

У стандарті Wi-Fi 6 (IEEE 802.11ax) безпека закладена «в кремній». Шифрування WPA3 забезпечує обмін ключами за схемою SAE без передачі пароля в відкритому вигляді, завдяки чому DNS-спуфінг, підміна точок доступу та атаки «brute-force» просто не проходять. Кожна точка доступу підтримує сегментацію на SSID/VLAN, виділяючи окремі віртуальні мережі для гостей, IoT-пристроїв і внутрішніх користувачів із власними правилами доступу. Вбудовані WIDS/WIPS (системи виявлення та запобігання вторгнень) автоматично фіксують будь-який аномальний трафік, спроби підміни або сканування, негайно повідомляють адміністратора та, за потреби, блокують зловмисників. Центральний контролер веде детальний журнал подій і дає змогу в один клік побачити, хто, коли й звідки підключався.

У 5G (IMT-2020) безпека – невід’ємна частина архітектури. Пристрої аутентифікуються через SIM-карту із 128- або 256-бітним шифруванням, а весь шлях від радіозв’язку до ядра мережі працює у захищеному режимі. Технологія network slicing створює ізольовані «слайси» всередині однієї фізичної мережі: індустріальні контролери з нульовою толерантністю до затримки, медичні пристрої з суворою гарантією цілісності даних або публічний інтернет-доступ – кожен слайс із власними правилами доступу й параметрами QoS. Компоненти PCF та NEF

дозволяють операторам у реальному часі коригувати політики передачі, встановлювати ліміти пропускної здатності, пріоритети або вводити тимчасові обмеження під час піків, перекриваючи підозрілий трафік ще до попадання в критичні сервіси.

Підхід SD-WAN підносить управління трафіком на рівень бізнес-логіки. Централізований оркестратор завантажує політики маршрутизації та безпеки, а філіальні маршрутизатори самі обирають канали – MPLS, IPsec, LTE чи інтернет – для кожного потоку даних. Критично важливі сервіси (CRM-запити, фінансові транзакції, відеоконференції) шифруються та рухаються по найстабільніших каналах, а менш чутливий трафік (оновлення, резервні копії) йде по дешевших інтернет-каналах. End-to-end шифрування, адаптивна маршрутизація за затримкою та втратами та глибока інтеграція з SIEM, IDS/IPS і Next-Gen Firewall забезпечують повну прозорість: хто, коли й звідки передає дані, а також які процеси чи користувачі можуть становити загрозу.



Рисунок 3.2 – Забезпечення безпеки та управління трафіком

В результаті маємо мережу, де швидкість, надійність, прозорість та автоматизація співіснують без компромісів. Wi-Fi 6 закладає локальний фундамент, 5G розширює покриття й інтегрує мобільну безпеку, а SD-WAN централізовано керує трафіком та захистом у десятках філій. Такий «гібридний»

підхід поєднує блискавичну швидкість з залізобетонною безпекою, інтелектом маршрутизації і штучним інтелектом захисту, готовий витримати будь-які навантаження й тримати мережу на крок попереду зловмисників та непередбачуваних стрибків трафіку.

3.4 Перевірка ефективності проєкту на практиці

У реальному впровадженні важливо починати не зі стовідсоткового охоплення всієї організації, а з ретельно спланованого пілотного проєкту. Обирається невелика, але репрезентативна ділянка — наприклад, один поверх офісу або кілька віддалених точок присутності — і на ній одночасно встановлюється обладнання Wi-Fi 6, 5G-модулі та SD-WAN-агенти з попередньо налаштованими політиками безпеки, маршрутизації та якості обслуговування.

Паралельно — ще до старту пілоту — визначаються ключові показники ефективності: середня й пікова пропускна здатність, затримки «північ–південь» і «схід–захід», втрати пакетів, частота збоїв при підключенні, частка помилок аутентифікації, а також розподіл трафіку за категоріями — голосові виклики, відеоконференції, IoT-дані, фонова передача великих файлів тощо. Для максимальної прозорості використовують SNMP-агентський моніторинг, NetFlow/IPFIX-аналітику, RMON-дані, а також системи виявлення загроз IDS/IPS і бездротові WIDS/WIPS, які в реальному часі фіксують аномальні шаблони: сканування портів, підміну DNS, brute-force-атаки або спроби створення фейкових точок доступу.

Всі події централізовано збираються у логовий стек на контролері чи SDN-оркестраторі, де автоматично корелюються за джерелом, часовою міткою, типом інциденту та впливом на сервіси. Додатково — для виявлення складних залежностей — застосовують алгоритми машинного навчання: наприклад, кластеризацію K-Means для групування схожих інцидентів або Isolation Forest для пошуку ізольованих аномалій.

