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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «КОРПОРАТИВНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА З ВИКОРИСТАННЯМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(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

_____ *Данііл СЛІПЧЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-42
Данііл СЛІПЧЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Ірина КУЗЬМІЧ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

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

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Бакалавр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ
«_____» _____ 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Сліпченко Даніїл Олександрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Корпоративна обчислювальна мережа з використанням бездротового зв'язку
керівник кваліфікаційної роботи Ірина КУЗЬМІЧ,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» 02 2026р. № 51
2. Строк подання кваліфікаційної роботи «08» 05 2026р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, методи системного аналізу, мережеві протоколи передачі даних, математичний апарат, емпіричні методи
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Бездротові мережі wi-fi: технологічні основи та еволюція стандартів
2. Практичні аспекти проектування та впровадження бездротової корпоративної мережі на основі технології wi-fi
3. Сучасні методи та технології захисту бездротових мереж wi-fi
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «09» 02 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02-24.03.2026	Виконано
2	Обробка матеріалу	23.03-05.04.2026	Виконано
3	Розробка теоретичної частини	06.04-10.04.2026	Виконано
4	Розробка практичної частини	11.04-20.04.2026	Виконано
5	Висновки за результатами аналізу	21.04-06.05.2026	Виконано
6	Оформлення пояснювальної записки	07.05-08.05.2026	Виконано
7	Розробка презентації	09.05-11.05.2026	Виконано
8	Передзахист	27.05-29.05.2026	Виконано
9	Здача в деканат	02.06-05.06.2026	Виконано

Здобувач вищої освіти _____ Даніїл СЛІПЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ірина КУЗЬМІЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 60 стор., 13 рис., 20 джерел.

Мета дослідження – розробка та практична реалізація сучасної корпоративної бездротової мережі для підприємства.

Об'єкт дослідження – корпоративна бездротова комп'ютерна мережа підприємства.

Предмет дослідження – технології, стандарти Wi-Fi, апаратне забезпечення та методи захисту інформації в корпоративних бездротових мережах.

Короткий зміст роботи: Сьогодні технологія Wi-Fi є фактичним стандартом де-факто для організації бездротових локальних мереж. Головна перевага цієї технології полягає у повній відмові від складного та дорогого прокладання кабельних трас, що робить її ідеальним вибором для розгортання корпоративних інфраструктур. Під час дослідження було проаналізовано еволюцію стандартів від 802.11b до сучасних Wi-Fi 6 та Wi-Fi 7, які забезпечують гігабітні швидкості. На основі аналізу розроблено проект бездротової мережі для підприємства «SoftSuper», що враховує просторове планування та специфіку бізнес-процесів різних відділів на двох поверхах будівлі. Для реалізації проєкту підібрано сучасне обладнання: маршрутизатори стандарту Wi-Fi 6 (TP-Link Archer AX73), 24-портові гігабітні комутатори та потужний сервер баз даних Dell PowerEdge T550. Особливу увагу приділено питанням безпеки: замість застарілих протоколів впроваджено сучасні криптографічні стандарти WPA3-Personal та WPA3-Enterprise для різних сегментів мережі.

КЛЮЧОВІ СЛОВА: WI-FI, КОРПОРАТИВНА МЕРЕЖА, БЕЗДРОТОВИЙ ЗВ'ЯЗОК, WPA3, IEEE 802.11, МАРШРУТИЗАТОР, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Textual part of the qualification work for the bachelor's degree: 60 pages, 13 figures, 20 sources.

Objective of the work – Development and practical implementation of a modern corporate wireless network for the "SoftSuper" enterprise.

Object of research – Corporate wireless computer network of the enterprise.

Subject of research – Technologies, Wi-Fi standards, hardware, and information security methods in corporate wireless networks.

Summary of the work: Today, Wi-Fi technology is the de facto standard for organizing wireless local area networks. The main advantage of this technology is the complete rejection of complex and expensive cable routing, making it an ideal choice for deploying corporate infrastructures. During the research, the evolution of standards from 802.11b to modern Wi-Fi 6 and Wi-Fi 7, which provide gigabit speeds, was analyzed. Based on the analysis, a wireless network project was developed for the "SoftSuper" enterprise, taking into account the spatial layout and specifics of business processes of various departments on two floors of the building. Modern equipment was selected for the project's implementation: Wi-Fi 6 standard routers (TP-Link Archer AX73), 24-port gigabit switches, and a powerful Dell PowerEdge T550 database server. Special attention was paid to security issues: instead of outdated protocols, modern cryptographic standards WPA3-Personal and WPA3-Enterprise were implemented for different network segments.

KEYWORDS: WI-FI, CORPORATE NETWORK, WIRELESS COMMUNICATION, WPA3, IEEE 802.11, ROUTER, INFORMATION SECURITY.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Сліпченко Д. О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)
на тему: «Корпоративна обчислювальна мережа з використанням бездротового зв'язку».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Сліпченко Д. О. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Сліпченка Даніїла Олександровича на оцінку «відмінно», та присвоїти йому кваліфікацію «бакалавр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Ірина КУЗЬМІЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«_» _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Сліпченко Д. О.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Сліпченко Даніїл Олександрович
(прізвище, ім'я, по батькові)
на тему: «Корпоративна обчислювальна мережа з використанням бездротового зв'язку»

Актуальність:

Бакалаврська кваліфікаційна робота присвячена актуальній проблемі розробки, оптимізації та захисту сучасних корпоративних комп'ютерних мереж із використанням бездротових технологій. В умовах стрімкого зростання обсягів корпоративних даних та високих вимог до мобільності персоналу, побудова надійної та захищеної інфраструктури Wi-Fi є пріоритетним завданням для будь-якого підприємства.

Позитивні сторони:

1. У роботі наведено глибокий теоретичний аналіз еволюції стандартів зв'язку сімейства IEEE 802.11, що дозволяє чітко обґрунтувати переваги сучасних поколінь над застарілими специфікаціями в контексті пропускної здатності.
2. Висока практична значущість дослідження: автор розробив детальну топологічну модель корпоративної мережі в середовищі Cisco Packet Tracer та виконав грамотне просторове радіопланування для приміщень компанії «SoftSuper».
3. Автор продемонстрував високу компетентність у питаннях кібербезпеки. У роботі переконливо аргументовано необхідність використання передових криптографічних протоколів WPA3-Enterprise та систем VPN (OpenVPN, WireGuard) для захисту комерційної таємниці компанії.

Недоліки:

1. У розділі, присвяченому вибору апаратного забезпечення, недостатньо уваги приділено розрахунку загальної вартості володіння мережею. Хоча теоретично Wi-Fi є економічно ефективним рішенням , було б доцільно навести порівняльну таблицю бюджету для обраного обладнання.
2. Бажано було б розширити експериментальну частину, додавши практичні симуляції загасання радіосигналу та впливу електромагнітних перешкод від капітальних стін будівлі на швидкість передачі даних.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку " відмінно", а здобувач Сліпченко Д. О. заслуговує присвоєння кваліфікації: бакалавра з комп'ютерної інженерії.*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП.....10
1 БЕЗДРОТОВІ МЕРЕЖІ WI-FI: ТЕХНОЛОГІЧНІ ОСНОВИ ТА ЕВОЛЮЦІЯ СТАНДАРТІВ.....11
1.1 Базові принципи та технологічні особливості функціонування мереж Wi-Fi 11
1.2 Еволюція та класифікація сучасних стандартів бездротового зв'язку сімейства Wi-Fi.....16
1.3 Сильні сторони та вразливості бездротових мереж: аналіз переваг і недоліків технології Wi-Fi.....22
1.4 Забезпечення інформаційної безпеки та сучасні методи захисту даних у бездротових мережах Wi-Fi.....25
2 ПРАКТИЧНІ АСПЕКТИ ПРОЕКТУВАННЯ ТА ВПРОВАДЖЕННЯ БЕЗДРОТОВОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ WI-FI 28
2.1 Загальна характеристика, специфіка діяльності та інформаційна інфраструктура досліджуваного підприємства.....28
2.2 Фізична топологія та апаратне забезпечення робочих просторів підприємства.....33
2.3 Обґрунтування та підбір сучасного апаратного забезпечення для розгортання мережевої інфраструктури.....36
2.4 Програмні комплекси та операційні системи для управління мережевою інфраструктурою.....42
3 СУЧАСНІ МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ WI-FI.....45
3.1 Комплексні підходи та фундаментальні принципи захисту інформації в бездротових системах.....45

3.2 Еволюція та технічні особливості стандартів безпеки: протоколи WPA та WPA2 48
3.3 Технології віртуальних приватних мереж: криптографічні протоколи та принципи шифрування трафіку 53
ВИСНОВКИ 57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 58
Додаток А 60

ВСТУП

Сьогодні технологія Wi-Fi є фактичним стандартом де-факто для організації бездротових локальних мереж у всьому світі. Головна ідея цієї технології полягає в забезпеченні надійного високошвидкісного обміну інформацією між пристроями без використання фізичних кабелів. Глобальне поширення цієї технології революціонізувало спосіб нашого доступу до інформації, дозволивши розгортати масштабні бездротові системи в дослідницьких інститутах, офісах та на підприємствах.

Разом із невпинним удосконаленням обчислювальної техніки розвиваються і стандарти зв'язку: сучасні покоління, такі як Wi-Fi 6 та Wi-Fi 7, здатні забезпечити гігабітні швидкості та ефективно обслуговувати десятки пристроїв одночасно завдяки впровадженню технологій MU-MIMO та OFDMA. Проте розгортання корпоративної мережі є складним процесом, який вимагає грамотного радіопланування для уникнення «мертвих зон» та налаштування надійної архітектури. Незахищені бездротові мережі стають легкою мішенню для несанкціонованого доступу та перехоплення конфіденційної інформації. Саме тому застосування новітніх криптографічних протоколів, таких як WPA3, є критично необхідною умовою для бізнесу.

Метою даної кваліфікаційної роботи є ґрунтовний аналіз технологічних основ бездротового зв'язку та практичне проектування безпечної, масштабованої корпоративної мережі на прикладі IT-підприємства «SoftSuper»...

1 БЕЗДРОТОВІ МЕРЕЖІ WI-FI: ТЕХНОЛОГІЧНІ ОСНОВИ ТА ЕВОЛЮЦІЯ СТАНДАРТІВ

1.1 Базові принципи та технологічні особливості функціонування мереж Wi-Fi

Сьогодні технологія Wi-Fi є фактичним стандартом де-факто для організації бездротових локальних мереж у всьому світі. Хоча цю абревіатуру часто помилково розшифровують як «Wireless Fidelity» (за аналогією з аудіотерміном Hi-Fi, що означає «висока точність»), історично це був просто успішний комерційний бренд, створений консорціумом Wi-Fi Alliance для позначення пристроїв, сумісних зі стандартом IEEE 802.11. Фундамент цієї технології був закладений ще у 1991 році в Нідерландах завдяки спільній роботі корпорацій NCR Corporation та AT&T, які розробили систему WaveLAN для бездротового підключення касових апаратів. Головна ідея полягала в забезпеченні надійного високошвидкісного обміну інформацією між двома або більшою кількістю пристроїв без використання фізичних кабелів. З того часу технологія пройшла величезний шлях еволюції. Якщо раніше вона створювалася переважно для портативних комп'ютерів та перших ноутбуків, то сьогодні Wi-Fi модулі є невід'ємною частиною практично всієї сучасної електроніки: смартфонів, смарт-телевізорів, ігрових консолей, цифрових камер, а також величезного спектра пристроїв «Інтернету речей» (IoT), починаючи від розумних годинників і закінчуючи кліматичною технікою та системами розумного дому. На архітектурному рівні взаємодія в таких мережах може бути реалізована за двома основними сценаріями: інфраструктурний режим (класичне підключення типу «точка доступу — клієнт», що використовується майже всюди) та режим Ad-Hoc (пряме

однорангове з'єднання типу «клієнт — клієнт» для локального обміну даними між пристроями без використання центрального вузла).

За своєю технічною суттю, Wi-Fi — це технологія побудови бездротових локальних мереж (WLAN). Її головна й безперечна перевага полягає у повній відмові від складного та дорогого прокладання кабельних трас, що робить її ідеальним, а часто і єдиним вибором як для створення домашніх мереж, так і для розгортання складних корпоративних інфраструктур. Інтегрований у комп'ютер чи телефон бездротовий мережевий адаптер виконує роль цифро-аналогового перетворювача та трансивера: він отримує цифровий потік даних від процесора, модулює його у високочастотний радіосигнал і через антену випромінює в ефір. Процес прийому відбувається у зворотному порядку, де електромагнітні хвилі вловлюються антеною, демодулюються та перетворюються назад у зрозумілий для операційної системи цифровий код.

Широке впровадження технології Wi-Fi дозволило забезпечити високошвидкісне та стабільне підключення до локальних ресурсів і глобальної мережі Інтернет, повністю усунувши прив'язку користувача до фізичних розеток. На фундаментальному рівні архітектура будь-якої бездротової мережі спирається на три базові елементи: електромагнітні радіосигнали як середовище передачі, антени для випромінювання та вловлювання цих хвиль, а також маршрутизатори (або точки доступу), які виконують роль координаторів мережі [1]. Сучасна бездротова інфраструктура зазвичай будується на базі точок доступу (Access Points), які фізично підключаються до провідної магістральної мережі, слугуючи мостом між оптоволоконним чи кабельним Інтернетом та бездротовими клієнтами. Завдяки впровадженню новітніх технологій, таких як MU-MIMO (багатокористувацький множинний ввід-вивід) та OFDMA, які з'явилися в сучасних стандартах (Wi-Fi 6 та новіших), одна розумна точка доступу здатна одночасно та вкрай ефективно обслуговувати десятки й сотні пристроїв, динамічно розподіляючи пропускну здатність каналу між ними без затримок у чергах, рис. 1.1.

