МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ, ПСИХОЛОГІЇ ТА БЕЗПЕКИ

Кафедра інформаційних технологій

РОЗРОБЛЕННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПРИВАТНОГО ПІДПРИЄМСТВА

Кваліфікаційна робота
здобувача вищої освіти
4 курсу заочної форми навчання
Олега ГУРСЬКОГО

Науковий керівник:
доцент, кандидат технічних наук
Любомир ФЛУД

Рецензент:

_____
вчене звання, науковий ступінь

_____
(Ім'я ПРІЗВИЩЕ рецензента)

Кваліфікаційна робота допущена до захисту
«___» _____ 2026 р., протокол № ____

Завідувач кафедри інформаційних технологій
_____ Олег ЗАЧЕК
(підпис)

Львів
2026

АНОТАЦІЯ

ГУРСЬКИЙ О. Розроблення локальної комп’ютерної мережі приватного підприємства. – Рукопис.

Дослідження на здобуття освітнього ступеня «бакалавр» за спеціальністю 126 «Інформаційні системи та технології». – Львівський державний університет внутрішніх справ, МВС України, Львів, 2026.

У кваліфікаційній роботі розглянуто питання проєктування, побудови та впровадження сучасної локальної комп’ютерної мережі для приватного підприємства. Актуальність теми зумовлена стрімким зростанням обсягів інформації, необхідністю ефективного обміну даними та підвищенням продуктивності роботи сучасних підприємств через якісну мережеву інфраструктуру.

У роботі проведено аналіз вимог до мережевої інфраструктури, огляд сучасних технологій та топологій локальних мереж структурованої кабельної системи, активного мережевого обладнання та засобів інформаційної безпеки. Розроблено детальний план IP- адресації, схему фізичного та логічного підключення пристроїв, а також організації гостьового доступу. Запропонована мережа орієнтована на ефективну підтримку бізнес-процесів, простоту адміністрування, захищеність інформації та гнучкість подальшого розвитку інфраструктури.

Ключові слова: локальна комп’ютерна мережа, проєктування мережі, мережеве обладнання, мережева безпека, структурована кабельна система, оптимізація.

ABSTRACT

HURSKYI O. Development of a Local Computer Network for a Private Enterprise. – Manuscript.

Research for obtaining a bachelor's degree in specialty 126 «Information systems and technologies». – Lviv State University of Internal Affairs, MIA of Ukraine, Lviv, 2026.

The qualification work examines the issues of design, construction, and implementation of a modern local computer network for a private enterprise. The relevance of the topic is due to the rapid growth of information volumes, the need for efficient data exchange, and the improvement of productivity of modern enterprises through high-quality network infrastructure.

The work analyzes the requirements for network infrastructure, provides an overview of modern technologies and topologies of local area networks, structured cabling systems, active network equipment, and information security tools. A detailed IP addressing plan, a scheme of physical and logical device connections, and the organization of guest access have been developed. The proposed network is focused on effective support of business processes, simplicity of administration, protection of information, and flexibility for further infrastructure development.

Keywords: local area network, network design, network equipment, network security, structured cabling system, optimization.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DHCP – Dynamic Host Configuration Protocol – протокол динамічного призначення IP-адрес

FTP – File Transfer Protocol – протокол передавання файлів

IP – Internet Protocol – протокол Інтернету

LAN – Local Area Network – локальна мережа

MAC – Media Access Control – апаратна адреса мережевого пристрою

MAN – Metropolitan Area Network – міська мережа

NAS – Network Attached Storage – мережевий пристрій зберігання

NAT – Network Address Translation – трансляція мережевих адрес

OSI – Open Systems Interconnection – модель взаємодії відкритих систем

PAN – Personal Area Network – персональна мережа

QoS – Quality of Service – якість обслуговування трафіку RJ-45 – Registered

SIP – Session Initiation Protocol – протокол ініціації сеансу для IP-телефонії

СКС – Структурована кабельна система

STP – Shielded Twisted Pair – екранована вита пара

UPS – Uninterruptible Power Supply – джерело безперебійного живлення

UTP – Unshielded Twisted Pair – неекранована вита пара

VoIP – Voice over IP – передача голосу через IP-мережі

VPN – Virtual Private Network – віртуальна приватна мережа

WAN – Wide Area Network – глобальна мережа

Wi-Fi – Wireless Fidelity – бездротовий доступ до мережі

ВСТУП

Із розвитоком інформаційних технологій та цифровізацією бізнес-процесів перед сучасними підприємствами ставлять завдання створення ефективної, надійної та безпечної локальної комп'ютерної мережі. У сучасному офісі щоденна діяльність залежить від швидкого обміну документами, спільної роботи з файлами, доступу до спільних ресурсів та стабільного підключення до Інтернету. Відсутність якісної мережевої інфраструктури призводить до зниження продуктивності, простоїв у роботі та зростання ризиків втрати даних.

Сьогодні більшість приватних підприємств України використовують комп'ютерну техніку, мобільні пристрої та хмарні сервіси, що вимагає сучасної локальної мережі, здатної забезпечити високу швидкість передачі даних, сегментацію трафіку, централізоване управління та базовий рівень інформаційної безпеки. Особливо актуальним є питання раціонального поєднання дротової та бездротової інфраструктури з урахуванням обмеженого бюджету та відсутності постійного штатного IT-фахівця. Багато підприємств використовують хаотично побудовані мережі з недостатньою сегментацією, слабким захистом та обмеженими можливостями масштабування. Це призводить до вразливості до зовнішніх загроз, зниження продуктивності та складнощів при розширенні компанії.

Мета роботи – розробити та практично реалізувати сучасну локальну комп'ютерну мережу для приватного підприємства, офісу, яка забезпечує високу продуктивність, надійність, інформаційну безпеку та можливість подальшого масштабування.

Для досягнення поставленої мети визначено такі **завдання**:

- Проаналізувати вимоги до мережевої інфраструктури підприємства та огляд існуючих технологій локальних мереж.
- Обґрунтувати вибір оптимальної топології, структури та обладнання для

мережі.

- Розробити структурну схему мережі, план IP-адресації та сегментацію.
- Вибрати та обґрунтувати активне та пасивне мережеве обладнання.
- Реалізувати заходи інформаційної безпеки, включаючи ізоляцію гостьової мережі та централізоване управління.
- Провести тестування працездатності, продуктивності та стабільності спроєктованої мережі.

Об'єкт дослідження – процеси проєктування, побудови та експлуатації локальних комп'ютерних мереж у офісному середовищі приватних підприємств.

Предмет дослідження – методи, технології та технічні рішення для створення ефективної, безпечної та масштабовної локальної комп'ютерної мережі.

Методи досліджень Під час проєктування та реалізації локальної комп'ютерної мережі застосовано ряд загальноприйнятих методів наукового дослідження, які дозволили у повній мірі досягти мету кваліфікаційної роботи та вирішити поставлені завдання. Зокрема:

- бібліографічний та аналітичний методи дозволили провести огляд сучасних технологій локальних мереж, класифікацію мереж за територіальним охопленням, аналіз типових топологій та оцінку доступних мережевих рішень;
- методи аналізу та синтезу застосовано для вивчення вимог приватного підприємства, визначення оптимальної структурної схеми мережі, розробки плану IP-адресації та вибору обладнання;
- порівняльний метод використано при обґрунтуванні вибору активного обладнання , кабельної системи та порівнянні традиційних і сучасних підходів до побудови мереж;
- експериментальний метод реалізовано через практичне впровадження мережі, тестування продуктивності, моніторинг трафіку, затримок та перевірку заходів безпеки;

- методи моделювання та оптимізації забезпечили розробку масштабованого рішення, сегментації трафіку та резервування.

Практичне значення. Розроблена локальна комп'ютерна мережа може бути безпосередньо впроваджена в діяльність приватного підприємства. Результати роботи можуть використовуватися як типове рішення для подібних офісів, а також як навчальний матеріал для студентів.