Під час пілотного пробігу, що зазвичай триває 4–6 тижнів, здійснюється збір фідбеку за змішаною методикою: аналітичні метрики доповнюються опитуванням користувачів за шкалами CSAT, NPS та MOS. Уточнюється: чи зберігається чіткість відеозв'язку у Zoom і Teams у години пік, чи немає провалів покриття в переговорних кімнатах або виробничих зонах, як поводяться пристрої при переході між Wi-Fi 6 і 5G, чи коректно працює сегментація в SD-WAN — зокрема, чи йдуть транзакції через зашифровані MPLS/IPsec-тунелі, а оновлення — через дешевші лінії з обмеженим SLA.

Паралельно запускаються автоматизовані сценарії навантаження (JMeter, iPerf3, TeraVM), що дозволяють змоделювати поведінку сотень одночасних користувачів із різним пріоритетом трафіку. Фіксується, наскільки швидко мережа відновлює продуктивність після сплеску активності, і які саме компоненти (QoS, буфери, radio scheduling) створюють «вузькі місця».

У фіналі формується аналітичний звіт із графіками та таблицями, які ілюструють динаміку показників «до» і «після» змін: зниження затримки на 10–30 %, зростання throughput на 20–40 %, зменшення інцидентів безпеки на 50 %, підвищення оцінки CSAT на 2–2,5 бала.

До кожного ідентифікованого обмеження (наприклад, перекриття радіоканалів, агресивне QoS-пріоритетування або нестача для критичних сервісів) додаються адресні рекомендації: оптимізація каналів Wi-Fi, підвищення рівня шифрування, збільшення кількості VLAN або виділення окремого slice з гарантованим SLA для відеозв'язку.

Після впровадження коригувальних заходів проводиться повторне тестування тієї ж пілотної зони. Заново налаштовуються точки доступу, профілі PCF/NEF у 5G-ядрі та політики в SD-WAN. Лише після верифікації змін розгортання масштабується на всю організацію: оптимізується щільність Wi-Fi 6-точок, обираються оператори з найкращим 5G-покриттям, а SD-WAN-агенти масштабуються на філії та віддалені офіси.

Останній етап — експлуатаційне супроводження, яке триває ще 3–6 місяців: проводяться періодичні аудити продуктивності, перевірки безпекових політик,

аналіз трендів трафіку та появи нових загроз. Якщо організація переходить до моделі Zero Trust, паралельно впроваджуються додаткові заходи: шифрування всіх з’єднань між сегментами, багатофакторна аутентифікація та динамічне надання прав доступу за принципом найменших привілеїв (PoLP).



Рисунок 3.4 — Етапи впровадження мережі

Такий підхід гарантує не просто стабільну роботу — а дійсно «живу» мережу: гнучку, самонавчальну та адаптивну до вимог бізнесу і викликів кіберсередовища. Це не просто впровадження — це еволюція мережі у високодоступну, самоконтрольовану та передбачувану систему.

3.5 Інтеграція з існуючою інфраструктурою

Інтеграція бездротової мережі з наявною дротовою інфраструктурою починається з продуманого маркування та сегментації трафіку, коли кожен бездротовий SSID отримує власний віртуальний канал завдяки IEEE 802.1Q-тегуванню. Таке рішення дозволяє ізолювати корпоративний трафік від службового або гостьового, зменшити ризик витоку даних і забезпечити чітке

розмежування прав доступу без зайвих витрат на виділені фізичні лінії. Одночасно централізація управління через CAPWAP чи LWAPP дає змогу оновлювати конфігурацію точок доступу миттєво й уніфіковано, що суттєво спрощує масштабування мережі та знижує ймовірність помилок під час внесення змін.

Сучасні платформи для управління мережею, такі як Cisco DNA Center, Aruba AirWave або Juniper Mist, вже давно стали стандартом де-факто. Вони об’єднують у собі автоматичне виявлення нових пристроїв через SNMP чи REST-API, зручні панелі для моніторингу продуктивності в реальному часі та єдину консоль для оновлення ПЗ. При цьому підключення до RADIUS-серверів із сертифікатами X.509 та протоколом IEEE 802.1X гарантує, що в мережу потраплять лише авторизовані користувачі й пристрої, а адміністратор матиме змогу відстежувати всі події входу та виходу без необхідності вручну редагувати списки допуску.