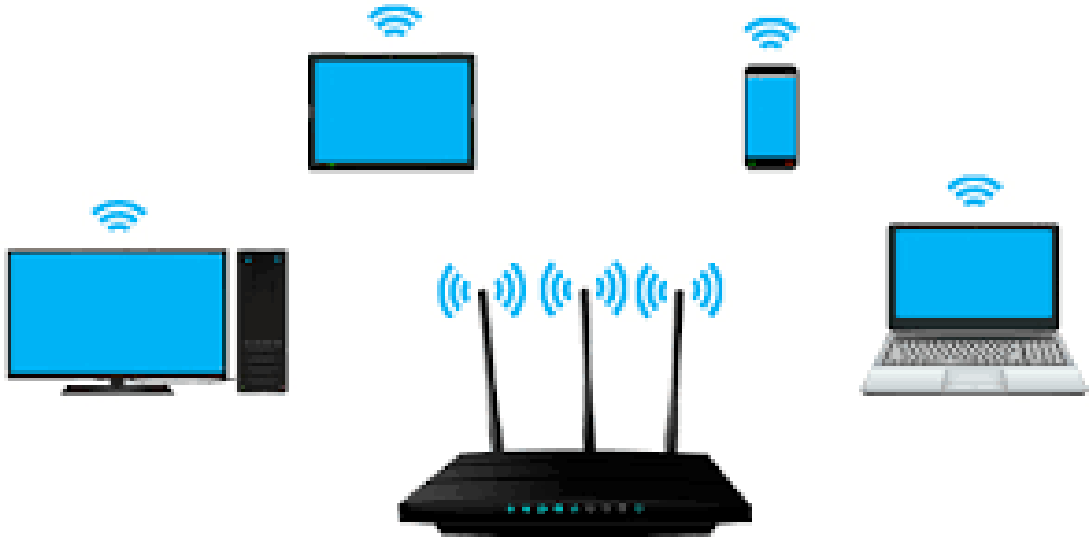


Рисунок 1.1. Базова архітектура та логіка взаємодії компонентів у бездротовій мережі.

Передача даних у такій системі відбувається шляхом розбиття інформації на чітко структуровані цифрові пакети. Ці пакети кодуються, надсилаються в радіоефір у визначеній послідовності, а потім приймаюча сторона дешифрує їх, перевіряє на цілісність та збирає назад у єдиний потік даних. Завдяки цьому складному, але миттєвому процесу користувач бачить на екрані завантажену веб-сторінку або відеоролик без жодних розривів чи спотворень.

Для розгортання повноцінної бездротової мережі необхідний специфічний набір апаратного забезпечення. Ключовою ланкою є точка доступу, або ж бездротовий маршрутизатор (роутер), який безпосередньо підключений до кабелю інтернет-провайдера. З іншого боку знаходиться клієнтський пристрій, який обов'язково має бути оснащений відповідним Wi-Fi радіомодулем, рис. 1.2.

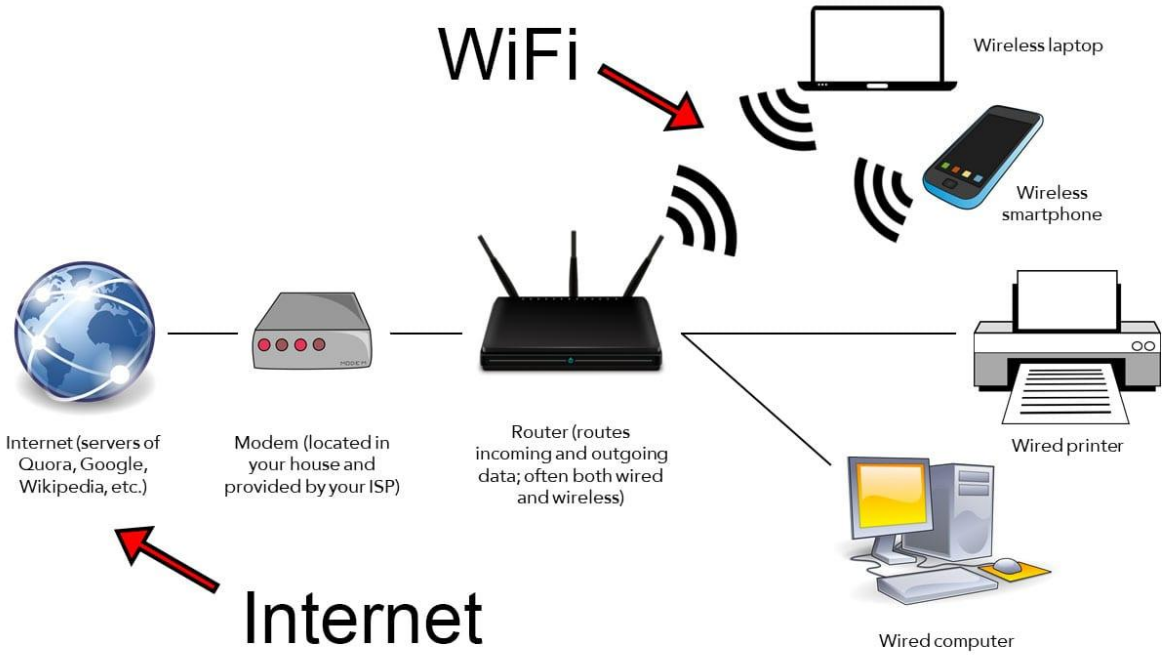


Рисунок 1.2. Структурна схема передачі даних через бездротовий маршрутизатор.

Як маршрутизатор, так і пристрій користувача містять складні мікросхеми (приймачі та передавачі). Варто зазначити, що хоча ці мікрочіпи розробляються різними світовими виробниками та мають відмінну внутрішню архітектуру, сувора стандартизація протоколів сімейства IEEE 802.11 та сертифікація гарантують їхню абсолютну взаємосумісність. Це дозволяє будь-якому смартфону підключитися до будь-якого роутера у світі. Проте слід розуміти: наявність модуля Wi-Fi у гаджеті забезпечує лише зв'язок із маршрутизатором, а для фактичного виходу у світову павутину сам маршрутизатор повинен мати активне підключення до мережі провайдера.

З технічної точки зору, приймачі та передавачі в мережах Wi-Fi працюють за тими ж фізичними принципами, що й портативні радіостанції чи модулі стільникового зв'язку, постійно перетворюючи цифрові сигнали на радіохвилі й навпаки. Їхня принципова відмінність полягає у використанні значно вищих частотних діапазонів. Традиційно це частоти 2,4 ГГц (яка має кращу пробивну здатність крізь перешкоди) та 5 ГГц (яка забезпечує вищу швидкість і менш завантажена). Більше того, у найсучасніших пристроях

стандартів Wi-Fi 6E та Wi-Fi 7 почав активно використовуватися новітній діапазон 6 ГГц. Використання таких надвисоких частот та широких каналів дозволяє передавати колосальні обсяги інформації, забезпечуючи гігабітні швидкості, що критично важливо для потокового відео у форматі 4K/8K, систем віртуальної реальності та хмарного геймінгу

Глобальне поширення цієї технології революціонізувало спосіб нашого доступу до інформації, дозволивши розгортати масштабні бездротові системи в бібліотеках, школах, університетських кампусах, дослідницьких інститутах та просто на вулицях міст. Для бізнес-середовища наявність якісної гостьової мережі стала не просто зручністю, а інструментом для підвищення прибутковості, адже це залучає клієнтів і дозволяє компаніям пропонувати цифрові сервіси безпосередньо на місці. До того ж, підприємства суттєво заощаджують кошти на проектуванні та монтажі десятків кілометрів кабельних мереж у своїх офісах.

Радіосигнали, що випромінюються антенами маршрутизаторів, безперервно скануються антенами клієнтських пристроїв. У стандартних умовах, коли комп'ютер чи смартфон потрапляє в зону впевненого покриття роутера (яка в середньому становить від 45 до 90 метрів на відкритому просторі), відбувається автоматичне узгодження параметрів і пристрій підключається до мережі. Проте реальний радіус дії сигналу та його стабільність сильно залежать від навколишнього середовища: наявності товстих бетонних стін, дзеркал, металевих конструкцій чи навіть радіоперешкод від сусідніх мереж. Мережеві адаптери постійно аналізують якість сигналу: чим ближче пристрій знаходиться до точки доступу, тим складніші алгоритми кодування застосовуються для забезпечення максимальної швидкості. Зі збільшенням відстані обладнання автоматично знижує швидкість передачі заради збереження стабільності з'єднання [1]. Для вирішення проблеми "мертвих зон" у великих приміщеннях сьогодні масово використовуються сучасні Mesh-системи, які створюють єдину безшовну мережу з кількох взаємопов'язаних вузлів.

Сучасний рівень розвитку мікроелектроніки призвів до того, що практично всі нові ноутбуки, планшети та смартфони мають інтегровані в єдиний чип (SoC) багатодіапазонні адаптери Wi-Fi, позбавляючи користувачів необхідності шукати чи купувати додаткові зовнішні карти розширення. Процес підключення став максимально інтуїтивним: якщо мережа є публічною і відкритою, пристрій може підключитися миттєво (іноді з вимогою пройти ідентифікацію через спеціальну веб-сторінку авторизації). У закритих домашніх чи корпоративних мережах, які сьогодні захищені потужними протоколами шифрування на кшталт WPA2 або новітнього WPA3, користувачеві достатньо ввести пароль доступу. Значну частину сучасної міської інфраструктури формують «гарячі точки» (hotspots). Це локальні зони публічного бездротового доступу до Інтернету, які масово розгортаються у громадських місцях: ресторанах, аеропортах, готелях, великих офісах та на вокзалах, дозволяючи людям залишатися на зв'язку та працювати віддалено в будь-якій точці світу.

1.2 Еволюція та класифікація сучасних стандартів бездротового зв'язку сімейства Wi-Fi

Разом із невпинним удосконаленням обчислювальної техніки та стрімким зростанням обсягів цифрового контенту, технології передачі даних також перебувають у стані безперервного розвитку. Для побудови оптимальної та ефективної бездротової мережі, що повною мірою відповідатиме актуальним потребам користувачів, критично важливо розуміти технічну специфіку існуючих стандартів. За роки свого існування консорціум Wi-Fi Alliance розробив та сертифікував понад двадцять різноманітних специфікацій підключення. Якщо на ранніх етапах розвитку індустрії домінували базові стандарти на зразок 802.11b, 802.11a та 802.11g, то сьогодні ринок перейшов

до більш інтуїтивно зрозумілої системи маркування поколінь (таких як Wi-Fi 4, 5, 6 та найновіший Wi-Fi 7), кожне з яких пропонує кардинальне покращення пропускної здатності та стабільності з'єднання. Загальну візуальну діаграму історичного розвитку цих стандартів та їх ключових характеристик наведено на рис. 1.3.

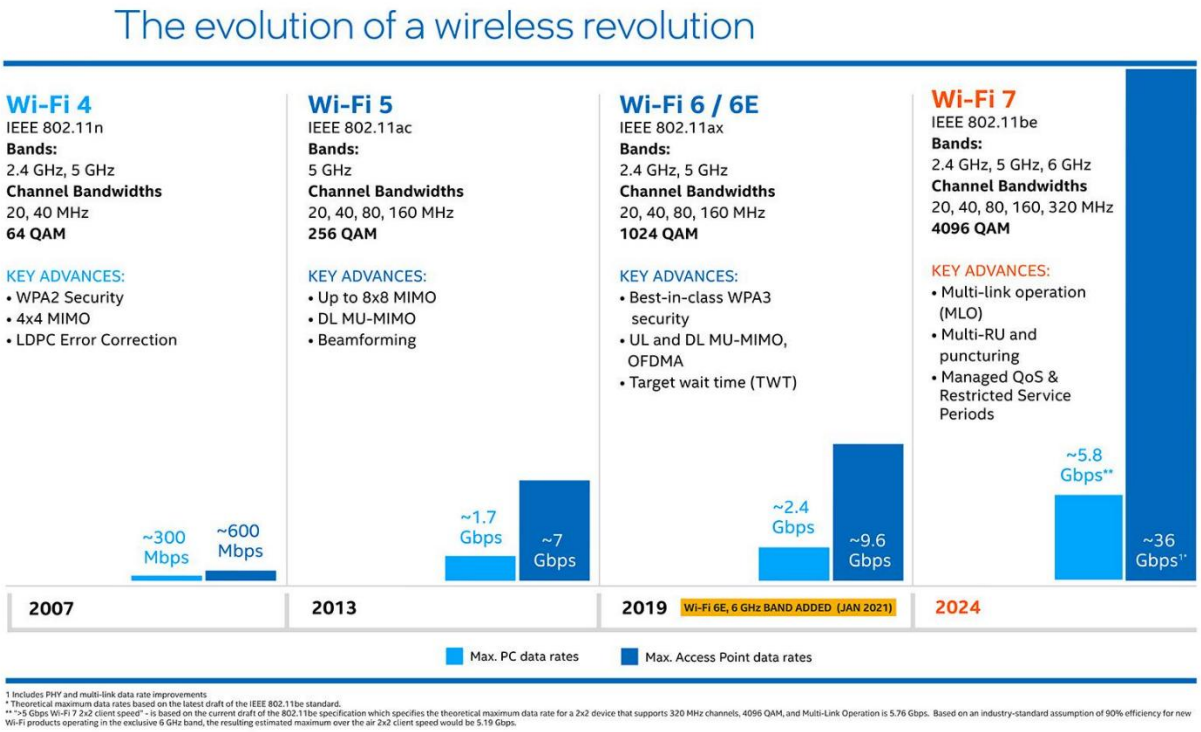


Рисунок 1.3. Хронологічна еволюція та поетапний розвиток базових стандартів технології Wi-Fi.