Структура роботи. Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел. Обсяг основного тексту роботи складає 58 сторінок, 9 рисунків, 9 таблиць і 16 бібліографічних джерела. Загальний обсяг роботи – 66 сторінок.

РОЗДІЛ 1
АНАЛІЗ ВИМОГ, ОГЛЯД ТА АНАЛІЗ ТЕХНОЛОГІЙ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Характеристика приватного підприємства та аналіз потреб у мережевій інфраструктурі

Приватне підприємство – це форма бізнесу, що перебуває у власності однієї або кількох фізичних чи юридичних осіб і функціонує з метою отримання прибутку. Таке підприємство діє самостійно, без прямого державного управління, і несе повну відповідальність за результати своєї діяльності.

Приватні підприємства можуть бути різних розмірів – від мікробізнесу з одним засновником до великих компаній з сотнями працівників. Вони здійснюють різноманітну господарську діяльність: виробництво товарів, надання послуг, торгівлю, IT-розробки, сільське господарство чи консалтинг. Успішна робота сучасного приватного підприємства тісно пов'язана з використанням цифрових технологій, автоматизацією процесів, ефективним управлінням даними та застосуванням інформаційних технологій, зокрема – використанням комп'ютерної мережі для забезпечення зв'язку, обміну даними, спільної роботи над проектами та доступу до Інтернету.

У рамках роботи ми будемо розглядати проєктування та розробку локальної комп'ютерної мережі для офісного приміщення.

Сучасний офіс зазвичай включає кілька комп'ютерів, ноутбуків, багатофункціональних пристроїв (принтери, сканери), IP-телефони, мережеві сховища (NAS) та точки доступу Wi-Fi. Важливо враховувати, що значна частина співробітників працює з мобільних пристроїв або потребує тимчасового гостьового доступу до мережі. Крім того, в офісі можуть бути встановлені системи відеоспостереження та контролю доступу, які також потребують підключення до мережі.

Вимоги до мережевої інфраструктури визначаються специфікою бізнес-процесів, кількістю користувачів та рівнем навантаження. Основним завданням є забезпечення стабільної та безперервної доступності як внутрішніх, так і зовнішніх інформаційних ресурсів. Мережа повинна ефективно підтримувати передачу великих обсягів даних, швидкий обмін файлами, спільну роботу з документами, а також інтеграцію з корпоративними сервісами, такими як CRM-системи та хмарні платформи.

Не менш важливим є надійний і стабільний доступ до Інтернету для всіх користувачів.

Особливу увагу необхідно приділити безпеці даних та захисту мережі. Офісна мережа, як правило, поєднує внутрішній і гостьовий сегменти, тому важливо забезпечити ізоляцію гостьового Wi-Fi, захист від несанкціонованого доступу, контроль підключених пристроїв та користувачів. Також варто впроваджувати регулярне резервне копіювання даних і механізми їх відновлення у разі збоїв.

Ще однією ключовою вимогою є масштабованість мережі. Інфраструктура повинна дозволяти легко розширювати кількість користувачів, пристроїв та сервісів, а також переходити на нові, швидші стандарти без значних витрат і глобальної перебудови мережі. При цьому система адміністрування має залишатися простою та зручною, щоб нею могли ефективно користуватися навіть без постійної присутності окремого IT-фахівця.

Таким чином, основними вимогами до мережевої інфраструктури офісу є: висока доступність і продуктивність, надійна інформаційна безпека, масштабованість, простота обслуговування та оптимальне співвідношення вартості й функціональних можливостей. Саме з урахуванням цих факторів буде здійснюватися подальше проєктування ефективної локальної комп’ютерної мережі.

Щодо структури та функціонування мережі, побудова локальної комп’ютерної мережі офісу потребує чіткого визначення вимог до її

архітектури, функціональних можливостей та технічних параметрів. Від якості цих вимог безпосередньо залежить стабільність роботи, рівень безпеки, гнучкість та перспективи розвитку мережевої інфраструктури.

Насамперед мережа повинна забезпечувати надійний і безперервний зв’язок між усіма робочими станціями, серверами, мережевими принтерами, системами відеоспостереження, IP-телефонами та іншими пристроями. Важливо гарантувати постійний доступ до внутрішніх корпоративних ресурсів, а також до зовнішніх інформаційних систем, включаючи Інтернет і хмарні сервіси.

Мережа має ефективно справлятися з передачею великих обсягів даних із мінімальними затримками. Це особливо актуально для спільної роботи з документами, проведення відеоконференцій, використання CRM- та ERP-систем і виконання резервного копіювання. Для цього рекомендується впроваджувати гігабітні канали між ключовими вузлами, що забезпечить високу пропускну здатність і усуне можливі «вузькі місця».

Важливим критерієм є масштабованість мережі. Вона повинна дозволяти легко підключати нових користувачів, пристрої чи робочі зони без необхідності радикальної перебудови інфраструктури. Оптимальний вибір топології (найчастіше зіркоподібної або ієрархічної) забезпечує зручність адміністрування та гнучкість розширення. Усі кабельні та бездротові сегменти мають бути об’єднані в єдину логічну структуру з можливістю централізованого управління.

Окремої уваги потребує інформаційна безпека. Мережа повинна мати чітке розділення на внутрішній і гостьовий сегменти, підтримувати автентифікацію користувачів, розмежування прав доступу, фільтрацію трафіку та надійний захист від зовнішніх загроз. Необхідно передбачити ізоляцію гостьового Wi-Fi, використання сучасного брандмауера, регулярне оновлення ПЗ та застосування політик безпеки на кінцевих пристроях.

Фізична організація мережі має бути зручною для монтажу, подальшого обслуговування та модернізації. Рекомендується використовувати

структуровану кабельну систему з чітким маркуванням, оптимальним розташуванням телекомунікаційних шаф, зручним розміщенням розеток і резервуванням живлення критичних елементів.

Також важливо забезпечити простоту адміністрування та моніторингу мережі. Процеси конфігурації обладнання, підключення або відключення пристроїв мають бути максимально автоматизованими та інтуїтивно зрозумілими, навіть якщо в офісі немає постійного IT-фахівця. Використання сучасного обладнання з графічними інтерфейсами, системами журнлювання подій та можливістю віддаленого доступу значно спрощує технічну підтримку.

Врахування всіх перелічених вимог дає змогу створити мережеву інфраструктуру, яка повністю відповідатиме поточним і майбутнім потребам офісу, буде стійкою до збоїв, захищеною, зручною в обслуговуванні та готовою до масштабування.

1.2. Поняття комп’ютерної мережі, її призначення та загальні характеристики

Комп’ютерна мережа – це система взаємопов’язаних технічних пристроїв, які забезпечують обмін інформацією, спільне використання апаратних і програмних ресурсів, а також ефективну взаємодію між користувачами. З технічної точки зору, мережею вважається будь-яке середовище, де два або більше пристроїв можуть обмінюватися даними за допомогою відповідних протоколів зв’язку[1-5].

Головне завдання комп’ютерної мережі полягає в організації централізованого зберігання даних, спрощенні доступу до ресурсів, прискоренні обміну інформацією та автоматизації бізнес-процесів. Це дозволяє зменшити дублювання даних, полегшити адміністрування та знизити загальні витрати на утримання інфраструктури.

Комп’ютерні мережі класифікують за кількома ознаками: за географічним охопленням (локальні, міські, глобальні), за типом організації

(клієнт-серверні, однорангові), за фізичними та логічними топологіями, а також за способом передачі даних (пакетний, потоковий). Залежно від потреб організації, мережа може об’єднувати різні пристрої: персональні комп’ютери, сервери, принтери, точки доступу Wi-Fi, IP-телефони, системи відеоспостереження та багато іншого.