Питання IP-адресації вирішується через поєднання статичних пулів для критично важливих серверів і динамічного розподілу адрес із DHCP relay, що забезпечує безперебійну роботу внутрішніх сервісів і дозволяє уникнути колізій у великих інтегрованих середовищах. Одночасно продумана маршрутизація та міжзонова сегментація за допомогою фаєрволів дають змогу мінімізувати потенційні загрози, адже кожен сегмент отримує власний рівень довіри й чіткі правила взаємодії з іншими зонами.

Нарешті, пілотне тестування є обов’язковим етапом: лише на обмеженій ділянці мережі можна перевірити коректність передачі даних до внутрішніх ресурсів, якість handover між контролерами та ефективність налаштованих політик QoS. Завдяки цьому підходу ризики суттєво знижуються, оскільки проблемні моменти виявляються на ранніх стадіях, а остаточне розгортання відбувається плавно, без простоїв та негативного впливу на кінцевих користувачів.

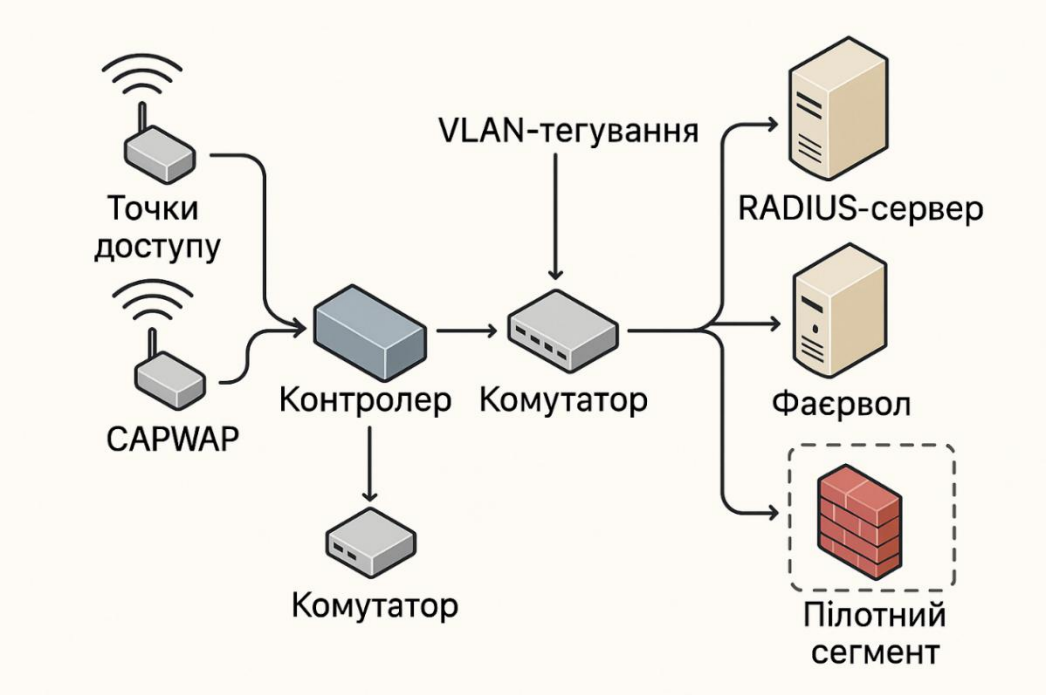


Рисунок 3.3 – Забезпечення безпеки та управління трафіком

На рисунку показано стандартний процес інтеграції бездротової мережі: точки доступу встановлюють захищений тунель CAPWAP до контролера, який централізовано керує їхніми конфігураціями та передає трафік із VLAN-тегуванням далі на комутатор. Одночасно контролер звертається до RADIUS-сервера для автентифікації користувачів і до DHCP-relay для видачі IP-адрес, а комутатор із фаєрволом реалізує міжзонну сегментацію та політики безпеки. Виділений «пілотний сегмент» слугує тестовим майданчиком, щоб перевірити всі налаштування перед повномасштабним розгортанням.

ВИСНОВКИ

У кваліфікаційній роботі проведено всебічне дослідження безпровідних мереж високої пропускної здатності. Оцінено сучасний рівень розвитку та практичні можливості впровадження новітніх стандартів і технологій.