Одним із перших масових і комерційно успішних стандартів став 802.11b. Незважаючи на свою високу доступність та популярність на початку нульових, сьогодні він вважається глибоко застарілим через вкрай низьку пропускну здатність. Ця технологія функціонувала у базовому радіодіапазоні 2,4 ГГц і забезпечувала максимальну теоретичну швидкість передачі даних лише на рівні 11 Мбіт/с при радіусі дії близько 50 метрів за умови відсутності капітальних перешкод.

Наступним логічним кроком стала розробка стандарту 802.11a, який запропонував суттєве покращення швидкості — до 54 Мбіт/с. Головною інновацією цього покоління став перехід на вільніший діапазон частот 5 ГГц, що дозволило практично повністю уникнути електромагнітних перешкод від інших радіопристроїв. Проте закони фізики зумовили його головний недолік: радіохвилі вищої частоти набагато гірше проникають крізь стіни та перекриття, тому ефективний радіус дії мережі скоротився приблизно до 30 метрів, а вартість самого обладнання залишалася високою порівняно з попередником.

Згодом на ринок вийшла модифікація 802.11g, яка стала своєрідним "золотим компромісом". Вона повернулася до більш «далекобійного» діапазону 2,4 ГГц із радіусом дії до 50 метрів, але при цьому зберегла високу швидкість передачі інформації на рівні 54 Мбіт/с, притаманну стандарту «a». Детальне порівняння контурів зон радіопокриття для цих класичних стандартів проілюстровано на рис. 1.4.

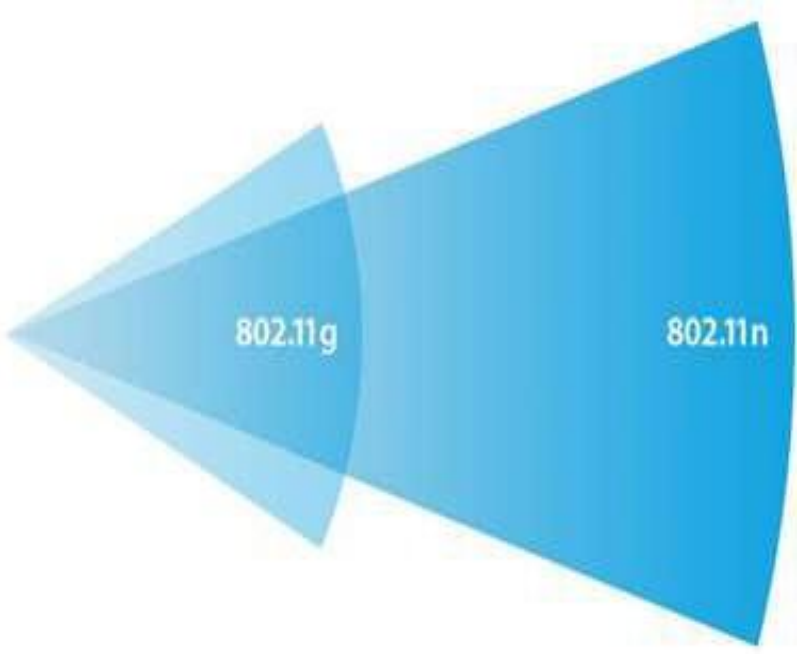


Рисунок 1.4. Схематичне відображення площі покриття сигналу для різних поколінь бездротових мереж.

Додатковою і вкрай важливою перевагою 802.11g стала повна зворотна сумісність зі старим обладнанням 802.11b, що зробило оновлення мережевої інфраструктури плавним та економічно вигідним.

Справжній прорив у швидкості та надійності відбувся з появою стандарту 802.11n, який пізніше отримав більш зрозумілу комерційну назву Wi-Fi 4. Всупереч поширеним міфам про його несумісність, це покоління чудово працювало зі старими стандартами і вперше запровадило підтримку обох діапазонів (2,4 та 5 ГГц). Завдяки впровадженню технології багатоантенного вводу-виводу (MIMO), швидкість передачі даних у ньому теоретично сягала до 600 Мбіт/с, а радіус дії на відкритому просторі збільшився до 100 метрів. Аналітичне зіставлення швидкостей цих поколінь відображено на рис. 1.5.

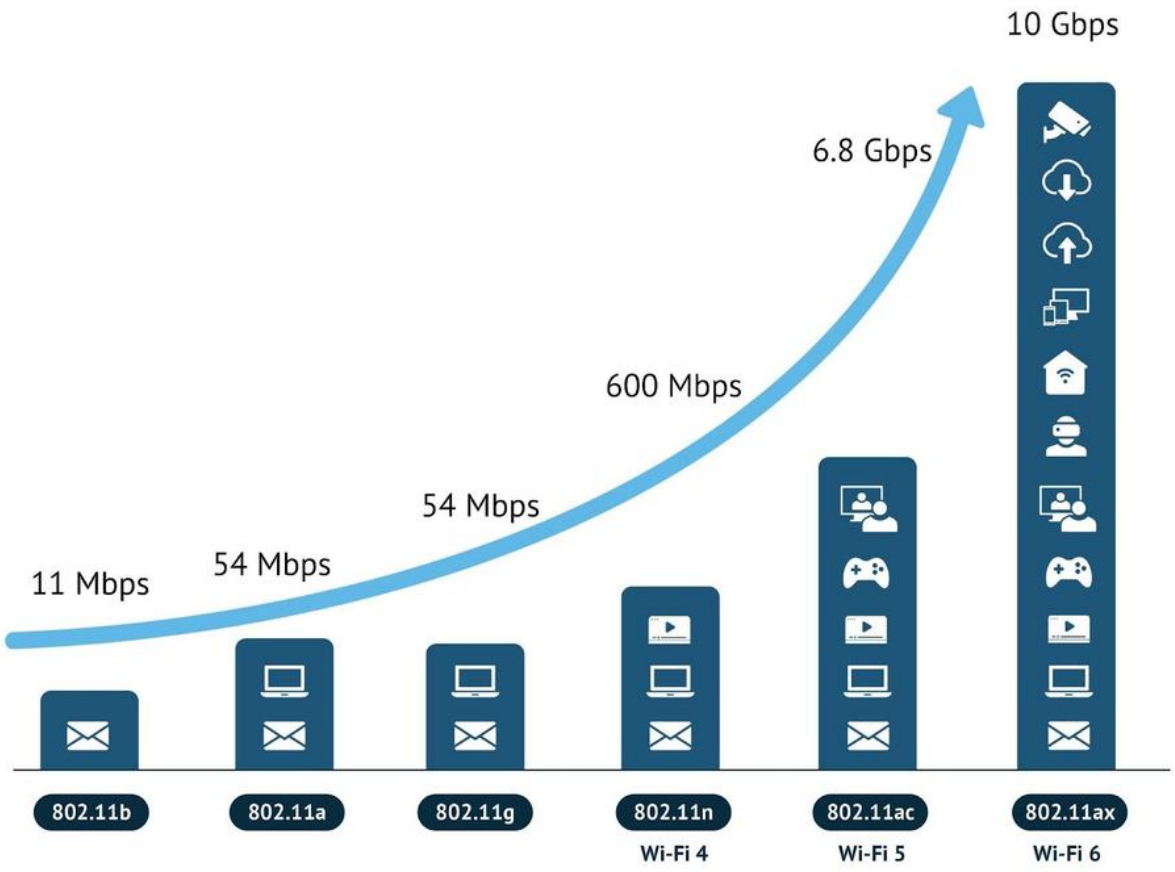


Рисунок 1.5. Аналітичний графік зростання швидкості передачі даних у розрізі різних поколінь мереж.

Ще більш потужним рішенням став стандарт 802.11ac (або Wi-Fi 5), який остаточно вивів якість бездротового доступу до Інтернету на рівень гігабітних швидкостей. Фокусуючись виключно на діапазоні 5 ГГц із використанням розширених каналів (до 160 МГц), він забезпечив величезну ємність, ідеальну для потокового відео у високій якості. Хоча високочастотний сигнал 5 ГГц фізично швидше загасає під час проходження крізь бетонні чи гіпсокартонні стіни, цей недолік був блискуче компенсований інтелектуальними інноваціями. Зокрема, технологія Beamforming дозволила маршрутизатору точно визначати просторове розташування підключеного клієнта і направляти сфокусований радіопромінь безпосередньо на нього. Крім того, саме в 802.11ac була повноцінно реалізована технологія MU-MIMO, яка гарантує безперебійний паралельний обмін даними одразу з кількома пристроями принцип роботи цього механізму показано на рис. 1.6.

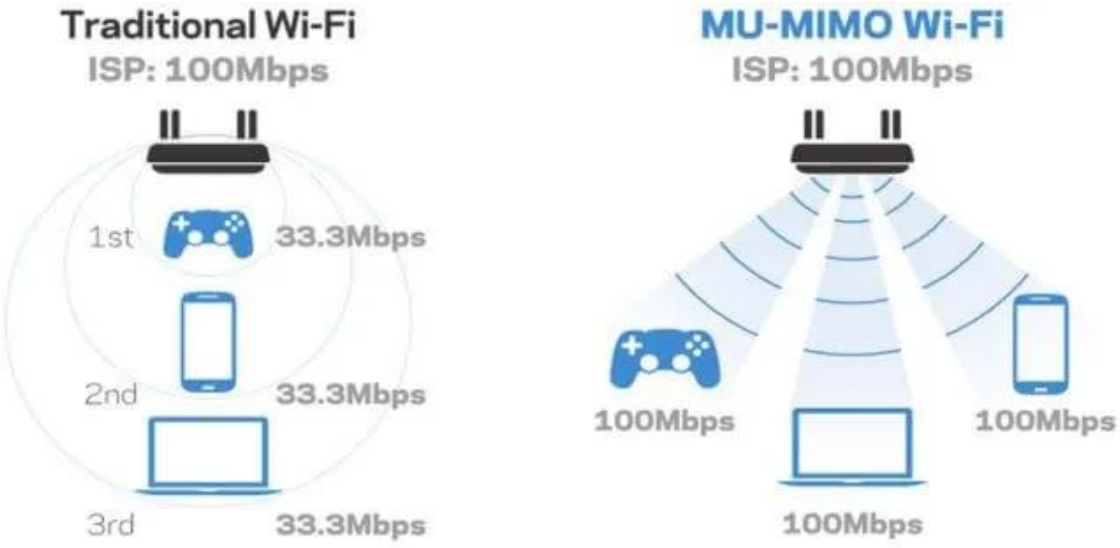


Рисунок. 1.6. Схема паралельної передачі даних клієнтам за допомогою технології MU-MIMO.

Оскільки технології швидко застарівають, сучасним промисловим і домашнім стандартом де-факто став 802.11ax (Wi-Fi 6 та його розширена версія 6E). Завдяки революційному методу модуляції OFDMA цей стандарт дозволяє розбивати радіоканал на дрібні частотні фрагменти та обслуговувати

десятки гаджетів одночасно без найменших затримок. Версія Wi-Fi 6E пішла ще далі, вперше відкривши доступ до абсолютно нового, чистого діапазону 6 ГГц, що повністю вирішило проблему перевантаженості радіоефіру в сучасних мегаполісах. На сьогоднішній день також розпочалося активне впровадження новітнього стандарту 802.11be (Wi-Fi 7), який здатний забезпечити феноменальну пропускну здатність понад 30 Гбіт/с та використовує надширокі канали по 320 МГц, що робить бездротове з'єднання практично таким же швидким і стабільним, як пряме підключення через оптичний кабель.

Окрім глобальних поколінь, консорціум розробив цілий набір вузькоспеціалізованих специфікацій. Наприклад, стандарт 802.11d забезпечує міжнародну сумісність пристроїв, адаптуючи їхні параметри до законодавчих вимог різних країн щодо радіовипромінювання. Доповнення 802.11e відповідає за пріоритезацію трафіку (QoS) для стабільної передачі потокових медіафайлів. Своєю чергою, розширення 802.11i лягло в основу сучасних протоколів шифрування (аж до найновіших версій WPA3), значно підвищивши рівень захисту особистої інформації користувачів.

Окремий вектор розвитку спрямований на обслуговування "Інтернету речей" (IoT). Стандарт 802.11ah (Wi-Fi HaLow) створювався спеціально для пристроїв, яким не потрібна шалена швидкість (до 347 Мбіт/с), але критично важливі великий радіус дії та низьке енергоспоживання [5]. Працюючи на частотах нижче 1 ГГц (близько 900 МГц), сигнал легко долає значні відстані та перешкоди, що робить технологію серйозним конкурентом для Bluetooth у системах розумного дому. На протилежному полюсі знаходиться стандарт 802.11ay, представлений у 2021 році, який оперує на надвисокій частоті 60 ГГц. Він забезпечує пропускну здатність понад 20 Гбіт/с на дуже коротких дистанціях, що є ідеальним для бездротових гарнітур віртуальної реальності та систем швидкісної передачі масивів даних.

Сучасні дослідницькі групи також активно переосмислюють самі можливості радіохвиль. Так, стандарт 802.11az (NGP) розробляється для

забезпечення високоточного позиціонування та навігації гаджетів всередині приміщень зі значно меншими енерговитратами [5]. Ще більш інноваційним є проект 802.11bf (WLAN Sensing), який перетворює мережу на своєрідний радар: він досліджує можливості використання відбиття бездротових сигналів для виявлення присутності людей або тварин, розпізнавання жестів та вимірювання швидкості рухомих об'єктів у кімнаті чи салоні автомобіля.