До ключових характеристик комп’ютерної мережі належать: масштабованість (можливість легкого розширення), надійність (стійкість до збоїв), безпека (захист від несанкціонованого доступу), продуктивність (швидкість передачі даних) та зручність адміністрування. Якісно спроєктована мережа повинна відповідати всім цим вимогам, особливо в умовах невеликого або середнього офісу, де часто відсутня окрема IT-служба.

Таким чином, комп’ютерна мережа є важливою складовою сучасного офісного середовища. Вона створює швидке, зручне та захищене простір для взаємодії працівників, підвищує ефективність роботи з даними та сприяє загальній оптимізації діяльності організації.

1.3. Класифікація комп’ютерних мереж за територіальним охопленням

Комп’ютерні мережі класифікуються за різними критеріями, серед яких одним із найважливіших є географічне (територіальне) охоплення. Від розмірів і просторового розташування мережевої інфраструктури залежить її структура, принципи побудови, обладнання, типи з’єднань і функціональні можливості.

Глобальні мережі (WAN) особливості та сфера застосування. Глобальна мережа, або WAN (Wide Area Network), – це тип комп’ютерної мережі, який охоплює великі географічні території: країни, континенти або навіть увесь світ. Головною метою такої мережі є забезпечення зв’язку між локальними мережами, розташованими на великій відстані одна від одної. Глобальні мережі дозволяють організаціям об’єднувати свої філії, офіси, склади чи виробничі майданчики в єдину інформаційну систему.

Особливістю WAN є її складна структура. На відміну від локальних

мереж, вона використовує орендовані або загальнодоступні комунікаційні лінії, зокрема волоконно-оптичні канали, супутниковий зв’язок, кабельні мережі, мікрохвильові або мобільні бездротові з’єднання. Передавання даних у таких мережах відбувається з використанням спеціалізованих протоколів маршрутизації, які дозволяють ефективно управляти трафіком у розподіленому середовищі.

У структурі WAN важливу роль відіграють маршрутизатори, комутатори магістрального рівня, міжмережеві екрани, проксі-сервери, шифрувальні шлюзи та інші пристрої, які забезпечують з’єднання між віддаленими ділянками мережі. Також часто використовуються VPN-технології, що дозволяють створювати захищені канали зв’язку поверх публічної мережі Інтернет.

Прикладами глобальних мереж є:

- Інтернет – найбільша у світі глобальна мережа, що об’єднує мільйони пристроїв і локальних мереж;
- Корпоративні мережі банків, логістичних компаній, міжнародних корпорацій, які мають офіси в різних країнах;
- Національні освітні або наукові мережі, що поєднують університети, дослідницькі центри та бібліотеки.

Попри очевидні переваги, глобальні мережі мають і свої обмеження. Зокрема, вони залежать від надійності каналів зв’язку, можуть мати високі затримки в передаванні даних, складніше адмініструються та вимагають серйозного підходу до інформаційної безпеки. Крім того, вартість оренди каналів зв’язку або використання спеціалізованих сервісів часто є доволі високою [1-9].

Отже, WAN є невід’ємною частиною сучасної інформаційної інфраструктури для великих організацій, що працюють у різних географічних регіонах. У контексті локальної мережі офісу глобальна мережа розглядається переважно як зовнішнє середовище – зокрема, у вигляді доступу до Інтернету або підключення до зовнішніх сервісів і хмарних

платформ.

Міські мережі (MAN) структура і типові рішення. Міська мережа, або MAN (Metropolitan Area Network), є проміжною ланкою між локальними (LAN) та глобальними (WAN) мережами. Вона охоплює більшу територію, ніж локальна мережа, але меншу, ніж глобальна
– зазвичай це межі одного великого міста або агломерації. MAN об'єднує декілька локальних мереж, розташованих у різних районах міста, у єдину інфраструктуру, яка дозволяє здійснювати обмін даними на високій швидкості.

Міські мережі часто використовуються великими організаціями з кількома офісами в межах одного населеного пункту. Завдяки MAN можливо централізовано керувати інформаційними ресурсами, забезпечувати доступ до внутрішніх сервісів та баз даних, синхронізувати документообіг та забезпечувати резервне копіювання між майданчиками. Такі мережі також активно застосовуються телекомунікаційними компаніями для надання послуг зв'язку кінцевим користувачам.

З технічної точки зору MAN будується на основі волоконно-оптичних ліній або радіорелейних з’єднань. Часто використовується топологія "кільце", що забезпечує високу надійність, оскільки при обриві одного сегмента трафік автоматично перенаправляється в інший бік кільця. На відміну від WAN, у MAN використовується власна інфраструктура, а не орендовані канали, що знижує витрати для великих операторів і дозволяє контролювати якість обслуговування [1-10].

У складі міських мереж функціонують маршрутизатори, мультиплексори, комутатори рівня ядра, сервери маршрутизації трафіку та обладнання для керування доступом користувачів. Пропускна здатність MAN зазвичай коливається в межах від сотень мегабіт до десятків гігабіт за секунду, що дає змогу обслуговувати тисячі абонентів і забезпечувати якісний обмін інформацією.

Прикладами використання MAN можуть бути:

- університетські кампуси, об’єднані в єдину освітню мережу в межах міста;
- Мережі органів місцевого самоврядування, що з’єднують адміністративні будівлі;
- інфраструктура кабельних операторів або провайдерів, що надають послуги Інтернет-доступу.

У контексті проєктування локальної мережі офісу міські мережі зазвичай відіграють роль зовнішнього середовища. Наприклад, через MAN-підключення офіс може отримати високошвидкісний доступ до Інтернету або бути частиною більшої корпоративної мережі, що охоплює всі підрозділи компанії в межах міста.

Персональні мережі (PAN) особливості впровадження. Персональні мережі, або PAN (Personal Area Network), – це найменший за охопленням тип комп’ютерних мереж, що створюється для забезпечення зв’язку між пристроями, які належать одній людині та розташовані в межах кількох метрів. Такі мережі призначені для організації швидкої та зручної взаємодії між пристроями в особистому користуванні без залучення зовнішніх інфраструктур або серверів.

До PAN зазвичай входять ноутбуки, смартфони, планшети, смарт-годинники, гарнітури, мишки, клавіатури, принтери та інші пристрої, що використовуються одним користувачем. Комунікація між ними найчастіше здійснюється за допомогою бездротових технологій – таких як Bluetooth, NFC (Near Field Communication), ІЧ-порт або Wi-Fi Direct. В окремих випадках PAN може також мати дротове з’єднання – наприклад, USB-інтерфейс між комп’ютером і зовнішнім накопичувачем.

Особливістю персональних мереж є їх простота, мобільність та автономність. PAN не потребує складного налаштування, централізованого адміністрування або використання зовнішнього обладнання – достатньо лише активувати відповідні інтерфейси зв’язку на пристроях. Завдяки цьому персональні мережі широко використовуються у повсякденному житті – для

передавання файлів між смартфоном і ноутбуком, синхронізації фітнес-даних, підключення бездротових навушників тощо.

Водночас PAN має обмежені функціональні можливості. Радіус дії такої мережі зазвичай не перевищує 10 метрів, швидкість обміну даними є нижчою порівняно з LAN або WAN, а кількість пристроїв, які можуть працювати одночасно, – обмежена. Крім того, бездротові персональні мережі потребують базових заходів безпеки: парного з'єднання, автентифікації, використання шифрування, щоб уникнути несанкціонованого доступу до особистих даних.

У межах проєктування мережі офісу персональні мережі можуть розглядатися як додатковий засіб для тимчасового підключення мобільних пристроїв працівників, передачі даних без використання спільних серверів або доступу до мережевого обладнання. Вони не є повноцінною частиною офісної LAN, але можуть працювати з нею паралельно – наприклад, у разі підключення смартфона до офісного Wi-Fi для обміну документами[1-10].