Основні результати роботи є такими:

– проведено детальний аналіз ключових компонентів безпровідних мереж — фізичного й канального рівнів OSI. Обґрунтовано принципи роботи та взаємодії радіочастотних технологій;

– досліджено інфраструктуру високошвидкісних мереж: класифіковано топології, обладнання та програмно-визначені рішення (SD-WAN, NFV);

– охарактеризовано й порівняно основні стандарти Wi-Fi 6/6E та 5G NR за показниками пропускної здатності, затримки, щільності підключень;

– проаналізовано механізми підвищення ефективності (MU-MIMO, OFDMA, beamforming) та засоби оптимізації (динамічний вибір каналів, QoS-пріоритезація);

– розглянуто сценарії практичного застосування: від забезпечення гігабітного Wi-Fi у кампусах до критично важливих мереж у промисловості;

– виконано моделювання радіопокриття й навантаження на прикладі корпоративної мережі, підтверджено доцільність гетерогенних HetNet-архітектур.

Розвиток високопропускних безпровідних мереж сьогодні відбувається у синергії апаратних інновацій і передових алгоритмів керування ефіром. Контрольовані та неконтрольовані методи оптимізації, зокрема машинне навчання для динамічного балансування трафіку, дедалі глибше інтегруються в практику проєктування мереж. Масштаби застосування цих підходів безмежні: від «розумних» міст до автоматизованого виробництва й телемедицини.

Наявні результати демонструють, що грамотне поєднання стандартів Wi-Fi 6/6E, 5G та технологій SD-WAN здатне забезпечити прогнозовану якість сервісу, гнучкість і безпеку. Подальша інтеграція штучного інтелекту для самонавчальних

MSON-мереж дозволить мережам самостійно адаптуватися до мінливих умов експлуатації без втручання оператора.

Отже, високопропускні безпровідні мережі — це не лише інструмент для передачі даних, а фундаментальна платформа майбутніх цифрових екосистем. Їхнє правильно спроєктоване та поетапно впроваджене рішення відкриває нові горизонти мобільності, ефективності та безпеки, що є запорукою конкурентоспроможності організацій у світі, де обсяги даних і вимоги до надійності зв’язку стрімко зростають

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сидоренко В. О. Класифікація безпровідних інтерфейсів // Наукові праці студентів Вінницького національного технічного університету: матеріали XLIX наук.-техн. конф. комп'ютерних систем і автоматики (м. Вінниця, 2020 р.). — Вінниця: ВНТУ, 2020. — С. 2–3. — [Електронний ресурс]. — Режим доступу:— https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2020/paper/view/9007

2. Бабчук С. М. Класифікація безпровідних спеціалізованих комп'ютерних мереж для систем моніторингу місцезнаходження об'єктів // Методи та прилади контролю якості. — 2019. — № 1 (42). — С. 4-6. — [Електронний ресурс]. — Режим доступу: http://elar.nung.edu.ua/handle/123456789/7416

3. Wireless Network [Електронний ресурс] // Fortinet. — Режим доступу: https://www.fortinet.com/resources/cyberglossary/wireless-network

4. Morillas L. Wireless Sensor Networks and Their Applications in Energy Efficiency [Електронний ресурс] / Llorenç Morillas. — Universitat Politècnica de Catalunya, 2017. — С. 12–15. — Режим доступу: https://upcommons.upc.edu/handle/2117/110811

5. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications [Електронний ресурс] / Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. — IEEE Communications Surveys & Tutorials. — 2015. — Vol. 17, No. 4. — С. 2347–2376. — Режим доступу:%20https:/ieeexplore.ieee.org/document/7123563

6. Singh S., Kapoor D. A survey on Internet of Things (IoT): Security, privacy, and other research challenges [Електронний ресурс] / S. Singh, D. Kapoor. — arXiv, 2020. — 13 с. — Режим доступу: https://arxiv.org/abs/2002.12646

7. Alnemran T., Qabazard M. Wireless Networks: Types, Implementations, and Applications // International Journal of Engineering Research and Applications. 2020. — Vol. 10, Issue 01 (Series -III). P. 23–27. — ISSN 2248-9622. [Електронний ресурс]. — Режим доступу:

8. Довженко Н. М., Григор'єв Д. В. Методи підвищення пропускної здатності бездротових мереж // Захист інформації. 2019. № 2(76). С. 14–21. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2034

9. D. A. G. Vieira, J. C. M. de Souza, L. Z. Granville. Techniques for improving the performance of wireless networks: A survey // Computer Networks. 2017. Vol. 112. P. 32–52. DOI: https://doi.org/10.1016/j.comnet.2016.11.001. IEEE Xplore: https://ieeexplore.ieee.org/document/7967048