Паралельно велика увага приділяється захисту цифрової приватності. Стандарт 802.11bh розробляється для вирішення технічних труднощів на стороні маршрутизаторів, що виникають через масове використання смартфонами випадкових (змінних) MAC-адрес для захисту від мережевого стеження [5]. Водночас поправка 802.11bi повністю зосереджена на глибокій модернізації механізмів управління доступом, щоб гарантувати надійний захист інформації про місцезнаходження, пересування та діяльність користувачів від сучасних методів аналітики та профілювання.

1.3 Сильні сторони та вразливості бездротових мереж: аналіз переваг і недоліків технології Wi-Fi

Будь-яка технологія має свій спектр застосування, який визначається балансом її позитивних рис та технічних обмежень. Технологія Wi-Fi не є винятком. Для правильного проектування та експлуатації мереж важливо чітко розуміти як її беззаперечні переваги, так і потенційні вразливості.

Головною і найбільш очевидною перевагою Wi-Fi є безпрецедентна мобільність та доступність. Завдяки повній відмові від фізичних дротів користувачі отримують свободу пересування в межах зони покриття без втрати зв'язку з мережею. Це фундаментально змінило підхід до організації робочого простору, дозволивши співробітникам вільно переміщатися офісом,

залишаючись онлайн, що своєю чергою суттєво підвищує загальну продуктивність та комфорт.

Процес розгортання та масштабування такої інфраструктури відзначається надзвичайною легкістю та швидкістю встановлення. На відміну від традиційних дротових мереж (LAN), які вимагають складного монтажу, штроблення стін та прокладання кілометрів кабелю, бездротова точка доступу встановлюється за лічені хвилини. Це не лише зберігає естетику приміщень, але й усуває фізичні ризики для безпеки, такі як можливість зачепитися за відкриті дроти. Більше того, у разі переїзду або зміни конфігурації офісу, бездротову мережу набагато простіше адаптувати до нових умов шляхом простого програмного переналаштування.

Бездротові мережі забезпечують надзвичайно широке охоплення, дозволяючи доставити інтернет-сигнал у ті місця, де прокладання кабельних трас є фізично неможливим, економічно недоцільним або забороненим (наприклад, в історичних будівлях чи на складних промислових об'єктах). Гнучкість цієї технології стала основою для сучасного формату віддаленої роботи: налаштувавши домашню мережу, користувач може легко виконувати свої професійні обов'язки, підтримувати високу продуктивність та мати безперешкодний доступ до корпоративних даних чи інформації клієнтів з будь-якого куточка власної оселі [3].

З точки зору рентабельності, незважаючи на необхідність початкових інвестицій у закупівлю якісних маршрутизаторів чи точок доступу, у довгостроковій перспективі Wi-Fi є економічно високоефективним рішенням. Відсутність витрат на закупівлю мідного чи оптичного кабелю, оплату монтажних робіт та подальше обслуговування фізичної інфраструктури робить загальну вартість володіння (TCO) такою мережею значно нижчою. Крім того, сучасні стандарти зв'язку забезпечують надзвичайно високу ефективність передачі даних, роблячи обмін інформацією між користувачами миттєвим.

Незважаючи на колосальний крок уперед, радіоефір як середовище передачі даних накладає певні обмеження. Історично найбільшою проблемою бездротових мереж вважається безпека. Оскільки сигнал поширюється у відкритому просторі, для спроби підключення до мережі зловмиснику не потрібен фізичний доступ до комутатора чи кабелю — достатньо просто знаходитися в зоні дії радіосигналу з відповідним адаптером. Якщо мережа налаштована некоректно, використовує застарілі протоколи шифрування або адміністратор залишив паролі за замовчуванням, це створює критичні загрози для конфіденційності даних. Варто зазначити, що сьогодні ця проблема успішно вирішується завдяки впровадженню новітніх криптографічних стандартів (таких як WPA3), проте людський фактор під час налаштування залишається слабкою ланкою.

Ще одним аспектом є пропускна здатність та швидкість. Раніше вважалося, що бездротові мережі не здатні підтримувати вимогливі сервіси на кшталт відеоконференцій (VTC) через мінімальну пропускну здатність. Хоча для старих стандартів це було справедливо, сучасні покоління Wi-Fi 6 та Wi-Fi 7 здатні без проблем передавати потокове відео у форматі 4K та обробляти гігабітні потоки даних. Тим не менш, пропускна здатність радіоканалу все одно залишається розділеним ресурсом. Якщо мережа не захищена, несанкціоновані користувачі можуть "відбирати" частину трафіку. До того ж, незважаючи на весь прогрес, швидкість і стабільність Wi-Fi все ще може поступатися прямому підключенню через оптоволокно, особливо коли йдеться про затримки (пінг) під час пікових навантажень. Швидкість також прямо пропорційна відстані: чим далі пристрій знаходиться від точки доступу, тим слабшим стає сигнал і повільнішим — обмін файлами. Для великих будівель це є серйозним викликом [3].

Фізична природа радіохвиль робить технологію схильною до перешкод. На якість зв'язку впливають численні зовнішні фактори. У приміщеннях це можуть бути товсті бетонні стіни, металеві конструкції або електромагнітне випромінювання від побутових приладів (наприклад, мікрохвильових печей,

які також працюють на частоті 2,4 ГГц). У багатоквартирних будинках чи щільних офісних центрах виникає проблема перевантаженості ефіру, коли десятки сусідніх мереж створюють взаємні перешкоди (інтерференцію). На відкритому просторі на поширення сигналу можуть впливати навіть складні погодні умови, такі як туман, сильні опади чи пилові бурі.

Зона покриття одного стандартного бездротового маршрутизатора зазвичай є обмеженою і в середньому становить від 45 до 90 метрів в умовах прямої видимості. Це породжує певну суперечність у питанні вартості: хоча базове обладнання для дому є дешевим, професійне налаштування корпоративної безшовної мережі здатне вилитися в серйозні витрати. Розширення покриття на великі площі вимагає закупівлі додаткових апаратних контролерів, репітерів або сучасних Mesh-систем.

Насамкінець, для створення дійсно надійної, швидкої та захищеної системи потрібні базові знання комп’ютерних мереж та розуміння принципів радіопланування. Користувачі без відповідного досвіду часто стикаються з проблемами "мертвих зон", конфліктами IP-адрес або залишають мережу відкритою для хакерських атак, що нівелює всі переваги бездротових технологій [3].

1.4 Забезпечення інформаційної безпеки та сучасні методи захисту даних у бездротових мережах Wi-Fi

Фундаментальна особливість технології Wi-Fi полягає у використанні відкритого радіоефіру як середовища для передачі сигналів, що робить питання інформаційної безпеки критично важливим. Забезпечення надійного захисту персональних та корпоративних даних є першочерговим завданням при розгортанні будь-якої бездротової інфраструктури. Незахищені, відкриті або неправильно налаштовані бездротові маршрутизатори стають легкою

мішенню для несанкціонованого доступу. Будь-яка стороння особа, яка знаходиться в радіусі дії сигналу та підключається до вразливого роутера, може не лише безкоштовно використовувати чужий інтернет-трафік, але й здійснити перехоплення конфіденційної інформації, паролів, банківських даних або ж інфікувати локальну мережу шкідливим програмним забезпеченням. Саме тому для гарантування безпеки пристроїв необхідно застосовувати сучасні криптографічні стандарти (наприклад, актуальні протоколи шифрування WPA2 або новітній WPA3), відключати застарілі та вразливі функції на кшталт WPS, а також регулярно оновлювати програмне забезпечення мережевого обладнання.

Основою будь-якої бездротової інфраструктури, як домашньої, так і корпоративної, є бездротовий маршрутизатор (роутер). Це ключовий апаратний пристрій локальної мережі (WLAN), який найчастіше використовується для прийому сигналу від інтернет-провайдера через фізичний кабель (оптичний або виту пару) та його подальшої роздачі "повітрям". Головна технічна функція сучасного маршрутизатора полягає у вдалому комбінуванні можливостей класичного роутера, який керує IP-трафіком і розподіляє адреси, та бездротової точки доступу, що випромінює радіосигнал. Якщо раніше в дротових мережах роль центрального вузла виконували прості концентратори (хаби), до яких фізично підключалися всі комп'ютери, то сьогодні сучасні настільні Wi-Fi маршрутизатори виконують роль інтелектуальних мережевих шлюзів. Вони мають компактні розміри, оснащуються внутрішніми або зовнішніми антенами для стабільного покриття та забезпечують зв'язок у будь-якій точці квартири або невеликого офісу.

Для вирішення проблеми "мертвих зон" та розширення радіуса дії мережі у великих приміщеннях традиційно використовують розширювачі діапазону (репітери). Їх розташовують на межі впевненого прийому сигналу від головного роутера: вони вловлюють цей сигнал і ретранслюють його далі. Проте варто зазначити, що класичні розширювачі сьогодні активно витісняються більш сучасними Mesh-системами, які створюють єдину

безшовну Wi-Fi мережу з кількох рівноправних модулів без втрати швидкості та пропускної здатності.

Окрім стаціонарного обладнання, величезної популярності набули мобільні точки доступу (Mobile Hotspots). Сьогодні кожен сучасний смартфон має вбудовану функцію роздачі Wi-Fi. Коли цю опцію активовано, телефон використовує стільникове підключення оператора (через мережі 4G LTE або 5G) як джерело Інтернету та перетворюється на мініатюрний портативний маршрутизатор. До такої мобільної точки доступу можна без жодних дротів підключити ноутбуки, планшети, розумні годинники чи інші портативні гаджети незалежно від вашого місцезнаходження. Окрім смартфонів, існують також спеціалізовані автономні 4G/5G Wi-Fi роутери з власними акумуляторами. Хоча використання такого способу зв'язку напряму залежить від тарифікації та лімітів вашого мобільного оператора, власна мобільна точка доступу є значно безпечнішою та надійнішою альтернативою, ніж підключення до відкритих та незахищених громадських мереж Wi-Fi у кав'ярнях чи аеропортах.

2 ПРАКТИЧНІ АСПЕКТИ ПРОЕКТУВАННЯ ТА ВПРОВАДЖЕННЯ БЕЗДРОТОВОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ WI-FI

2.1 Загальна характеристика, специфіка діяльності та інформаційна інфраструктура досліджуваного підприємства

У межах даного проекту здійснюється ґрунтовний аналіз та практична реалізація сучасної корпоративної бездротової мережі для підприємства «SoftSuper». Ця компанія позиціонує себе як динамічний гравець на ринку інформаційних технологій, що спеціалізується на наданні широкого спектра послуг: від апаратного обслуговування комп'ютерної техніки до розробки та впровадження комплексних програмних рішень. Фізично офіс підприємства розташований у сучасній двоповерховій будівлі. Просторове планування приміщень безпосередньо впливає на архітектуру майбутньої мережі, оскільки кожен відділ має власні унікальні вимоги до пропускної здатності, стабільності та рівня безпеки з'єднання. На першому поверсі будівлі компактно розміщені технічний відділ, головна серверна кімната, зона по роботі з корпоративними клієнтами, а також кабінет генерального директора.

Технічний відділ є своєрідним "серцем" компанії, адже його фахівці відповідають за розробку, тестування та безперебійну підтримку всіх технологічних продуктів і сервісів. Співробітники цього підрозділу постійно працюють із великими масивами даних, здійснюють розгортання програмного забезпечення (використовуючи сучасні DevOps-практики), займаються оновленням існуючих систем та дистанційним вирішенням складних технічних інцидентів. Для виконання таких завдань їм потрібен максимально швидкісний та безперебійний доступ до локальних і хмарних ресурсів. Поруч розташований відділ роботи з клієнтами, який виконує функцію "першої лінії".

Менеджери цього відділу використовують сучасні CRM-системи, IP-телефонію та платформи для відеоконференцій, щоб надавати вичерпні консультації, презентувати нові IT-продукти та забезпечувати якісну післяпродажну підтримку. Стабільний Wi-Fi із пріоритезацією мультимедійного трафіку (QoS) тут є критично необхідним для підтримки високого рівня сервісу.

Особливою зоною на першому поверсі є серверна кімната, де зосереджено головне комунікаційне обладнання, локальні бази даних та шлюзи до корпоративних хмарних сховищ. З міркувань суворої інформаційної безпеки, фізичний доступ до цього приміщення суворо регламентований і дозволений виключно генеральному директору та профільним системним адміністраторам технічного відділу (зазвичай із використанням систем електронного контролю доступу). У кабінеті керівника також потрібен гарантовано захищений бездротовий канал для безпечної роботи з комерційною таємницею. Візуальне відображення розташування цих робочих зон можна побачити на планах приміщень, рис. 2.1 - 2.2.



Рисунок 2.1. Архітектурне планування та розташування робочих зон першого поверху.



Рисунок 2.2. Схема просторового розміщення підрозділів на другому поверсі будівлі.

Другий поверх повністю відведений під адміністративні та комерційні структури підприємства, де функціонують фінансовий відділ, служба управління персоналом та відділ продажу. Фінансовий відділ здійснює повний цикл економічного контролю: від класичного бухгалтерського обліку та управління податками до складного фінансового моделювання, бюджетування та стратегічного планування. Оскільки тут обробляється найбільш конфіденційна інформація компанії із застосуванням сучасних ERP-систем, мережевий сегмент цього відділу вимагає застосування найвищих стандартів корпоративного шифрування (наприклад, WPA3 Enterprise) та логічної ізоляції від інших підрозділів.