Отже, PAN – це компактна, особиста мережа короткого радіусу дії, яка виконує допоміжну роль і підвищує гнучкість використання цифрових пристроїв. Її використання є доцільним у тих випадках, коли необхідна швидка передача даних або синхронізація між індивідуальними пристроями користувача без використання сторонніх інструментів чи інтернет-з'єднання.

Локальні мережі (LAN) основні характеристики та переваги

Локальні комп'ютерні мережі, або LAN (Local Area Network), є найбільш поширеним типом мереж, який об'єднує комп'ютери, сервери, периферійні пристрої та інше обладнання в межах обмеженої географічної зони – наприклад, офісу, квартири, школи або окремого поверху будівлі.

Основною особливістю LAN є висока швидкість обміну даними та незначна затримка, що дозволяє забезпечити ефективну взаємодію між усіма учасниками мережі.

Типова локальна мережа містить мережеві пристрої, такі як маршрутизатори, комутатори, точки доступу, комп'ютери, принтери,

мережеві накопичувачі (NAS) тощо. Усі вони з’єднуються за допомогою структурованої кабельної системи або бездротових засобів зв’язку. LAN може бути побудована як на дротовій основі (Ethernet), так і бездротовій (Wi-Fi), або мати комбіновану структуру. У сучасних офісах дедалі частіше використовують гігабітні з’єднання, що забезпечують високу продуктивність при передачі великих обсягів даних.

Основні переваги локальних мереж полягають у простоті впровадження, низькій вартості обладнання, можливості гнучкої конфігурації та легкому адмініструванні. Завдяки LAN підприємство може централізувати управління документами, контролювати доступ до ресурсів, здійснювати колективне використання принтерів, сканерів, баз даних і програмного забезпечення. Локальні мережі також дозволяють розгортати внутрішні сервери, наприклад, файлові, поштові або сервери резервного копіювання.

Зазвичай LAN працює в межах одного або кількох приміщень і належить одній організації, що дає змогу повністю контролювати мережеву інфраструктуру. Це спрощує впровадження заходів безпеки, таких як використання фаєрволів, обмеження доступу, шифрування трафіку та моніторинг подій. LAN може бути основою для побудови більш складних систем, які згодом об’єднуються в MAN або WAN [1-10].

У контексті кваліфакаційної роботи локальна мережа розглядається як оптимальне рішення для офісу. Вона забезпечує швидкий обмін інформацією, стабільний зв’язок між усіма пристроями та дає можливість організувати надійне внутрішнє середовище для щоденної діяльності офісу без потреби в складній та дорогій інфраструктурі.

1.4. Огляд типових топологій локальних мереж

При проєктуванні локальної комп’ютерної мережі важливим етапом є вибір відповідної топології – способу фізичного або логічного з’єднання пристроїв у мережі. Від вибраної топології залежить ефективність роботи мережі, її надійність, простота розширення, складність обслуговування та

витрати на обладнання.

Топологія «шина» є однією з найстаріших і найпростіших форм організації комп'ютерної мережі, у якій усі пристрої (вузли) підключаються до одного спільного каналу передачі – лінії, яка виконує роль магістралі. Передавання даних у такій мережі здійснюється у вигляді широкомовних повідомлень: сигнал, що передається одним пристроєм, доступний усім іншим, але обробляється лише тим, кому він адресований. На кінцях кабелю обов'язково встановлюються термінатори – резистори, що поглинають сигнал і запобігають його відбиттю назад, яке може спричинити помилки у передаванні.

Однак сучасні умови експлуатації значно обмежують застосування шинної топології. Основним її недоліком є слабка масштабованість: зі зростанням кількості пристроїв зростає навантаження на спільний канал, що спричиняє зниження продуктивності, затримки в передаванні даних і підвищену ймовірність колізій (одночасна передача від кількох пристроїв). Крім того, вихід з ладу навіть одного кабелю або термінатора може призвести до повного порушення роботи всієї мережі.

Ще однією суттєвою проблемою є складність у діагностиці несправностей. У шині всі пристрої підключені послідовно, тому виявити точне місце обриву або пошкодження буває складно. Крім того, додавання нових вузлів вимагає переривання роботи всієї мережі, що є неприйнятним для більшості сучасних офісних середовищ [1-10].

Попри ці недоліки, топологія «шина» досі може застосовуватися у вузькоспеціалізованих системах – наприклад, у промислових мережах (RS-485), простих системах моніторингу або в середовищах, де мережа будується тимчасово й з мінімальними витратами. Порівняльна характеристика (табл. 1.1) дозволяє оцінити її основні переваги та недоліки у порівнянні з іншими популярними схемами побудови мереж.

Таблиця 1.1

Основні характеристики топології «шина»

Характеристика	Значення / Особливості
Тип передавання	Спільний кабель, широкомовна передача
Необхідність активного обладнання	Відсутня (лише термінатори)
Надійність	Низька (вразлива до обривів кабелю)
Виявлення помилок	Складне
Простота впровадження	Висока (мінімум обладнання)
Масштабованість	Обмежена (до 10–20 пристроїв без втрати
Вартість	Низька
Швидкість обміну	Залежить від навантаження, схильна до колізій
Підходить для	Тимчасові або прості малі мережі, навчальні цілі
Сучасність	Застаріла, практично не застосовується у сучасних

Таким чином, топологія «шина» хоча й має певні історичні переваги, на сьогодні є морально застарілою для широкого використання в корпоративних умовах. У сучасних локальних мережах її витіснили більш надійні та масштабовані структури – насамперед топологія «зірка», яка краще задовольняє вимоги до швидкості, безпеки, доступності й гнучкості.

Топологія «зірка» є найпоширенішим варіантом побудови локальних комп’ютерних мереж у сучасних офісах, навчальних закладах, малих підприємствах та будинках. У цій топології всі пристрої (вузли мережі) підключаються до одного центрального елемента – зазвичай це комутатор (switch) або маршрутизатор (router), який виконує функції розподілу трафіку між учасниками мережі.

Передавання даних у мережі зі структурою «зірка» здійснюється через центральний вузол: коли один пристрій передає дані іншому, ці дані спочатку надходять до центрального комутатора, який вирішує, куди їх направити. Такий принцип дозволяє чітко контролювати маршрути трафіку та мінімізувати кількість колізій у мережі.

Головною перевагою цієї топології є висока надійність. Вихід з ладу

одного кабелю або пристрою не призводить до зупинки роботи всієї мережі – лише конкретного вузла. Це суттєво спрощує обслуговування та діагностику несправностей: адміністратор може швидко визначити джерело проблеми й ізолювати його, не впливаючи на інші частини інфраструктури.

Іншою важливою перевагою є гнучкість у масштабуванні. У разі потреби додати новий пристрій достатньо просто прокласти окремий кабель до комутатора – це не потребує перебудови мережі. Така гнучкість робить «зірку» ідеальною для умов офісу, де можливе поступове зростання кількості співробітників або розширення функціоналу мережі.

Таблиця 1.2

Основні характеристики топології «зірка»

Характеристика	Значення / Особливості
Тип передавання	Через центральний вузол (switch/router)
Необхідність активного обладнання	Обов’язкова (комутатор або маршрутизатор)
Надійність	Висока (вихід з ладу одного вузла не впливає на інших)
Виявлення помилок	Просте (ізольовані лінії зв’язку)
Простота впровадження	Середня (потрібна СКС і планування центральної точки)
Масштабованість	Висока (можна легко додавати нові пристрої)
Вартість	Вища, ніж у «шини» (через додаткове обладнання та кабелі)
Швидкість обміну	Висока, особливо при використанні Gigabit Ethernet
Підходить для	Офіси, підприємства, навчальні заклади, квартири
Сучасність	Найбільш актуальна та рекомендована для локальних мереж

До недоліків топології «зірка» можна віднести залежність від

центрального вузла. Якщо виходить з ладу комутатор або маршрутизатор, вся мережа стає непрацездатною. Тому важливо обирати надійне обладнання, забезпечувати його стабільне живлення та резервування. Порівняльна характеристика (табл. 1.2) дозволяє оцінити її основні переваги та недоліки у порівнянні з іншими популярними схемами побудови мереж [1-10].