10. El-Hajj M. Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions // Network. 2025. Vol. 5, No. 1. P. 1–45. DOI: https://doi.org/10.3390/network5010001

11. Keenetic. Способи збільшення швидкості з'єднання, пропускної здатності і стабільності бездротової мережі Wi-Fi. URL: https://help.keenetic.com/hc/uk/articles/213968749

12. Cisco. What is Wi-Fi 6? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en_sg/products/wireless/what-is-wi-fi-6.html

13. Tektronix. Wi-Fi Overview: 802.11 Physical Layer and Transmitter Measurements [Електронний ресурс]. – Режим доступу: https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements

14. Dordal, P. L. An Introduction to Computer Networks. 2nd ed. [Електронний ресурс]. – Open Textbook Library, 2017. — С. 98–125 – Режим доступу: https://open.umn.edu/opentextbooks/textbooks/353

15. Bonaventure, O. Computer Networking: Principles, Protocols and Practice. [Електронний ресурс]. – Open Textbook Library, 2011. — С. 19–22 – Режим доступу: https://open.umn.edu/opentextbooks/textbooks/352

16. IEEE Std 802.11-2020 «Інтерфейс середовища радіодоступу локальних бездротових мереж (Wi-Fi)»: стандарт [Електронний ресурс] / IEEE. — Режим доступу: https://standards.ieee.org/standard/802_11-2020.html

17. Keenetic. Базові положення стандарту IEEE 802.11ac для мереж Wi-Fi [Електронний ресурс]. — Режим доступу: https://help.keenetic.com/hc/uk/articles/213968949-Базові-положення-стандарту-IEEE-802-11ac-для-мереж-Wi-Fi

18. Cisco Systems. Cisco Wireless LAN Controller Configuration Guide, Release 8.10 [Електронний ресурс]. — Режим доступу: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_aps.html

19. Badman L. Wi-Fi AP placement best practices and security policies [Електронний ресурс] / Lee Badman. — TechTarget, 2023. — Режим доступу: https://www.techtarget.com/searchsecurity/feature/Wireless-AP-placement-basics

20. Mareco D. Wireless Access Point Placement: 3 Common Mistakes [Електронний ресурс] / Danny Mareco. — TechGrid, 2020. — Режим доступу: https://techgrid.com/blog/access-point-placement-mistakes

21. IEEE. IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications 802.11ax™-2021 [Електронний ресурс] / IEEE. — Нью-Йорк : IEEE, 2021. — Режим доступу: https://standards.ieee.org/standard/802_11ax-2021.html

22. Cisco Catalyst SD-WAN Solution Overview [Електронний ресурс] / Cisco Systems, Inc. — Сан-Хосе : Cisco, 2022. — Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html

23. International Telecommunication Union. IMT-2020: 5G Vision and Requirements [Електронний ресурс] / ITU. — Женева : ITU, 2020. — Режим доступу: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

24. IEEE 802.11ax: The Sixth Generation of Wi-Fi [Електронний ресурс] / Cisco Systems, Inc. — Сан-Хосе : Cisco, 2021. — Режим доступу:

25. Lin X. та ін. 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology [Електронний ресурс] / X. Lin, J. Li, R. Baldemair та ін. — arXiv, 2018. — Режим доступу:%20https:/arxiv.org/abs/1806.06898 (дата звернення: 16.05.2025)

26. Wi-Fi Alliance. Wi-Fi CERTIFIED WPA3™ Technology Overview : technical specification [Електронний ресурс]. — Austin : Wi-Fi Alliance, 2021. — 12 с. — Режим доступу: https://www.wi-fi.org/file/wi-fi-certified-wpa3-technology-overview-2021

27. McWade S., Flanagan M. F., Zhang L., Farhang A. Interference and Rate Analysis of Multinumerology NOMA : доповідь з міжнародної конференції [Електронний ресурс] / S. McWade, M. F. Flanagan, L. Zhang, A. Farhang. — Dublin : IEEE, 2020. — С. 1–6. — Режим доступу: https://ieeexplore.ieee.org/document/9149041

28. Arista Networks. Integrating Wired and Wireless Enterprise Networks [Електронний ресурс] / Arista Networks. — Santa Clara, CA : Arista, 2019. — С. 3–12. — Режим доступу: https://www.arista.com/en/company/news/press-release/21271-pr-20250312 https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.html

29. Gast M. 802.11 Wireless Networks: The Definitive Guide [Електронний ресурс] / M. Gast. — Sebastopol : O'Reilly Media, 2005. — С. 130–145. — Режим доступу: https://learning.oreilly.com/library/view/802-11-wireless-networks/0596100523/