Відділ продажу є найбільш мобільним підрозділом на поверсі. Його співробітники відповідають за розширення клієнтської бази, проведення складних переговорів, укладання контрактів та підтримку довготривалих партнерських відносин. Менеджери з продажу часто переміщуються офісом із ноутбуками та планшетами, проводячи онлайн-презентації. Для них життєво важливою є підтримка технології безшовного роумінгу, щоб сигнал Wi-Fi не переривався під час переходу між різними кабінетами. Не менш важливу роль відіграє відділ управління персоналом (HR), який формує корпоративну культуру та забезпечує підприємство кваліфікованими кадрами. Робота цього

відділу базується на комплексному підході, що включає пошук та рекрутинг талановитих спеціалістів (часто через онлайн-співбесіди), розробку програм адаптації та дистанційного навчання через корпоративні портали, регулярну оцінку ефективності персоналу з розробкою мотиваційних схем, а також моніторинг дотримання сучасного трудового законодавства. Окрім того, HR-спеціалісти виступають медіаторами у вирішенні конфліктних ситуацій та формують сприятливий психологічний клімат, що вимагає постійної комунікації як всередині компанії, так і за її межами.

На момент початку проекту модернізації, існуючий парк комп'ютерної техніки компанії «SoftSuper» складається з базового набору обладнання. У робочому процесі задіяні 13 стаціонарних персональних комп'ютерів (для яких передбачено використання 13 спеціальних бездротових мережевих адаптерів для інтеграції в середовище Wi-Fi), 2 мобільні ноутбуки для керівної ланки, а також центральний сервер для обробки локальних баз даних та управління обліковими записами. Периферійна інфраструктура представлена 4 мережевими принтерами та 2 сканерами документів. Ядро локальної мережі спирається на 2 комутатори для розподілу трафіку та 2 маршрутизатори, які слугуватимуть основою для розгортання нових бездротових точок доступу.

Для створення грамотної, масштабованої та безпечної структурної схеми бездротової мережі було прийнято рішення використати спеціалізоване програмне середовище Cisco Packet Tracer. Наочну топологію майбутньої мережі, розроблену в цій системі, наведено на відповідній ілюстрації, рис. 2.3.

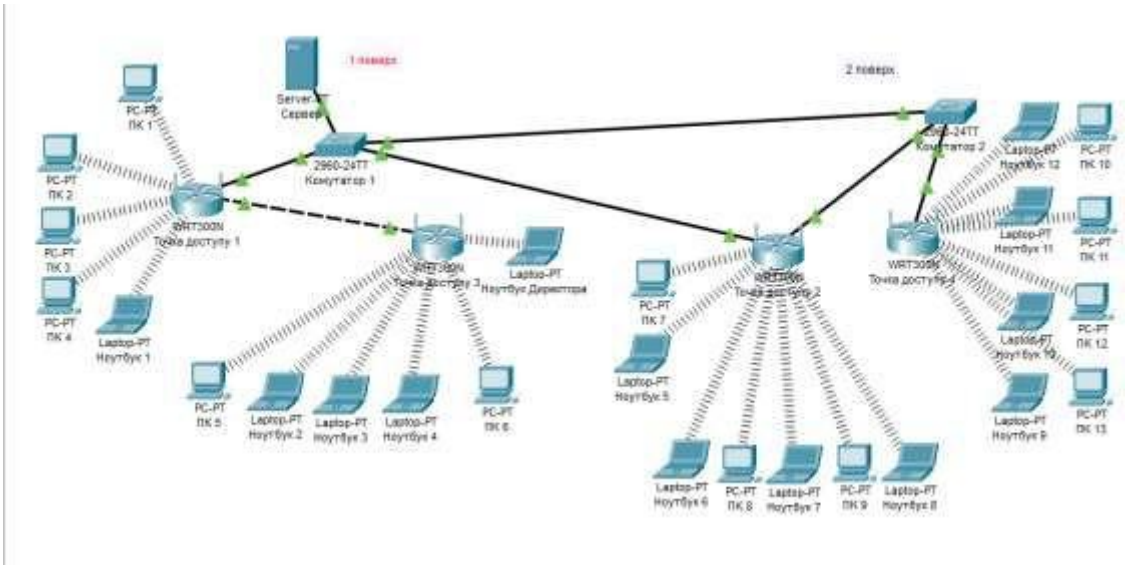


Рис. 2.3. Топологічна модель та віртуальна структурна схема корпоративної бездротової мережі.

Cisco Packet Tracer — це потужний кросплатформний інструмент для візуального моделювання та глибокої симуляції мережевих процесів, розроблений світовим лідером телекомунікаційного обладнання компанією Cisco Systems. Цей комплекс дозволяє мережевим інженерам та системним адміністраторам конструювати складні топології, додаючи віртуальні копії реальних маршрутизаторів, комутаторів, точок доступу та клієнтських пристроїв за допомогою зручного графічного інтерфейсу (перетягуванням об'єктів мишею). Головна перевага платформи полягає в можливості повноцінно імітувати конфігурацію обладнання через інтерфейс командного рядка (CLI), повністю відтворюючи поведінку реальної операційної системи Cisco IOS. Спочатку програма розроблялася виключно як закритий навчальний інструмент для слухачів Мережевої академії Cisco (в рамках сертифікації CCNA), допомагаючи їм безпечно відпрацьовувати фундаментальні навички маршрутизації та комутації без ризику вивести з ладу дороге "живе" обладнання.

2.2 Фізична топологія та апаратне забезпечення робочих просторів підприємства

Проектування ефективної IT-інфраструктури вимагає ретельного планування фізичного розміщення кінцевого та мережевого обладнання в робочих приміщеннях компанії «SoftSuper». Наочну схему розташування технічних засобів на першому поверсі відображено на відповідному архітектурному плані, рис. 2.4. У технічному відділі, який обробляє найскладніші обчислювальні задачі, встановлено чотири високопродуктивні стаціонарні робочі станції, один сучасний ноутбук для мобільних або віддалених завдань та багатофункціональний мережевий пристрій (БФП). Головним інфраструктурним центром будівлі є серверна кімната, де в спеціальній телекомунікаційній шафі змонтовано потужний сервер для баз даних, центральний керований комутатор агрегації та апаратний маршрутизатор, що виконує роль головного шлюзу безпеки та брандмауера (Firewall) підприємства. Відділ роботи з корпоративними клієнтами укомплектований двома десктопними ПК та трьома корпоративними ноутбуками, що забезпечує менеджерам необхідну мобільність під час проведення відеопрезентацій та роботи в сучасних хмарних CRM-системах. Кабінет генерального директора оснащений преміальним бізнес-ноутбуком, сучасним мережевим принтером і сканером, а також виділеною точкою доступу Wi-Fi для гарантування максимально захищеного, ізольованого та безперебійного каналу зв'язку.

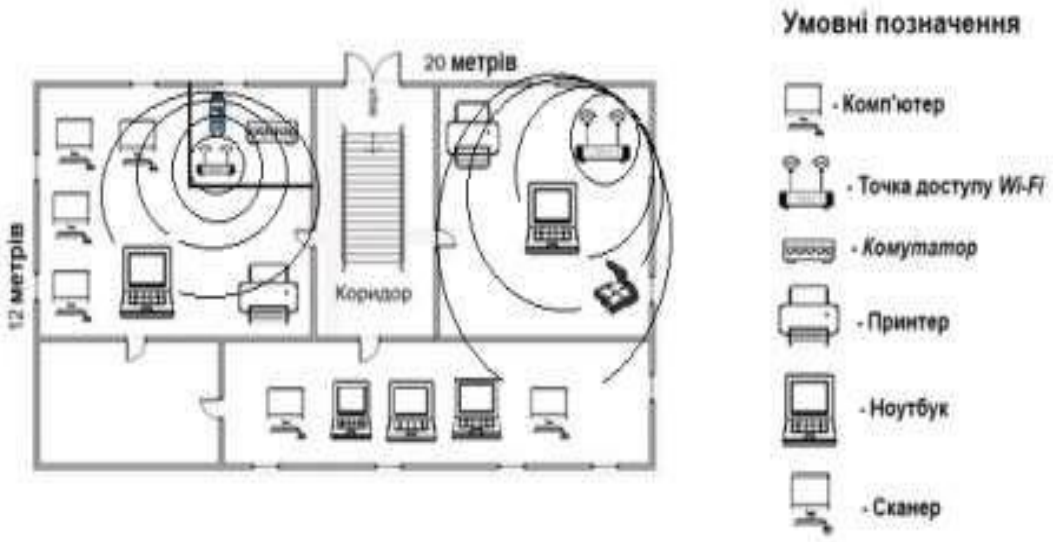


Рисунок 2.4. Схема просторового розміщення апаратного забезпечення на першому поверсі.

Розподіл комп'ютерної техніки на другому поверсі також суворо підпорядкований логіці бізнес-процесів та вимогам інформаційної безпеки кожного підрозділу. У фінансовому відділі організовано робочі місця на базі одного стаціонарного комп'ютера та одного ноутбука. Крім того, тут встановлено спеціалізований принтер для безпечного локального друку суворої фінансової звітності. Зважаючи на високий рівень конфіденційності даних, для цього відділу передбачено окреме маршрутизуюче обладнання та виділену точку доступу Wi-Fi, що дозволяє створити захищену віртуальну локальну мережу (VLAN) і повністю ізолювати фінансовий трафік від інших співробітників. Відділ продажу, робота якого орієнтована на постійну комунікацію, використовує два стаціонарні комп'ютери та три мобільні ноутбуки. Найбільша ж концентрація обладнання на другому поверсі зосереджена у відділі управління персоналом (HR). Інфраструктура цього підрозділу налічує чотири ПК, чотири ноутбуки, локальний керований комутатор для оптимізації трафіку, власну точку доступу Wi-Fi для забезпечення надійного з'єднання під час масових онлайн-співбесід, а також високошвидкісний мережевий принтер і сканер для цифровізації великих масивів кадрової документації, рис. 2.5.

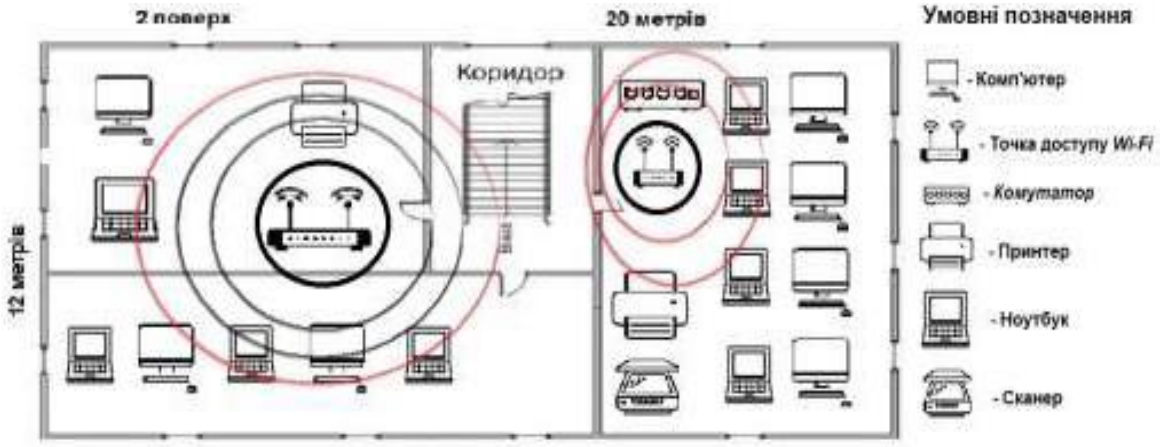


Рисунок 2.5. Схема просторового розміщення апаратного забезпечення на другому поверсі.

Загальна концепція розташування обраного комп'ютерного та мережевого обладнання базується на принципах ергономіки, корпоративної безпеки та максимальної зручності для співробітників підприємства. Особливу увагу під час проектування було приділено грамотному радіопланування. Точки доступу Wi-Fi змонтовані таким чином, щоб забезпечити щільне, рівномірне та перехресне покриття сигналом абсолютно всієї корисної площі офісу, повністю усуваючи так звані «мертві зони». Використання двох продуктивних точок доступу корпоративного класу (наприклад, стандарту Wi-Fi 6 з підтримкою технологій OFDMA та MU-MIMO) на кожному поверсі гарантує, що навіть за умови одночасного підключення десятків смартфонів, ноутбуків та смарт-пристроїв, швидкість і стабільність Інтернету залишатимуться незмінно високими.

Більше того, завдяки розгортанню бездротової мережі під управлінням єдиного апаратного або хмарного контролера, на підприємстві реалізується технологія безшовного роумінгу (стандарти 802.11k/r/v). Це означає, що працівники можуть вільно переміщатися між поверхами та кабінетами під час відеодзвінків або завантаження об'ємних файлів — їхні пристрої будуть автоматично і непомітно перемикатися на найближчу точку доступу з найкращим сигналом без жодного розриву з'єднання. Уся периферійна техніка для друку та сканування також інтегрована в цю сучасну бездротову

екосистему. Сучасні принтери підтримують мережевий та хмарний друк, що дозволяє співробітникам відправляти документи на друк прямо зі своїх мобільних пристроїв або ноутбуків з будь-якого куточка офісу, значно зменшуючи кількість кабелів та роблячи робочий простір більш охайним і технологічним.

2.3 Обґрунтування та підбір сучасного апаратного забезпечення для розгортання мережевої інфраструктури.

Для забезпечення максимальної продуктивності та надійності роботи підприємства «SoftSuper» було прийнято рішення відмовитися від застарілого обладнання (на зразок маршрутизаторів стандарту Wi-Fi 5 та 100-мегабітних комутаторів) на користь актуальних високотехнологічних рішень.