Фізична реалізація цієї топології передбачає розгалужену структуровану кабельну систему, в якій кожен пристрій підключається окремим кабелем до телекомунікаційної шафи або точки комутації. Для невеликих офісів, де кількість пристроїв не перевищує 10–20, така схема є економічно доцільною та легкою в адмініструванні.

Таким чином, топологія «зірка» поєднує у собі простоту експлуатації, високий рівень стабільності, легкість масштабування та добру адаптацію до потреб офісу. Вона є рекомендованим рішенням у більшості практичних випадків побудови сучасних локальних мереж.

Топологія «кільце» передбачає таку організацію мережі, при якій кожен пристрій з’єднується з двома іншими, утворюючи замкнене коло. Дані передаються по кільцю від одного вузла до іншого в одному визначеному напрямку (односторонньо або двосторонньо – залежно від реалізації), доки не досягнуть адресата. У кожному вузлі може бути вбудований повторювач сигналу, який допомагає підтримувати якість передачі на великих відстанях.

Ключовою особливістю такої структури є послідовний маршрут передавання даних – усі пакети проходять через проміжні вузли. Це дозволяє забезпечити стабільне навантаження на мережу, уникати широкомовних штормів і мати передбачуваний час доставки. У деяких реалізаціях кільця використовуються механізми маркерного доступу (token passing), які запобігають колізіям, оскільки лише вузол із маркером має право передавати дані.

Серед переваг топології «кільце» варто зазначити збалансоване використання смуги пропускання, відсутність широкомовного шуму та підтримку гарантованої доставки. Однак структура має й серйозні

обмеження. Найбільш критичним є те, що вихід з ладу будь-якого вузла або порушення ланки розриває кільце, що паралізує всю мережу. Для підвищення надійності іноді реалізується подвійне кільце (Dual Ring), де сигнал може передаватися в протилежному напрямку, але це значно ускладнює і здорожчує реалізацію.

Таблиця 1.3

Основні характеристики топології «кільце»

Характеристика	Значення / Особливості
Тип передавання	Послідовно, по замкненому кільцю
Необхідність активного обладнання	Варіативно (можуть бути повторювачі або концентратори)
Надійність	Низька без резервування, висока при подвійному кільці
Виявлення помилок	Складне, особливо в разі аналогової реалізації
Простота впровадження	Середня, залежить від кількості вузлів
Масштабованість	Обмежена: додавання вузлів вимагає переривання кільця
Вартість	Вища за «шину», нижча за повну «сітку»
Швидкість обміну	Стабільна, особливо за наявності маркерного доступу
Підходить для	Промислові мережі, транспортні кільцеві канали, старі системи
Сучасність	Застаріла для офісів, використовується у спеціалізованих сферах

Діагностика несправностей у кільцевій мережі є складнішою, ніж у «зірці», особливо в аналогових реалізаціях без активного обладнання. Кожен вузол виконує роль транзитного пункту, тому навіть тимчасова втрата зв’язку одного пристрою призводить до порушення мережевої цілісності. Через це в умовах сучасних офісів топологія «кільце» майже не використовується, поступившись більш гнучким і надійним рішенням. Порівняльна

характеристика (табл. 1.3) дозволяє оцінити її основні переваги та недоліки у порівнянні з іншими популярними схемами побудови мереж [1-10].

Історично така структура активно використовувалася в мережах Token Ring (IBM), а також у деяких промислових і телекомунікаційних рішеннях, де потрібна передбачувана затримка. Сьогодні вона частіше зустрічається в оптоволоконних транспортних мережах або в замкнених сегментах систем відеоспостереження.

У контексті локальної мережі офісу використання топології «кільце» недоцільне через її уразливість до збоїв, складність модернізації та обмежену гнучкість. Натомість більш ефективними є сучасні реалізації з топологією «зірка», які краще підходять до вимог стабільності, безпеки та простоти обслуговування.

Топологія «дерево» – це ієрархічна структура побудови мережі, яка поєднує в собі риси топологій «зірка» та «шина». Вона передбачає організацію мережі у вигляді розгалуженої структури, де декілька локальних сегментів, зібраних за принципом «зірки», під'єднуються до центрального магістрального вузла або верхнього рівня. Таким чином, утворюється деревоподібна ієрархія, де кожен рівень підключений до вищого через комутаційне обладнання.

Кожна гілка дерева може виступати як самостійний сегмент з окремим комутатором, до якого підключені кінцеві пристрої: комп'ютери, принтери, точки доступу тощо. Ці гілки потім підключаються до центрального вузла або магістрального комутатора. Така організація дозволяє легко масштабувати мережу: у разі необхідності додавання нових пристроїв достатньо приєднати нову гілку до відповідного рівня дерева.

Головною перевагою цієї топології є висока масштабованість. Завдяки ієрархічній побудові, адміністратор може логічно розділити мережу на окремі зони (відділи, поверхи, зали), які керуються незалежно. Це спрощує управління мережею та дає змогу ізолювати трафік певних сегментів. Крім того, кожен сегмент може працювати автономно – у межах свого вузла –

навіть якщо інші частини мережі мають проблеми.

Таблиця 1.4

Основні характеристики топологія «дерево»

Характеристика	Значення / Особливості
Тип передавання	Ієрархічна структура, через рівні комутаторів
Необхідність активного обладнання	Обов’язкова (на кожному рівні)
Надійність	Середня, залежить від резервування магістрального
Виявлення помилок	Відносно проста у локальних гілках
Простота впровадження	Складніша, ніж у «зірці» через планування ієрархії
Масштабованість	Висока (зручне додавання нових сегментів)
Вартість	Середня або висока (залежить від розміру мережі та
Швидкість обміну	Висока у межах гілки, можлива затримка через вузли вищого рівня
Підходить для	Університети, великі офіси, будівлі з багатьма зонами або поверхами
Сучасність	Актуальна і широко використовується в середніх і великих мережах

Однак у структурі «дерево» є й суттєвий недолік – залежність від вузлів вищого рівня. Вихід з ладу центрального комутатора або магістрального каналу може порушити роботу цілих підмереж. Тому в критичних інфраструктурах використовують резервування основних ліній або відмовостійке обладнання з двома живленнями та захистом від збоїв.

Топологія «дерево» є ефективною для середніх і великих організацій, де необхідно з’єднати в єдину систему багато локальних мереж. Вона застосовується в університетах, багатоповерхових офісах, супермаркетах, медичних установах, де структура мережі повинна відповідати фізичній або функціональній структурі об’єкта. Порівняльна характеристика (табл. 1.4)

дозволяє оцінити її основні переваги та недоліки у порівнянні з іншими популярними схемами побудови мереж [1-10].

Таким чином, топологія «дерево» є універсальним рішенням для побудови складних і структурованих мереж. Вона дозволяє логічно впорядкувати мережу, легко її масштабувати та управляти окремими сегментами. Проте для її успішної реалізації потрібне ретельне планування, особливо з урахуванням резервування ключових вузлів.

Топологія «сітка» – це структура побудови мережі, за якої кожен вузол підключається безпосередньо до кількох або до всіх інших вузлів. Така схема створює численні маршрути для передавання даних між пристроями, що значно підвищує надійність і відмовостійкість мережі. Існують два основні типи сітчастої топології: повна сітка (full mesh), де кожен вузол має пряме з’єднання з усіма іншими, та часткова сітка (partial mesh), де лише деякі вузли мають прямі з’єднання, а решта з’єднані через проміжні вузли.

Головною перевагою топології «сітка» є її надзвичайна стійкість до збоїв. Якщо одна або навіть кілька ліній зв’язку перестають працювати, дані автоматично маршрутизуються через інші доступні шляхи. Це особливо важливо для критичних систем, де втрата зв’язку може мати серйозні наслідки: наприклад, у банках, медичних установах, системах відеонагляду, військових об’єктах або центрах обробки даних.