30. Благовісний Д. В., Зуб О. В. Забезпечення безпеки у бездротових мережах з високою пропускною здатністю. Застосування програмного забезпечення в ІКТ : VI Науково-техн. конф., м. Київ, 24 трав. 2025 р. Київ, 2025. С. 429–431.URL: https://duikt.edu.ua/uploads/p_2779_56719466.pdf

31. Благовісний Д. В., Зуб О. В. безпровідні мережі високої пропускної здатності в умовах зростання навантаження на хмарні сервіси. Сучасні інтелектуальні інформаційні технології в науці та освіті : V Всеукр. Науково-практ. конф., м. Київ, 15 травня. 2025 р. Київ, 2025. – Подано на друкування.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії



на тему: «Безпровідні мережі високої пропускної здатності»

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ
БАКАЛАВРА

Виконав студент групи КІД-42
Благовісний Дмитро Вікторович

Науковий керівник:
Олександр Зуб

Київ 2025

Мета роботи – Дослідження безпровідних мереж високої пропускної здатності та аналіз сучасних технологій їх реалізації.

Об'єкт дослідження – Безпровідні мережі, орієнтовані на високу пропускну здатність у різних середовищах.

Предмет дослідження – Технології побудови, оптимізації та впровадження безпровідних мереж з акцентом на продуктивність.

Актуальність обраної теми

У сучасному світі бездротові мережі стали критично важливою складовою цифрової інфраструктури. Щодня зростає кількість пристроїв, що вимагають швидкого та стабільного підключення — від смартфонів і ноутбуків до сенсорів Інтернету речей. Водночас обсяги трафіку стрімко зростають через відеозв'язок, потокове мовлення та хмарні сервіси.
У цих умовах класичні рішення вже не забезпечують належної продуктивності, тому виникає потреба у впровадженні сучасних технологій: Wi-Fi 6/6E/7, 5G, SD-WAN. Вони дозволяють суттєво підвищити ефективність, енергоощадність та надійність бездротової інфраструктури як у побуті, так і в корпоративному середовищі.

Класифікація безпровідних мереж



Рисунок 1.1 – Класифікація безпровідних мереж

Тип мережі	Абревіатура	Радіус дії	Приклад
Персональна мережа	WPAN	до 10 м	Bluetooth, ZigBee
Локальна мережа	WLAN	до 100 м	Wi-Fi (802.11n/ac/ax)
Міська мережа	WMAN	до кількох км	WiMAX (802.16)
Глобальна мережа	WWAN	десятки та сотні км	LTE, 5G, супутниковий зв'язок

Таблиця 1.1.1 – Класифікація безпровідних мереж за масштабом покриття

Ознака класифікації	Варіанти
Радіус дії	WPAN, WLAN, WMAN, WWAN
Технологія	Wi-Fi, Bluetooth, LTE, LoRa, ZigBee, NB-IoT
Топологія	Ad-hoc, Mesh, Star, Tree
Призначення	Споживчі, Промислові, IoT, Військові
Частотний діапазон	2.4 ГГц, 5 ГГц, 900 МГц, ліцензовані діапазони.

Таблиця 1.1.4 – Узагальнена класифікація безпровідних мереж за основними ознаками

Основні стандарти Wi-Fi, LTE, 5G

Характеристика	Wi-Fi 6 (802.11ax)	LTE / LTE-Advanced	5G (NR – New Radio)
Частотний діапазон	2.4 / 5 GHz	< 6 GHz	<6 GHz (Sub-6) та >24 GHz (mmWave)
Пропускна здатність	До 9.6 Гбіт/с	До 1 Гбіт/с	До 10 Гбіт/с і більше
Затримка	~20-30 мс	~10 мс	<1 мс
Масштабування	Для локального покриття	Широкомасштабне	Масове підключення (IoT, URLLC, eMBB)
Мобільність	Обмежена	Висока	Дуже висока
Архітектура	Децентралізована (локальна)	Централізована	Хмарна, віртуалізована
Сфери застосування	Домашні, офісні, кампуси	Мобільний зв'язок	Вся цифрова інфраструктура

Таблиця 1.2 – Порівняльна характеристика стандартів Wi-Fi 6, LTE та 5G

Технології підвищення пропускної здатності мереж

- Зростання пристроїв і трафіку
- Оптимізація на старті:
- Периферійна агрегація й стиснення:
- Wi-Fi 5/6 (802.11ac/ax): OFDMA, MU-MIMO, Target Wake Time
- Просунуті техніки:
- AI-підхід (SON):