Основою бездротової мережі став сучасний дводіапазонний маршрутизатор покоління Wi-Fi 6 TP-Link Archer AX73.

Цей пристрій ефективно розподіляє навантаження: діапазон 2,4 ГГц з розширеним покриттям використовується для роботи з електронною поштою, базового веб-серфінгу та обслуговування офісних IoT-пристроїв, тоді як вільний діапазон 5 ГГц резервується для ресурсоємних завдань, відеоконференцій та передачі великих масивів даних. Безпеку корпоративної мережі гарантує підтримка найновішого криптографічного протоколу WPA3, який унеможливлює більшість сучасних хакерських атак на паролі.

Завдяки масиву високопродуктивних зовнішніх антен та інтелектуальній технології Beamforming, маршрутизатор автоматично виявляє просторове розташування підключених пристроїв і фокусує радіосигнал безпосередньо в їхньому напрямку. Наявність технологій OFDMA та MU-MIMO дозволяє маршрутизатору взаємодіяти з десятками клієнтів одночасно без жодних затримок, забезпечуючи загальну пропускну здатність бездротового каналу до

5400 Мбіт/с. Для підключення кабельної інфраструктури пристрій оснащений гігабітними портами (1 WAN та 4 LAN), що гарантує блискавичний обмін даними для стаціонарних комп'ютерів та серверів.



Рисунок. 2.6. Зовнішній вигляд сучасного маршрутизатора стандарту Wi-Fi 6.

Для розширення зони покриття додаткові маршрутизатори переведені в режим точок доступу, створюючи єдину безшовну мережу.

Оскільки використання 100-мегабітних комутаторів у сучасних умовах створює критичне «вузьке місце» (bottleneck) для обміну даними, для дротового сегмента мережі було обрано сучасний гігабітний комутатор класу TP-Link TL-SG1024, рис.2.7. Це високопродуктивний пристрій, який забезпечує оновлення інфраструктури та миттєве збільшення пропускної здатності кожного порту до 1000 Мбіт/с. Усі 24 порти комутатора підтримують технологію Auto-MDI/MDIX, що повністю усуває необхідність використання специфічних крос-кабелів — пристрій сам визначає тип підключення.



Рисунок. 2.7. Гігабітний 24-портовий мережевий комутатор.

Важливою перевагою є вбудована технологія енергозбереження Green Ethernet. Вона інтелектуально аналізує довжину підключеного кабелю та статус активності з'єднання, дозволяючи суттєво (до 75%) знизити споживання електроенергії без втрати мережевої продуктивності, що робить цей комутатор екологічно безпечним та економічно вигідним рішенням для бізнесу. Міцний металевий корпус та неблокуюча архітектура дозволяють пристрою фільтрувати та пересилати пакети даних на максимально можливій швидкості кабелю. Комутатор належить до класу Plug-and-Play, тому не потребує складного попереднього налаштування: функція автоузгодження на кожному порту самостійно визначає максимальну швидкість підключеного клієнта і встановлює оптимальний режим роботи.

У ролі центрального вузла обробки даних використовується сучасний сервер Dell PowerEdge T550 Tower, рис.2.8. Це потужна та масштабована система, ідеальна для середніх підприємств, яка забезпечує розгортання корпоративних баз даних, хмарних сховищ та інфраструктури віртуальних робочих столів (VDI).



Рисунок 2.8. Сучасний баштовий сервер Dell серії PowerEdge.

Обчислювальна потужність сервера базується на двох новітніх процесорах сімейства Intel Xeon Scalable (до 36 ядер на кожен процесор), що гарантує безпрецедентну швидкість обробки інформації [4]. Високу надійність роботи забезпечують резервні блоки живлення стандарту Platinum із підтримкою гарячої заміни. Підсистема оперативної пам'яті підтримує встановлення новітніх модулів DDR4/DDR5 з корекцією помилок (ECC), загальний обсяг яких може сягати кількох терабайт, що дозволяє миттєво обробляти найважчі корпоративні завдання. Сервер оснащений передовою дисковою підсистемою: замість старих жорстких дисків використовуються високошвидкісні твердотільні накопичувачі (NVMe SSD) формату 2.5 дюйма, об'єднані в захищені масиви за допомогою апаратного RAID-контролера

останнього покоління серії PERC. Для подальшого розширення на материнській платі передбачені слоти PCIe 4.0, які дозволяють встановлювати додаткові швидкісні мережеві карти (на 10 або 25 Гбіт/с) та потужні графічні прискорювачі для обчислень штучного інтелекту.

Для того, щоб інтегрувати стаціонарні ПК у швидкісну бездротову мережу, використовуються сучасні зовнішні Wi-Fi 6 адаптери TP-Link Archer TX20U Plus, рис.2.9.



Рисунок 2.9. Дводіапазонний бездротовий USB-адаптер стандарту Wi-Fi 6.

Цей пристрій підключається через високошвидкісний порт USB 3.0 і забезпечує пропускну здатність класу AX1800 (до 1201 Мбіт/с на частоті 5 ГГц та до 574 Мбіт/с на частоті 2,4 ГГц). Наявність двох потужних зовнішніх антен, які можна регулювати, гарантує стабільний прийом сигналу навіть крізь кілька стін. Адаптер повністю підтримує сучасні технології MU-MIMO та OFDMA, а також протокол шифрування WPA3, забезпечуючи рівень безпеки та швидкості, який раніше був доступний лише при підключенні кабелем.

Робочі місця співробітників підприємства обладнані сучасними комп'ютерами серії ARTLINE Business (або їх аналогами). Замість застарілих рішень, нові робочі станції базуються на актуальних багатоядерних процесорах Intel Core i5 13-го покоління (наприклад, i5-13400), що забезпечують чудову багатозадачність. Системи оснащені 16 ГБ швидкої оперативної пам'яті стандарту DDR4/DDR5 та працюють виключно на базі твердотільних накопичувачів M.2 NVMe SSD об'ємом 1 ТБ, що гарантує миттєве завантаження операційної системи Windows 11 Pro та офісних додатків (повністю виключаючи повільні та ненадійні HDD-диски). Обробка графіки здійснюється або потужним інтегрованим ядром, або сучасними енергоефективними відеокартами, що є оптимальним для бізнес-середовища.

Крім стаціонарних ПК, мобільність персоналу забезпечують 13 сучасних корпоративних ноутбуків класу Lenovo ThinkBook 15 (або актуальні моделі серії IdeaPad Slim). Ці пристрої вирізняються тонким алюмінієвим корпусом, якісними IPS-дисплеями та потужною апаратною платформою (на базі сучасних процесорів Intel Core або AMD Ryzen з 16 ГБ оперативної пам'яті та швидкими SSD), що дозволяє комфортно працювати як в офісі, так і у відрядженнях.

Для оптимізації документообігу підприємство оновило парк периферійної техніки. Використовуються 4 багатофункціональні пристрої корпоративного рівня HP LaserJet Pro MFP (замість базових домашніх моделей). Це швидкісні лазерні принтери з підтримкою двостороннього друку, які інтегруються безпосередньо в бездротову мережу підприємства,

дозволяючи співробітникам відправляти документи на друк прямо зі своїх смартфонів або ноутбуків. Оцифрування документації здійснюється за допомогою 2 професійних потокових сканерів Canon, які здатні автоматично обробляти пачки документів з високою швидкістю та одразу відправляти відскановані файли на корпоративний сервер або в хмарне сховище.

2.4 Програмні комплекси та операційні системи для управління мережевою інфраструктурою

Для забезпечення безперебійної та максимально ефективної роботи всіх підрозділів підприємства «SoftSuper» впроваджено сучасну екосистему програмного забезпечення. Оскільки кожен відділ виконує свою специфічну роль у загальному бізнес-механізмі, для них підібрано спеціалізовані цифрові інструменти, які відповідають найвищим корпоративним стандартам.

У фінансовому відділі, де точність і безпека даних є критично важливими, спеціалісти відмовилися від розрізнених локальних файлів на користь комплексних хмарних рішень. Для глибокого фінансового моделювання, складних розрахунків та консолідації звітів використовується багатофункціональне середовище Microsoft 365 (яке прийшло на зміну класичному локальному Excel). Що стосується безпосередньо бухгалтерського обліку, то замість застарілих десктопних версій програм на кшталт класичного QuickBooks, компанія використовує сучасні хмарні SaaS-системи обліку. Такі платформи дозволяють у режимі реального часу відстежувати грошові потоки, автоматично генерувати рахунки-фактури, зводити баланс та аналізувати прибутковість. Для повсякденної спільної роботи з текстовими документами та презентаціями відділ покладається на корпоративну платформу Google Workspace (яка включає Google Docs, Sheets та Slides). Це забезпечує можливість одночасного редагування документів кількома співробітниками з

будь-якого пристрою. Хоча історично для стиснення великих обсягів даних використовувалися локальні архіватори на кшталт WinRAR (що підтримують формати RAR, ZIP, 7Z, TAR, ISO), сьогодні підприємство все частіше переходить на безпечний обмін корпоративними даними через зашифровані хмарні посилання, залишаючи базові функції архівації на рівні вбудованих інструментів сучасних операційних систем Windows 11 Pro.

Технічний відділ компанії потребує найпотужніших інструментів для проектування та розробки. Для вирішення інженерних завдань, розробки апаратних компонентів та створення детальних 2D/3D моделей в області механіки й електрики використовується система автоматизованого проектування AutoCAD. Для складного математичного моделювання, тестування алгоритмів та глибокого аналізу великих масивів даних (Data Science) інженери застосовують платформу MATLAB. Окрім цього, оскільки компанія активно займається розробкою сучасних програмних продуктів, технічний стек відділу був суттєво розширений. Інженери активно використовують передові інструменти для бекенд-розробки, зокрема середовища для роботи з Node.js, платформи для проектування та тестування API на базі GraphQL, а також сучасні рішення для серверного адміністрування та DevOps-практик (такі як Docker для контейнеризації), що забезпечує безперервну інтеграцію та надійну роботу корпоративних сервісів.

Відділ управління персоналом (HR) керує найціннішим ресурсом компанії — людьми, тому для автоматизації рутинних процесів тут впроваджено потужну корпоративну платформу SAP SuccessFactors. Це сучасне хмарне програмне забезпечення дозволяє ефективно супроводжувати співробітника на всіх етапах його роботи: від рекрутингу та адаптації (онбордингу) до регулярної оцінки продуктивності (KPI), планування розвитку кар'єри, організації внутрішнього навчання та адміністрування процесів звільнення.

Під час логічного проектування бездротової комп’ютерної мережі Wi-Fi для автоматизації підключення клієнтських пристроїв був задіяний протокол

DHCP (Dynamic Host Configuration Protocol). Його головна функція полягає в тому, щоб звільнити системних адміністраторів від необхідності вручну прописувати налаштування для кожного нового смартфона чи ноутбука. Коли пристрій підключається до мережі, корпоративний DHCP-сервер миттєво та автоматично виділяє йому вільну IP-адресу з доступного пулу, а також передає всі супутні параметри: маску підмережі, адресу основного шлюзу для виходу в Інтернет та адреси DNS-серверів. Цей стандартизований протокол підтримується абсолютно всіма сучасними операційними системами, зводячи до нуля ризик виникнення конфліктів IP-адрес через людський фактор.

Особливу увагу під час модернізації мережі було приділено питанням інформаційної безпеки, оскільки використання застарілих технологій є неприпустимим у сучасному корпоративному середовищі. Початковий проект передбачав використання стандарту WPA2 PSK на першому поверсі та WEP на другому. Однак протокол WEP (Wired Equivalent Privacy) був визнаний критично вразливим і офіційно застарілим ще понад п'ятнадцять років тому — його шифрування можна зламати за лічені хвилини за допомогою загальнодоступних програм.

Тому конфігурацію безпеки було повністю переглянуто та оновлено до сучасних вимог:

На першому поверсі (де працюють технічні спеціалісти та відбувається комунікація з клієнтами) розгорнуто мережу із захистом WPA3-Personal (зі зворотною сумісністю WPA2-PSK для старіших пристроїв). Цей новітній стандарт гарантує надійний захист від атак типу "перебір за словником".

На другому поверсі, де розташовані фінансовий та HR-відділи, які обробляють суворо конфіденційну інформацію підприємства, впроваджено максимальний рівень захисту — WPA3-Enterprise. Замість одного спільного пароля для всіх, ця технологія вимагає від кожного працівника вводити власні унікальні облікові дані (логін та пароль) через виділений сервер авторизації (RADIUS), що забезпечує абсолютний контроль над тим, хто саме і коли отримує доступ до корпоративної мережі.

3 СУЧАСНІ МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ WI-FI

3.1 Комплексні підходи та фундаментальні принципи захисту інформації в бездротових системах

Для забезпечення надійного функціонування та мінімізації будь-яких ризиків компрометації корпоративної чи домашньої бездротової мережі необхідно реалізувати комплексний підхід до її налаштування. Насамперед, критично важливою дією є негайна зміна всіх паролів, встановлених виробником за замовчуванням. Більшість сучасного мережевого обладнання, включно з бездротовими точками доступу та маршрутизаторами, постачається з універсальними заводськими обліковими даними адміністратора (наприклад, admin/admin), що робиться виключно для спрощення первинного налаштування. Оскільки ці стандартні комбінації є загальнодоступними в Інтернеті і навіть зашиті в бази даних автоматизованих хакерських скриптів, вони забезпечують лише ілюзію безпеки. Встановлення унікального, складного пароля, що складається з комбінації літер різного регістру, цифр та спеціальних символів, а також його періодичне оновлення — це фундаментальна, перша лінія оборони вашого пристрою від несанкціонованого втручання.