Сітчаста структура також дозволяє ефективно балансувати навантаження, розподіляючи трафік по декількох каналах. У повній сітці досягається максимальна пропускна здатність, адже кожен пристрій має незалежний канал до решти, що виключає вузькі місця. Проте така реалізація вимагає великої кількості кабелів і портів, що суттєво ускладнює монтаж, підвищує витрати й вимагає складного управління мережею.

Часткова сітка являє собою компромісний варіант порівняно з повною сіткою, поєднуючи переваги високої надійності з економічною доцільністю впровадження. Така топологія передбачає, що лише частина вузлів мережі має резервні з’єднання між собою, тоді як інші пристрої підключаються за

допомогою простіших схем, наприклад, «зірка» або «дерево». Завдяки цьому суттєво зменшуються витрати на прокладання ліній зв’язку без значної втрати відмовостійкості мережі. Порівняльна характеристика (табл. 1.5) дозволяє оцінити її основні переваги та недоліки у порівнянні з іншими популярними схемами побудови мереж [1-10].

В умовах офісу повна сітчаста топологія використовується дуже рідко через свою складність і надмірність. Водночас часткові елементи сітки – наприклад, резервне з’єднання між двома комутаторами або додатковий маршрут до сервера – можуть бути цілком виправданими для підвищення надійності.

Таблиця 1.5

Основні характеристики топології «сітка»

Характеристика	Значення / Особливості
Тип передавання	Множинні з’єднання між вузлами, кілька маршрутів
Необхідність активного обладнання	Висока (особливо у повній сітці)
Надійність	Дуже висока, за рахунок резервування каналів
Виявлення помилок	Просте: ізоляція пошкодженого вузла не порушує загальну мережу
Простота	Низька у повній сітці, середня у частковій
Масштабованість	Обмежена через різке зростання кількості з’єднань при додаванні вузлів
Вартість	Дуже висока у повній сітці (кабелі, порти,
Швидкість обміну	Висока, навантаження розподіляється між кількома каналами

Таким чином, сітчаста топологія є надзвичайно надійним і потужним рішенням для специфічних завдань, де безперервність передавання даних критично важлива. У межах малих офісів повна реалізація такої схеми є надмірною, проте окремі елементи сітки можуть використовуватися для

підвищення відмовостійкості ключових вузлів мережі.

1.5. Software-Defined Networking та хмарні рішення в сучасних локальниї мережах

Software-Defined Networking (SDN) – це сучасна парадигма побудови комп'ютерних мереж, при якій управління мережевим трафіком відділяється від апаратного забезпечення та реалізується через програмне забезпечення. У традиційних мережах кожний комутатор або маршрутизатор самостійно приймає рішення щодо маршрутизації пакетів. У SDN ці рішення приймає централізований контролер, який має повне уявлення про всю мережеву інфраструктуру.

Основна ідея SDN полягає в розділенні плоскостей управління:

Data Plane (площина даних) – безпосереднє пересилання пакетів обладнанням;

Control Plane (площина управління) – централізоване програмне керування.

Таке відокремлення дозволяє динамічно конфігурувати мережу, швидко реагувати на зміни та автоматизувати процеси адміністрування.

Класична архітектура SDN складається з трьох рівнів:

Інфраструктурний рівень – фізичне та віртуальне мережеве обладнання (комутатори, точки доступу, маршрутизатори).

Рівень керування – SDN-контролер (наприклад, OpenDaylight, ONOS, Ubiquiti UniFi Network Application).

Рівень додатків – бізнес-додатки, системи моніторингу, політики безпеки, оркестратори.

Для взаємодії між рівнями використовуються стандартизовані протоколи:

OpenFlow – основний протокол для комунікації контролера з комутаторами;

NETCONF, REST API, SNMP – для конфігурації обладнання.

Переваги SDN:

- Централізоване управління всією мережею з єдиної панелі;
- Висока гнучкість та швидкість внесення змін;
- Автоматизація рутинних операцій (provisioning, VLAN-конфігурація, QoS);
- Поліпшена інформаційна безпека завдяки централізованим політикам;
- Краща масштабованість та підтримка віртуалізації;
- Економія ресурсів завдяки оптимізації трафіку.

Недоліки SDN:

- Залежність від надійності контролера (single point of failure);
- Потреба в обладнанні з підтримкою SDN-протоколів;
- Вищі вимоги до кваліфікації адміністраторів;
- Можливі проблеми сумісності з legacy-обладнанням.

Хмарні мережеві рішення (Cloud-Managed Networking). Хмарні рішення є логічним розвитком SDN. У них контролер розміщується не локально, а в хмарі провайдера. Це дозволяє керувати мережею з будь-якої точки світу через веб-інтерфейс або мобільний додаток.

Ubiquiti UniFi – одна з найпопулярніших для малого та середнього бізнесу. Підтримка Wi-Fi 7, централізоване управління, хмарний доступ.

Cisco Meraki – лідер enterprise-сегменту з потужними інструментами аналітики та безпеки.

TP-Link Omada SDN – бюджетне, але функціональне рішення.

Aruba Central, ExtremeCloud IQ, Fortinet FortiManager.

Переваги хмарних рішень:

- Відсутність необхідності у потужному локальному сервері для контролера;
- Автоматичні оновлення прошивок;
- Вбудована аналітика та штучний інтелект (AI-driven insights);
- Просте масштабування (додавання нових точок доступу одним кліком);
- Високий рівень безпеки (Zero-Touch Provisioning, автоматична

сегментація).

- Порівняння традиційного та SDN-підходу

Таблиця 1.6

Порівняння традиційних мереж та SDN

Характеристика	**Традиційна мережа**	**SDN / Хмарне рішення**
Управління	Децентралізоване	Централізоване
Швидкість внесення змін	Низька	Висока (автоматизація)
Масштабованість	Середня	Висока
Складність адміністрування	Висока	Низька
Рівень безпеки	Залежить від конфігурації	Високий (централізовані політики)
Вартість володіння (TCO)	Нижча на старті	Нижча в перспективі 3–5 років
Підтримка Wi-Fi 6/7	Обмежена	Повна

Для офісу хмарні SDN-рішення є оптимальним вибором. Вони дозволяють:

- Швидко розгортати мережу без глибоких знань мережевого адміністрування;
- Легко організовувати гостьовий Wi-Fi з ізоляцією;
- Налаштовувати VLAN (корпоративний, гостьовий, VoIP, IoT);
- Моніторити навантаження та продуктивність у реальному часі;
- Автоматично застосовувати політики безпеки.

У межах даного проєкту рекомендується використовувати екосистему Ubiquiti UniFi як найбільш збалансоване рішення за співвідношенням ціна/якість/функціональність. Вона поєднує сучасний SDN-підхід з простотою використання, що ідеально відповідає потребам офісу.

Software-Defined Networking та хмарні мережеві рішення представляють сучасний етап розвитку мережевих технологій. Вони дозволяють перейти від ручного налаштування окремих пристроїв до програмного, гнучкого та централізованого управління всією інфраструктурою.

Використання SDN і хмарних платформ у проєкті локальної мережі

офісу забезпечує не тільки поточні потреби, але й створює надійний фундамент для подальшого масштабування, інтеграції хмарних сервісів та впровадження сучасних технологій інформаційної безпеки.

РОЗДІЛ 2
ФІЗИЧНА РЕАЛІЗАЦІЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1. Вимоги до фізичної інфраструктури офісу

Якісна організація фізичної інфраструктури є фундаментальною основою стабільної та продуктивної роботи локальної комп'ютерної мережі в офісі. Усі етапи створення мережі – від вибору місця для обладнання до прокладання кабелів – мають враховувати не тільки технічні параметри пристроїв, а й особливості самого офісного приміщення.