Інфраструктура бездротового зв’язку



Рисунок 2.1 – Структура інфраструктури бездротового зв’язку

Компоненти та топологія інфраструктури бездротового доступу



Рисунок 2.3 – Архітектура бездротової мережі

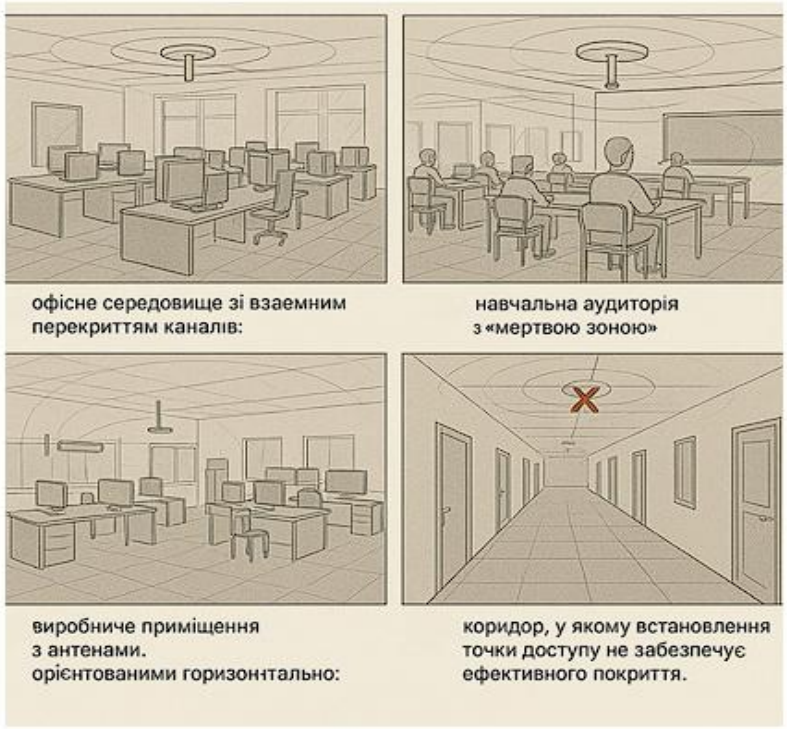


Рисунок 2.4 — Приклади невдалого розміщення точок доступу у типових приміщеннях

Безпека й енергоефективність у сучасних бездротових мережах

- **Безпека**
- Радіопланування
- 802.1X + VLAN
- WPA3-SAE + IPsec/TLS 1.3
- WIDS/WIPS 24/7 + SIEM
- **Енергоефективність**
- Балансування навантаження AP
- TWT, OFDMA, MU-MIMO (IoT)
- Зниження потужності вночі + BMS
- Відновлювана енергія,
- оптимізація трафіку + довший час роботи

Проєктування та аналіз бездротової мережі



Рисунок 3.1 — Основні аспекти проєктування бездротової мережі

Вибір стандарту та мережевих технологій

У роботі використано три ключові технології:

- *Wi-Fi 6 (IEEE 802.11ax)*
- *5G (IMT-2020)*
- *SD-WAN*

Характеристика	Wi-Fi 6 (IEEE 802.11ax)	5G / IMT-2020	SD-WAN
Пропускна здатність	до 9,6 Гбіт/с	до 20 Гбіт/с	залежить від обраного каналу
Радіус дії	до 100 м (локально)	до кількох км	не залежить від радіуса (WAN-транспорт)
Затримка	≈ 10 мс	< 1 мс	оптимізується програмно, залежить від WAN
Орієнтація	внутрішні мережі, кампуси	мобільність, широка зона	централізоване керування розподіленою мережею
Ідеальний сценарій	офіси, Wi-Fi IoT, навчальні заклади	Smart City, транспорт	корпоративна WAN-інфраструктура

Таблиця 3.1 – Порівняння ключових характеристик технологій Wi-Fi 6 (IEEE 802.11ax), 5G (IMT-2020) та SD-WAN

Забезпечення безпеки та управління трафіком



Рисунок 3.2 – Забезпечення безпеки та управління трафіком

Перевірка ефективності проєкту на практиці

- ***Зона тесту:*** репрезентативна ділянка
- ***KPI:*** пропускна здатність
- ***Моніторинг:*** SNMP / IDS
- ***Кореляція:*** централізована подій
- ***ML-аналітика:*** кластеризація, IsolationForest
- ***Фідбек:*** CSAT/NPS
- ***Стрес-тест:*** JMeter
- ***Результати:*** ± продуктивність
- ***Рекомендації:*** оптимізація RF
- ***Верифікація:*** повторне тестування
- ***Масштаб:*** організація
- ***Супровід:*** аудити