Наступним важливим етапом є суворе обмеження фізичного та логічного доступу до мережевої інфраструктури. Підключатися до внутрішніх ресурсів повинні виключно авторизовані користувачі та перевірені корпоративні пристрої. Одним із методів базового контролю є фільтрація за MAC-адресами (унікальними апаратними ідентифікаторами мережевих адаптерів). Створивши так званий «білий список», адміністратор дозволяє підключення лише заздалегідь визначеним гаджетам. Хоча сучасні мобільні операційні

системи часто використовують динамічну зміну MAC-адрес задля приватності користувачів, на рівні стаціонарного офісного обладнання ця функція залишається дієвим додатковим бар'єром. Для відвідувачів, клієнтів або особистих смартфонів співробітників (концепція BYOD) абсолютно необхідним є налаштування ізольованої гостьової мережі. Ця функція, доступна в більшості сучасних маршрутизаторів, дозволяє створити паралельний бездротовий канал зі своїм окремим паролем та жорсткими обмеженнями, надаючи гостям доступ лише до глобального Інтернету і повністю блокуючи будь-які спроби проникнути в конфіденційну локальну мережу підприємства.

Центральне місце в архітектурі безпеки займає надійне криптографічне шифрування трафіку. Перехоплення радіосигналів у відкритому ефірі є тривіальним завданням для зловмисників, тому дані повинні перетворюватися на нечитабельний код. Сучасні протоколи, такі як сімейство Wi-Fi Protected Access (WPA, WPA2 та найновіший WPA3), відповідають за безпечну передачу інформації між маршрутизатором та клієнтом. Хоча WPA та WPA2 досі широко підтримуються для забезпечення сумісності зі старим обладнанням, галузевим еталоном на сьогодні є стандарт WPA3. Він забезпечує неперевершену криптографічну стійкість та захищає навіть від атак перебору словника, коли користувач встановив слабкий пароль. Тому для побудови безпечної інфраструктури наполегливо рекомендується використовувати виключно те обладнання, яке повноцінно підтримує WPA3, оскільки використання застарілих алгоритмів може залишити критичні прогалини в захисті [10].

Не менш важливо приділити увагу захисту публічного ідентифікатора набору послуг (SSID), тобто назви вашої Wi-Fi мережі. Залишати заводську назву (наприклад, "TP-Link_5G" чи "ASUS_Router") вкрай небезпечно, оскільки це миттєво розкриває зловмисникам виробника вашого обладнання, дозволяючи їм швидко підібрати специфічні експлойти для відомих вразливостей цієї моделі. Назву слід змінити на щось нейтральне та унікальне. Крім того, для ускладнення розвідки мережі можна вимкнути широкомовну

трансляцію SSID. Хоча професійні хакери здатні виявити приховану мережу за допомогою спеціалізованих аналізаторів пакетів, для базового захисту від випадкових спроб підключення це залишається корисною практикою.

Комплексна безпека також вимагає обов'язкового розгортання брандмауерів (мережевих екранів) на кількох рівнях. Перший рубіж оборони — це апаратний брандмауер, вбудований безпосередньо в маршрутизатор, який фільтрує вхідний трафік з глобальної мережі та блокує несанкціоновані зовнішні запити. Проте, якщо зловмисник зуміє підключитися до вашого Wi-Fi (наприклад, зламавши пароль або перебуваючи всередині офісу), він опиниться за цим першим бар'єром. Саме тому на кожному робочому комп'ютері повинен бути активований брандмауер на базі хоста (вбудований в операційну систему), який контролюватиме локальні підключення та додасть необхідний внутрішній рівень ізоляції. Цей захист обов'язково має доповнюватися сучасним антивірусним програмним забезпеченням (або системами класу EDR для підприємств), яке не лише шукає класичні віруси, але й евристично аналізує поведінку програм, блокуючи шпигунське програмне забезпечення, програми-вимагачі та приховане рекламне ПЗ. Бази даних таких антивірусів повинні оновлюватися в автоматичному режимі.

Особливої обережності вимагає функція спільного доступу до файлів та принтерів у локальній мережі. Цю опцію слід тримати вимкненою за замовчуванням на всіх пристроях і активувати виключно за наявності чіткої виробничої необхідності. Якщо обмін файлами потрібен для роботи, його варто організовувати лише в межах довіреної домашньої або корпоративної мережі, створюючи спеціальні виділені каталоги. Доступ до таких папок має бути суворо регламентований і захищений окремими надійними паролями. Використання функцій спільного доступу під час підключення до публічних і незахищених Wi-Fi мереж (у кафе, готелях чи аеропортах) є категорично неприпустимим, оскільки це відкриває ваші дані для прямого доступу будь-якому користувачеві тієї ж мережі [10].

Жодна архітектура безпеки не буде дієвою без регулярного оновлення мікропрограм (прошивок) мережевого обладнання. Виробники маршрутизаторів та точок доступу постійно виявляють нові програмні вразливості та випускають патчі безпеки для їх усунення. Адміністраторам необхідно регулярно моніторити офіційні вебсайти виробників на наявність таких оновлень або налаштувати автоматичне встановлення критичних виправлень у панелі керування пристроєм. Додаткову інформацію та рекомендації щодо специфічних параметрів безпеки можна також отримати від вашого інтернет-провайдера або звернувшись до розділу підтримки клієнтів виробника обладнання.

Нарешті, для гарантування безпеки під час віддаленої роботи або використання неперевірених мереж, стандартом де-факто є застосування віртуальних приватних мереж (VPN). Сучасні компанії використовують VPN-тунелі для того, щоб їхні співробітники могли безпечно отримувати доступ до внутрішніх корпоративних баз даних з будь-якої точки світу. VPN-клієнт створює захищений криптографічний канал, який повністю шифрує весь інтернет-трафік на стороні відправника. Навіть якщо зловмисник перехопить цей потік даних у відкритій Wi-Fi мережі, він отримає лише беззмістовний набір символів, оскільки розшифрувати його зможе лише авторизований сервер-отримувач на стороні компанії [10].

3.2 Еволюція та технічні особливості стандартів безпеки: протоколи WPA та WPA2

Технологія Wi-Fi Protected Access (WPA) стала фундаментальним стандартом мережевої безпеки, який сьогодні є абсолютно обов'язковим для функціонування будь-яких бездротових мереж. Цей протокол був розроблений консорціумом Wi-Fi Alliance і офіційно впроваджений у 2003 році як екстрена

та надійна заміна для застарілої системи WEP (Wired Equivalent Privacy), чиї криптографічні алгоритми виявилися критично вразливими до хакерських атак. Спочатку WPA проектувався як проміжне, тимчасове рішення, покликане захистити користувачів до моменту виходу повноцінного стандарту другого покоління. Головною перевагою першої версії WPA стала її зворотна сумісність: користувачам не потрібно було купувати нові маршрутизатори, достатньо було лише оновити мікропрограму (прошивку) існуючого обладнання. Відмовившись від статичних ключів, ця технологія запровадила обов'язкову автентифікацію через пароль або виділені сервери RADIUS, використовуючи для шифрування алгоритм RC4 та протокол TKIP.

Організації та приватні користувачі можуть розгортати стандарти сімейства WPA у двох принципово різних архітектурних режимах, які підтримуються всіма поколіннями цієї технології. Перший режим — це персональний (WPA-Personal або WPA-PSK), який базується на використанні єдиного попередньо наданого ключа. Він ідеально підходить для домашніх або невеликих офісних мереж завдяки максимальній простоті налаштування. Проте його головний недолік полягає в тому, що у разі компрометації пароля (наприклад, при втраті корпоративного ноутбука) системному адміністратору доведеться змінювати ключ доступу абсолютно на всіх пристроях у мережі [11]. Альтернативою є корпоративний режим (WPA-Enterprise або WPA-802.1x), створений спеціально для середніх та великих підприємств. Ця архітектура вимагає наявності сервера автентифікації RADIUS. Замість загального пароля кожен співробітник використовує власні унікальні облікові дані для підключення до Wi-Fi. Якщо певний пристрій зламано або працівник звільняється, адміністратор може миттєво заблокувати доступ лише цьому конкретному користувачеві, не перериваючи роботу всієї компанії. Незважаючи на очевидні переваги, розгортання режиму Enterprise вимагає глибокої експертизи від IT-відділу та може передбачати додаткові витрати на інфраструктуру, а також не підтримується дуже старим обладнанням або застарілими операційними системами.

Фундамент безпеки бездротових мереж базується на кількох надзвичайно важливих програмних компонентах та алгоритмах. Першим із них є протокол цілісності тимчасового ключа (TKIP). Він був створений робочою групою IEEE 802.11i спеціально для подолання слабких місць WEP. Хоча TKIP і використовує той самий потоковий шифр RC4, він запровадив революційну на той час концепцію: генерацію 128-бітного тимчасового ключа, який автоматично змінюється кожні 10 000 переданих пакетів. Це гарантує, що зловмисник не зможе накопичити достатньо даних для розшифрування мережевого трафіку.

Згодом, разом із виходом стандарту WPA2, індустрія перейшла на розширений стандарт шифрування (AES). Це потужний симетричний блоковий шифр військового класу (з підтримкою ключів на 128, 192 та 256 біт), який працює виключно на новому обладнанні з відповідною апаратною підтримкою. На відміну від TKIP, AES забезпечує найвищий рівень безпеки (на рівні протоколів IPSec), що робить його єдиним правильним вибором для мереж, де циркулює конфіденційна комерційна інформація.

Додатковий рівень захисту забезпечується вбудованою машинною автентифікацією. У цьому сценарії пристрої підключаються до мережі автоматично, обмінюючись цифровими сертифікатами або спеціальними ключами із сервером RADIUS без ручного введення паролів користувачами. Для цього використовуються захищені транспортні протоколи на кшталт EAP-TLS або PEAP-MSCHAP v2 [11].

Сам процес встановлення захищеного з'єднання між клієнтським пристроєм (наприклад, смартфоном) та маршрутизатором відбувається за допомогою так званого «чотиристороннього рукостискання» (4-way handshake). Це геніальний криптографічний алгоритм, який дозволяє обом сторонам довести одна одній, що вони знають правильний пароль (головний ключ PMK), жодного разу не пересилаючи сам цей пароль через відкритий радіоефір. Замість цього вони обмінюються зашифрованими математичними підтвердженнями. Нарешті, щоб уникнути атак типу "зловмисник посередині"

(MitM), коли хакер перехоплює пакет даних, змінює в ньому кілька бітів і відправляє далі, застосовується перевірка цілісності повідомлення (MIC). Завдяки спеціальним алгоритмам хешування, отримувач може миттєво розпізнати підроблений пакет і відкинути його.

Перше покоління (WPA1) стало рятівним колом для індустрії. Використовуючи 256-розрядні ключі замість слабких 64-розрядних у WEP, воно запровадило алгоритм MIC та централізовану автентифікацію через структуру 802.1X EAP. Це дозволило захистити заголовки пакетів та інтегрувати спеціальний лічильник кадрів, який унеможливив атаки повторного відтворення.

Справжнім індустріальним стандартом на довгі роки стала сертифікація другого покоління — WPA2, офіційно ратифікована у 2006 році на базі повного стандарту IEEE 802.11i [11]. Ключовою відмінністю від попередника стала повна відмова від вразливого шифру RC4 на користь монолітного протоколу AES-CCMP. Графічне відображення логіки підключення пристроїв у цьому середовищі представлено на відповідній схемі, рис. 3.1.

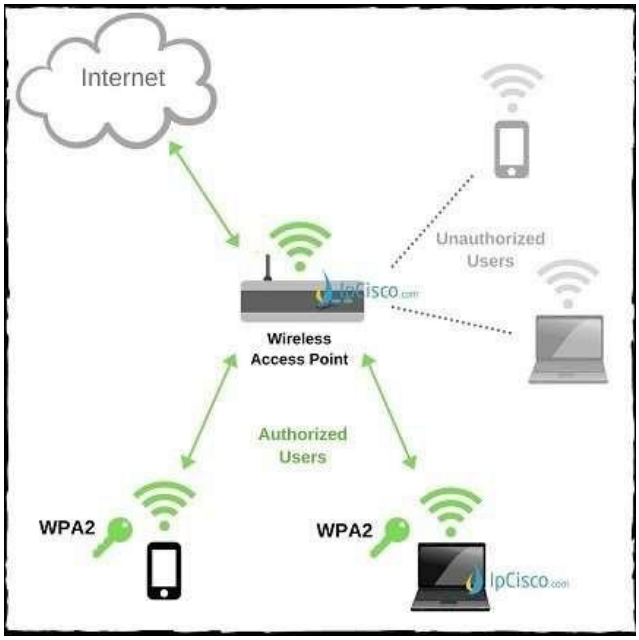


Рисунок 3.1. Схематичне відображення процесу авторизації та підключення клієнтських пристроїв у середовищі WPA2.

Незважаючи на високу надійність, з часом дослідники кібербезпеки виявили слабкі місця WPA2, зокрема вразливість до офлайн-атак за словником (коли хакер перехоплює "рукостискання" і намагається підібрати слабкий пароль на потужному комп'ютері вдома). Крім того, функція швидкого підключення WPS (Wi-Fi Protected Setup) через PIN-код виявилася критичною діркою в безпеці, яку сьогодні рекомендують повністю вимикати.