Насамперед приміщення для мережевого обладнання повинно відповідати санітарним, технічним та експлуатаційним нормам. У ньому необхідно підтримувати стабільну температуру, оптимальний рівень вологості та достатню вентиляцію. Перегрів активного обладнання (маршрутизаторів, комутаторів, серверів, NAS) суттєво знижує продуктивність і скорочує термін його служби, тому обладнання не можна розміщувати біля джерел тепла чи під прямим сонячним світлом. Водночас доступ до обладнання має бути обмежений для сторонніх осіб, але зручний для спеціалістів, які проводять обслуговування та профілактику.

Критично важливим є забезпечення надійного електроживлення. Для мережевих пристроїв бажано використовувати окрему електролінію з заземленням і захисними автоматами. Найважливіші елементи інфраструктури рекомендується підключати до джерел безперебійного живлення (UPS). Це захищає мережу від раптових відключень електроенергії та перепадів напруги, що особливо важливо для серверів і систем зберігання даних. Додаткову надійність забезпечує резервування живлення та регулярна перевірка працездатності UPS.

Особливу увагу потрібно приділити прокладанню кабельної системи. Кабелі слід розміщувати в спеціальних кабель-каналах, під фальшпідлогою або в стінах, використовуючи надійні кріплення. Категорично заборонено

прокладати їх поряд із силовими електрокабелями, щоб уникнути електромагнітних перешкод. Кабелі не повинні бути відкритими або знаходитися в зонах ризику механічного пошкодження. Всі з’єднання та лінії необхідно чітко маркувати для спрощення подальшого обслуговування та модернізації.

Не менш важливим є дотримання норм електробезпеки та пожежної безпеки. Монтажні роботи повинні виконуватися із сертифікованих матеріалів з урахуванням усіх вимог безпеки. Телекомунікаційна шафа або серверна зона має бути обладнана пожежною сигналізацією та первинними засобами пожежогасіння.

Загалом, фізична інфраструктура офісу повинна бути спроєктована так, щоб забезпечити зручний доступ до обладнання, можливість швидкого розширення мережі, надійний захист від несанкціонованого доступу та негативних зовнішніх факторів. Комплексний підхід до організації фізичного середовища гарантує високу надійність, безпеку та гнучкість локальної комп’ютерної мережі, що є запорукою ефективної роботи всього офісу.

2.2. Середовище передавання даних та вибір кабельної системи

Вибір оптимального середовища передавання даних та кабельної системи є одним із найважливіших етапів проєктування локальної комп’ютерної мережі офісу. Саме ці компоненти визначають швидкість, надійність і масштабованість мережевої інфраструктури, а також можливість її подальшої модернізації.

У сучасних офісах для створення фізичних з’єднань між пристроями переважно використовують дротові рішення, оскільки вони забезпечують найкращу якість сигналу, мінімальні затримки та максимальну пропускну здатність. Основними типами кабельних середовищ є мідна вита пара (UTP/STP), коаксіальний кабель та оптоволоконний кабель. Кожен із цих типів має свої переваги й недоліки, проте для офісу найбільш доцільним є використання витої пари категорії 6A.

Вита пара категорії 6A (Cat 6) стала стандартом для офісних мереж завдяки своїй високій пропускній здатності стійкості до перешкод і простоті монтажу. Така кабельна система дозволяє об’єднати робочі місця, сервери, мережеві пристрої, IP-телефони та точки доступу Wi-Fi в єдину інфраструктуру з централізованим керуванням. Важливим аспектом є дотримання вимог щодо максимальної довжини каналу (до 100 метрів) для уникнення втрат сигналу.

Альтернативою може бути використання екранованої витої пари (STP), яка додатково захищає дані від електромагнітних завад, особливо якщо кабелі прокладаються поблизу силових ліній або промислового обладнання. Проте у більшості сучасних офісів цілком достатньо якісної неекранованої витої пари (UTP) зі строгим дотриманням стандартів прокладання.

Оптоволоконні кабелі забезпечують ще більшу швидкість та відстань передавання, а також повний імунітет до електромагнітних перешкод, однак їх застосування в малих офісах є малодоцільним через високу вартість обладнання, складність монтажу та надмірну для невеликої кількості пристроїв пропускну здатність. Зазвичай оптика використовується для магістральних ліній між будівлями або серверними.

Бездротове середовище (Wi-Fi) виступає як доповнення до основної дротової мережі. Воно забезпечує мобільність для ноутбуків, смартфонів і гостьових пристроїв, проте не може замінити кабельну систему в задачах, що вимагають стабільної високої швидкості та мінімальних затримок, наприклад, при роботі з великими файлами чи голосовим трафіком. Для організації Wi-Fi-зони у межах офісу використовуються точки доступу, які підключаються до дротової мережі через окремий порт комутатора або маршрутизатора.

Вибір конкретної структури кабельної системи для офісу передбачає створення структурованої кабельної системи (СКС), що складається з основних магістральних ліній, робочих розеток (RJ-45), патч- панелей, комутаційних шнурів та монтажних коробів. Правильне планування СКС

дозволяє забезпечити зручне підключення всіх необхідних пристроїв, уникнути хаосу в розташуванні кабелів, спростити технічне обслуговування та забезпечити можливість розширення мережі в майбутньому.

В результаті, основна частина мережевого трафіку в офісі має передаватися через виту пару категорії 6А, а бездротові технології – використовуватись як додатковий інструмент для забезпечення мобільності та гостьового доступу. Такий підхід дозволяє досягти оптимального балансу між вартістю впровадження, продуктивністю та зручністю експлуатації мережі. Нижче (таблиця 2.1) приведено порівняльну характеристику основних типів кабелів, що застосовуються для побудови локальних комп'ютерних мереж.

Таблиця 2.1

Порівняльна характеристика видів проводів

Тип кабелю	Пропускна здатність	Максимальна відстань	Захищеність від завад	Вартість	Складність монтажу	Сфера застосування
Вита пара (UTP Cat 6)	До 1 Гбіт/с (10 Гбіт/с на <55 м)	До 100 м	Середня	Низька	Низька	Невеликі офіси, квартири, навчальні заклади
Вита пара (UTP/STP Cat 6A)	До 10 Гбіт/с	До 100 м	Висока	Середня	Середня	Сучасні офіси, корпоративні мережі
Вита пара (Cat 8)	До 40 Гбіт/с	До 30 м	Дуже висока	Висока	Середня	Дата-центри, серверні, високопродуктивні робочі місця
Коаксіальний кабель	До 10 Гбіт/с (рідко)	До 500 м	Висока	Середня	Середня	Відеоспостереження, застарілі системи
Оптоволоконний кабель (Multi-mode)	До 100 Гбіт/с+	До 550 м	Дуже висока (імунітет)	Висока	Висока	Магістральні лінії, серверні, міжбудинкові з'єднання
Оптоволоконний кабель (Single-mode)	До 400 Гбіт/с+	Кілька кілометрів	Дуже висока (імунітет)	Висока	Висока	Великі корпоративні мережі, провайдери

Аналізуючи наведені в таблиці характеристики основних типів кабелів, можна зробити висновок, що для побудови локальної комп'ютерної мережі офісу оптимальним рішенням є використання витої пари категорії 6 (UTP або STP).