Рисунок 3.4 — Етапи впровадження мережі

Інтеграція з існуючою інфраструктурою

- VLAN 802.1Q
- CAPWAP/LWAPP
- DNA Center / AirWave / Mist
- RADIUS + 802.1X
- IP
- Маршрутизація
- Пілот

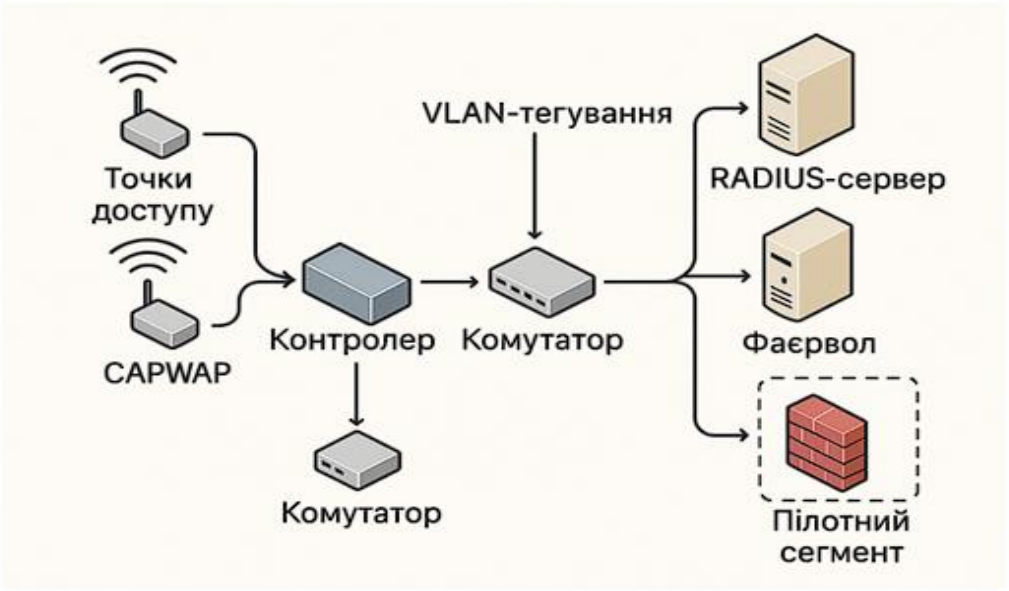


Рисунок 3.3 – Забезпечення безпеки та управління трафіком

ВИСНОВКИ

1. Проведено аналіз ключових компонентів фізичного й канального рівнів безпровідних мереж, обґрунтовано взаємодію радіотехнологій.
2. Досліджено інфраструктуру високошвидкісних мереж: класифіковано топології, обладнання та програмно-визначені рішення (SD-WAN, NFV).
3. Охарактеризовано й порівняно стандарти Wi-Fi 6/6E та 5G NR за пропускною здатністю, затримками й щільністю підключень.
4. Проаналізовано механізми підвищення ефективності (MU-MIMO, OFDMA, beamforming) і методи оптимізації (динамічний вибір каналів, QoS-пріоритезація).
5. Розглянуто практичні сценарії: від гігабітного Wi-Fi в кампусах до критично важливих промислових мереж із гетерогенними HetNet-архітектурами.
6. Виконано моделювання радіопокриття й навантаження корпоративної мережі, підтверджено доцільність поєднання Wi-Fi 6/6E, 5G та SD-WAN для прогнозованої якості, гнучкості й безпеки з подальшим впровадженням SON-мереж на базі ШІ.

Перелік публікацій

Благовісний Д. В., Зуб О. В. Забезпечення безпеки у бездротових мережах з високою пропускною здатністю. Застосування програмного забезпечення в ІКТ : VI Науково-техн. конф., м. Київ, 24 трав. 2025 р. Київ, 2025. С. 429–431.

URL: https://duikt.edu.ua/uploads/p_2779_56719466.pdf

Благовісний Д. В., Зуб О. В. безпровідні мережі високої пропускної здатності в умовах зростання навантаження на хмарні сервіси. Сучасні інтелектуальні інформаційні технології в науці та освіті : V Всеукр. Науково-практ. конф., м. Київ, 15 травня. 2025 р. Київ, 2025. – Подано на друкування.