Щоб відповісти на сучасні виклики кіберзлочинності, було розроблено стандарт третього покоління — WPA3. Він забезпечує безпрецедентний рівень криптографічного захисту. Протокол CCMP був замінений на ще більш стійкий Галуа/лічильник (GCMP), а довжина ключа для корпоративного сектора зросла до 192 біт. Замість вразливого WPS було запроваджено протокол DPP, який дозволяє безпечно додавати пристрої до мережі скануванням QR-коду або через NFC. Найважливішою інновацією WPA3 стала заміна старого алгоритму рукостискання на протокол одночасної автентифікації рівних (SAE). SAE має імунітет до офлайн-атак за словником: система просто не дозволить хакеру безкінечно підбирати пароль до перехопленого хешу. Крім того, WPA3 запровадив технологію прямої секретності (Forward Secrecy). Це означає, що навіть якщо зловмисник колись у майбутньому дізнається пароль від вашої мережі, він все одно не зможе розшифрувати архівний трафік, який перехопив і записав раніше. Для відкритих публічних мереж (наприклад, у кафе) WPA3 пропонує опортуністичне бездротове шифрування (OWE), яке автоматично і непомітно шифрує трафік кожного окремого користувача, не вимагаючи введення жодних паролів [11].

У підсумку, використання технологій сімейства WPA є критично важливою умовою існування сучасних бездротових мереж. Вони забезпечують надійний криптографічний бар'єр, роблячи перехоплені дані абсолютно нечитабельними для сторонніх осіб, тим самим захищаючи комерційні таємниці організацій та особисту приватність користувачів від постійних загроз у цифровому світі.

3.3 Технології віртуальних приватних мереж: криптографічні протоколи та принципи шифрування трафіку

У сучасному цифровому світі, де зловмисники постійно полюють на конфіденційну інформацію під час її передачі через відкриті мережі, використання надійних механізмів захисту є критично необхідним. Оскільки для розшифрування перехоплених даних хакерам потрібен відповідний криптографічний ключ, вони зазвичай уникають складних систем і переслідують більш легкі, незахищені цілі. Саме тому шифрування трафіку за допомогою віртуальних приватних мереж (VPN) має вирішальне значення для зменшення ризику компрометації корпоративних та особистих даних підприємства «SoftSuper» під час їх транзиту через глобальний Інтернет.

Головне завдання будь-якого VPN-сервісу полягає у виконанні двох базових функцій: надійному кодуванні пакетів даних (щоб зробити їх нечитабельними для сторонніх) та маскуванні реальної IP-адреси користувача (для забезпечення анонімності та захисту приватності). Важливо розуміти межі дії цієї технології: VPN шифрує виключно інтернет-трафік (веб-серфінг, повідомлення в месенджерах, пересилку файлів). Він жодним чином не захищає стандартні текстові SMS-повідомлення чи звичайні телефонні дзвінки, оскільки вони передаються через закриті стільникові мережі мобільних операторів, а не через інтернет-канали [11].

Концептуально робота VPN виглядає наступним чином: між пристроєм користувача (наприклад, смартфоном співробітника у відрядженні) та віддаленим VPN-сервером компанії створюється захищений, зашифрований віртуальний "тунель". Усі дані проходять виключно через цей тунель, а сам VPN-сервер слугує єдиним шлюзом для виходу в загальнодоступний Інтернет. Надійність цього процесу цілком залежить від обраних протоколів та алгоритмів шифрування. Протокол VPN — це набір стандартизованих правил та математичних процесів, які визначають, як саме формується цей безпечний

шлях. Різні постачальники послуг використовують різні протоколи, що безпосередньо впливає на швидкість з'єднання, його стабільність та рівень захищеності від вразливостей.

Сучасний ландшафт протоколів тунелювання є досить різноманітним, тому для потреб підприємства необхідно обирати лише найбезпечніші рішення:

OpenVPN: На сьогодні цей протокол заслужено вважається золотим галузевим стандартом безпеки. Це гнучка технологія з відкритим вихідним кодом (Open Source), що дозволяє незалежним експертам постійно перевіряти її на наявність вразливостей. OpenVPN спирається на потужну криптографічну бібліотеку OpenSSL та протоколи безпеки транспортного рівня (TLS). Його архітектура розділяє шифрування на два потоки: канал даних (захищає саму інформацію за допомогою шифру та хеш-автентифікації) та канал управління (захищає процес з'єднання між пристроєм і сервером). Використання технології ідеальної прямої секретності (Perfect Forward Secrecy) гарантує, що для кожної нової сесії генеруються унікальні ефемерні ключі, які одразу знищуються після завершення з'єднання, що робить OpenVPN надзвичайно стійким до компрометації.

WireGuard: Це відносно новий, але надзвичайно перспективний протокол з відкритим вихідним кодом, який стрімко набирає популярність як сучасна альтернатива OpenVPN. Його головна перевага — мінімалістична та оптимізована архітектура коду (лише кілька тисяч рядків порівняно з сотнями тисяч у OpenVPN), що забезпечує блискавичну швидкість з'єднання, менше споживання заряду батареї на мобільних пристроях та використання виключно найсучасніших криптографічних примітивів.

IKEv2/IPSec: Протокол обміну ключами Інтернету версії 2 (Internet Key Exchange v2), який завжди працює в парі з набором протоколів безпеки IPSec. Ця комбінація є ідеальним вибором для мобільних пристроїв. Її унікальна властивість полягає у здатності миттєво та непомітно для користувача відновлювати розірване з'єднання (наприклад, коли смартфон перемикається з

домашнього Wi-Fi на мобільний 4G-інтернет), зберігаючи при цьому найвищий рівень захисту [11].

L2TP/IPSec: Протокол тунелювання другого рівня (L2TP) сам по собі не забезпечує шифрування, тому його завжди використовують разом із IPSec. IPSec працює на мережевому рівні, шифруючи як корисне навантаження пакета, так і його заголовок. Однак використання цієї зв'язки сьогодні вважається менш доцільним через складнощі з проходженням через брандмауери (які часто блокують його специфічні порти) та потенційні вразливості при використанні попередньо наданих ключів (PSK).

SSTP (Secure Socket Tunneling Protocol): Це пропрієтарний протокол, розроблений корпорацією Microsoft. Він глибоко інтегрований в операційні системи Windows і забезпечує високий рівень безпеки (схожий на OpenVPN, оскільки також використовує SSL/TLS-канали). Проте через закритий вихідний код та обмежену підтримку на інших платформах (наприклад, на пристроях Apple) він використовується переважно в моноплатформних корпоративних середовищах.

PPTP (Point-to-Point Tunneling Protocol): Один із найстаріших протоколів, створений ще в епоху комутованих з'єднань (dial-up). Важливо наголосити, що сьогодні PPTP вважається критично застарілим і абсолютно небезпечним. Його алгоритми шифрування легко зламуються сучасними обчислювальними потужностями, тому його використання в мережі «SoftSuper» суворо заборонено.

Будь-яке шифрування базується на математичній функції (алгоритмі або шифрі), яка бере зрозумілий відкритий текст і хаотично перетворює його на зашифрований набір символів (шифротекст). Цей процес унеможливлює прочитання або компрометацію даних у разі їх перехоплення. Щоб розблокувати таку інформацію, отримувач повинен мати правильний "пароль" — ключ шифрування. Надійність ключа прямо залежить від його довжини: наприклад, ключ розміром 256 біт створює астрономічну кількість можливих комбінацій, що робить його злам методом простого перебору (brute-force)

практично неможливим навіть для найпотужніших сучасних суперкомп'ютерів.

Симетричне шифрування: Цей метод використовує один і той самий секретний ключ як для шифрування повідомлення відправником, так і для його розшифрування отримувачем. Це вимагає, щоб обидві сторони заздалегідь безпечно обмінялися цим ключем. Найвідомішим і найбезпечнішим стандартом симетричного шифрування, який сертифікований Національним інститутом стандартів і технологій США (NIST) і використовується в найкращих VPN, є алгоритм Advanced Encryption Standard (AES), зокрема його модифікація з довжиною ключа 256 біт (AES-256) [11].

Асиметричне шифрування (криптографія з відкритим ключем): Цей підхід вирішує проблему безпечної передачі ключів, використовуючи пару математично пов'язаних ключів: відкритий та закритий. Відкритий ключ вільно розповсюджується і використовується будь-ким для шифрування повідомлення. Проте розшифрувати це повідомлення може лише той користувач, який володіє унікальним закритим (приватним) ключем, що зберігається в суворій таємниці. Класичним прикладом такого алгоритму є RSA, який широко застосовується для безпечного встановлення первинного з'єднання між клієнтом і сервером.

Підсумовуючи, використання VPN є незамінним інструментом для уникнення моніторингу інтернет-активності та захисту корпоративних даних від перехоплення. Завдяки шифруванню як самого тунелю, так і потоку даних у ньому, VPN зберігає анонімність і безпеку. Для досягнення максимального рівня захисту в IT-інфраструктурі підприємства рекомендується впроваджувати галузеві стандарти на кшталт OpenVPN або WireGuard у комбінації з військовим рівнем симетричного шифрування AES-256. Однак слід пам'ятати головне правило криптографії: безпека будь-якого, навіть найсучаснішого методу шифрування, цілком і повністю залежить від збереження абсолютної секретності криптографічних ключів.

ВИСНОВКИ

Технологія Wi-Fi має безперечні переваги для розгортання корпоративних інфраструктур, головною з яких є безпрецедентна мобільність та відсутність необхідності прокладання складних кабельних трас. Еволюція стандартів сімейства IEEE 802.11 призвела до появи надшвидкісних технологій Wi-Fi 6 та Wi-Fi 7, які функціонують у діапазонах 2,4 ГГц, 5 ГГц та 6 ГГц, забезпечуючи колосальну пропускну здатність.

Під час виконання проєкту було розроблено та практично обґрунтовано архітектуру бездротової мережі для підприємства «SoftSuper». Просторове планування та розміщення точок доступу враховує специфіку роботи технічного відділу, відділу роботи з клієнтами, фінансового департаменту та служби HR на двох поверхах, усуваючи радіоперешкоди та забезпечуючи безшовний роумінг. Для побудови ядра мережі підібрано високопродуктивне обладнання: дводіапазонні маршрутизатори Wi-Fi 6 (TP-Link Archer AX73), гігабітні комутатори (TP-Link TL-SG1024) та сервер Dell PowerEdge T550. Візуальне моделювання топології успішно реалізовано в середовищі Cisco Packet Tracer.

Вирішальним етапом проектування стало гарантування інформаційної безпеки. Оскільки відкритий радіоефір вимагає суворого криптографічного контролю, у мережі було відкинуто застарілі вразливі протоколи. Замість них впроваджено стандарти WPA3-Personal для загальних зон та найвищий рівень захисту WPA3-Enterprise із сервером авторизації RADIUS для фінансового відділу. Для захисту корпоративного трафіку під час віддаленої роботи обґрунтовано необхідність використання віртуальних приватних мереж (VPN) на базі сучасних протоколів OpenVPN та WireGuard із застосуванням шифрування AES-256..

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Таненбаум Е., Уезерролл Д. Комп’ютерні мережі. 6-те вид. Київ : Діалектика, 2020. 960 с.

2 Оліфер В. Г., Оліфер Н. А. Комп’ютерні мережі. Принципи, технології, протоколи : підручник. 5-те вид. Київ : Видавництво, 2021. 992 с.

3 Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2020. 864 p.

4 IEEE 802.11-2020: IEEE Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks. IEEE, 2021. 4372 p.

5 Wi-Fi CERTIFIED WPA3™ Technology and Security Specification. Wi-Fi Alliance. URL: https://www.wi-fi.org/discover-wi-fi/security

6 Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2020. 768 p.

7 Технічні характеристики та посібник користувача маршрутизатора TP-Link Archer AX73. Офіційний сайт TP-Link. URL: https://www.tp-link.com/ua/home-networking/wifi-router/archer-ax73/.

8 Dell PowerEdge T550 Tower Server: Technical Guide. Dell Technologies. URL: https://www.dell.com.

9 Cisco Packet Tracer 8.x: User Guide & Simulation Tool. Cisco Networking Academy. URL: https://www.netacad.com/.

10 Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium, 2017. URL: https://www.wireguard.com/papers/wireguard.pdf.

11 OpenVPN Official Documentation and Security Overview. OpenVPN Inc. URL: https://openvpn.net/community-resources/.

12 FIPS PUB 197: Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), 2001. 51 p.

13 Rigney C., Willens S., Rubens A., Simpson W. Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865. URL: https://datatracker.ietf.org/doc/html/rfc2865.

14 High-Efficiency Wireless LANs: 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7) Performance Analysis. IEEE Communications Magazine. 2023. Vol. 61, No. 2. P. 112–118.

15 Налаштування безшовного роумінгу (стандарти 802.11k, 802.11r, 802.11v) у корпоративних WLAN. Cisco Systems Design Guide. 2022.

16 Технології MU-MIMO та OFDMA у сучасних бездротових мережах: принципи роботи та оцінка пропускної здатності. Journal of Network and Computer Applications, 2024.

17 Комутатори некеровані гігабітні TP-Link TL-SG1024: Технічна документація. URL: https://www.tp-link.com/.

18 арні сервіси та платформи (SaaS, IaaS) у корпоративному середовищі: інтеграція Microsoft 365 та SAP SuccessFactors. IT Enterprise Journal. 2025. № 4. С. 45–52.

19 Інтернет речей (IoT) та протокол 802.11ah (Wi-Fi HaLow): особливості побудови низькоенергетичних мереж. Журнал телекомунікаційних технологій. 2024. № 1. С. 30–38.

20 Динамічна конфігурація вузлів (DHCP) та маршрутизація в локальних мережах. Комп'ютерні системи та інженерія. 2023. Вип. 12. С. 88–95.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)