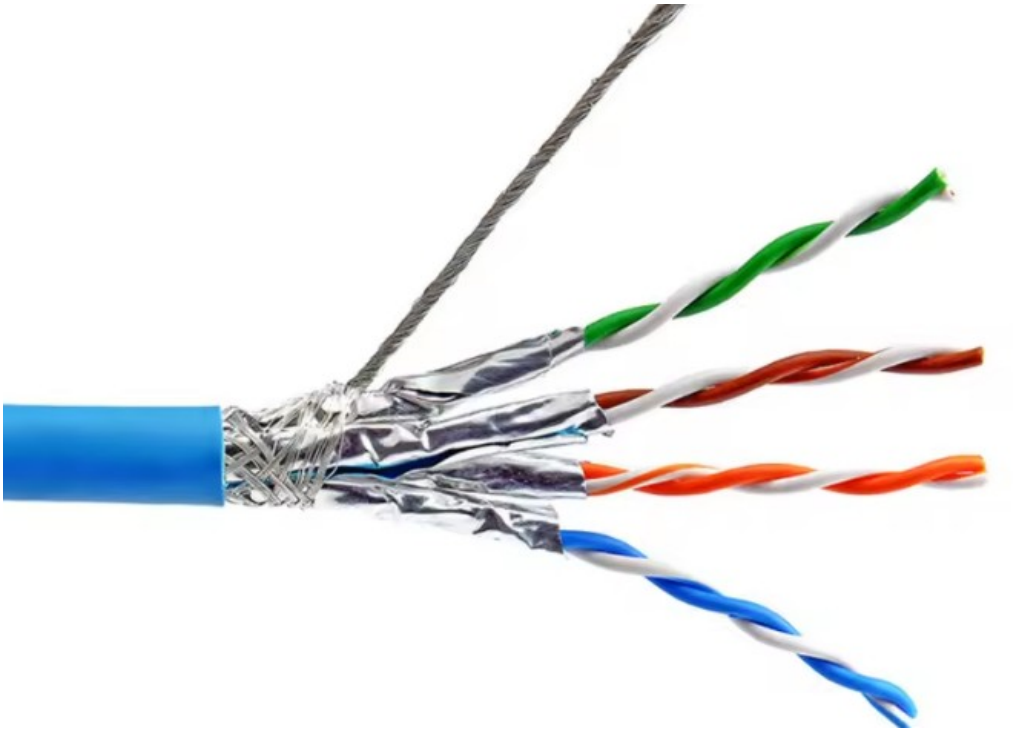

Рис. 2.1. Вита пара Cat6A для простих офісних з'єднань

Такий кабель забезпечує необхідну пропускну здатність для сучасних офісних завдань, має достатній рівень захисту від електромагнітних завад (особливо у виконанні STP), відзначається невисокою вартістю та простотою монтажу. Це робить його найбільш розповсюдженим і практичним вибором для невеликих офісних приміщень. В пстанні роки поширеними стали вита пара Cat6A – для простих офісних з'єднань із пропускною здатністю 1 Гбіт/с або навіть вище.

Оптоволоконний кабель значно перевищує UTP/STP за швидкістю і дальністю передавання, але його використання економічно доцільне лише для магістральних з'єднань або серверних, де потрібна максимальна пропускна здатність і захист від зовнішніх впливів. Коаксіальний кабель сьогодні майже не застосовується для нових офісних мереж через обмежену

швидкість і застарілість технології, однак може зустрічатися у спеціалізованих сферах, наприклад, у системах відеоспостереження.

Таким чином, вита пара категорії 6А поєднує в собі баланс між продуктивністю, вартістю та гнучкістю використання, що повністю відповідає завданням локальної мережі офісу.

2.3 Побудова дротової та бездротової інфраструктури

Після вибору кабельної системи наступним етапом є організація дротової та бездротової інфраструктури, які разом формують єдине інформаційне середовище офісу. Від правильного планування і реалізації цього етапу залежать надійність, масштабованість та зручність подальшої експлуатації мережі.

Дротова інфраструктура є основою для передавання основної маси даних між пристроями мережі. Для офісу зазвичай використовується структурована кабельна система на базі витої пари категорії 6, яка прокладається від центральної телекомунікаційної шафи (де розташовані маршрутизатор і комутатор) до всіх робочих місць, серверного обладнання IP-телефонів, мережевих принтерів та інших стаціонарних пристроїв. Кабелі розміщуються у пластикових кабель-каналах, під фальшпідлогою чи всередині стін, із дотриманням радіусів вигину й маркуванням кожної лінії для полегшення обслуговування та діагностики. На робочих місцях встановлюються мережеві розетки RJ-45, які дозволяють швидко і зручно підключати кінцеві пристрої.

Додаткову увагу приділяють комутаційній шафі або технічній зоні – саме тут зосереджуються активні пристрої (маршрутизатор, комутатор, NAS, джерело безперебійного живлення). Важливо забезпечити зручний доступ для обслуговування, якісну вентиляцію, електроживлення з резервуванням та захист від несанкціонованого доступу.

Бездротова інфраструктура, або Wi-Fi-мережа, служить доповненням до дротової і забезпечує мобільність для користувачів із ноутбуками,

смартфонами, планшетами та IoT-пристроями. Для цього встановлюється одна або кілька точок доступу (access point), які підключаються до основної дротової мережі через комутатор або маршрутизатор. Вибір місця встановлення точки доступу має враховувати розташування офісних перегородок, меблів та інших об’єктів, які можуть екранувати сигнал. Оптимально розмістити точку доступу так, щоб забезпечити рівномірне покриття усіх робочих зон без «мертвих зон» та з мінімальними перешкодами.

У налаштуваннях Wi-Fi-мережі рекомендується створювати окремі сегменти для службових пристроїв і для гостьового доступу. Це дозволяє підвищити безпеку офісної мережі й уникнути несанкціонованого доступу до критичних ресурсів. Використання сучасних стандартів Wi-Fi 6A дозволяє отримати високу швидкість передавання даних і стабільність з’єднання навіть за значної кількості одночасних підключень.

Для живлення точок доступу часто застосовується технологія Power over Ethernet (PoE), що дозволяє подавати живлення та дані по одному кабелю, спрощуючи монтаж і розміщення обладнання в оптимальних місцях.

Таким чином, побудова дротової та бездротової інфраструктури забезпечує надійну та швидку передачу даних між усіма пристроями офісу, сприяє підвищенню продуктивності праці, дозволяє швидко масштабувати мережу у разі потреби та гарантує зручність експлуатації для користувачів різних категорій.

2.4 Встановлення та інтеграція активного мережевого обладнання

Після завершення прокладання кабельної інфраструктури наступним етапом є встановлення активних мережевих пристроїв, які забезпечують логіку функціонування мережі, обробку та маршрутизацію трафіку, доступ до зовнішніх ресурсів і організацію внутрішніх сервісів.

Для офісу доцільним є використання універсального маршрутизатора, який поєднує функції маршрутизатора, комутатора, брандмауера та точки

доступу Wi-Fi. Такий підхід дозволяє зменшити кількість пристроїв, спростити адміністрування та знизити витрати на обладнання.

Розміщення маршрутизатора здійснюється у центральному комутаційному вузлі – в телекомунікаційній шафі або в безпечному місці з належним доступом до електроживлення. Усі дротові пристрої (ПК, NAS, IP-телефони) підключаються до портів LAN, а з'єднання з Інтернетом здійснюється через WAN-порт. Для розширення кількості портів може бути використано окремий комутатор, що підключається до одного з LAN-портів маршрутизатора.

Wi-Fi-точка доступу встановлюється таким чином, щоб забезпечити рівномірне покриття всіх офісних приміщень. У разі потреби точка доступу підключається до PoE-комутатора або живиться окремим адаптером. У налаштуваннях рекомендується створити окремі сегменти для службового і гостьового трафіку.

NAS-сервер підключається безпосередньо до комутатора абомаршрутизатора та отримує статичну IP-адресу. На ньому налаштовуються мережеві спільні папки з відповідними правами доступу для співробітників. Окремі робочі станції також можуть бути підключені до мережі за допомогою Wi-Fi або Ethernet, залежно від їхнього розташування.

Завершальним етапом є конфігурація логіки взаємодії між пристроями, присвоєння IP-адрес (статичних або через DHCP), а також налаштування мережевої безпеки – паролів, фільтрації, сегментації трафіку. Усі пристрої бажано підключити до джерела безперебійного живлення (UPS), щоб забезпечити стабільність роботи в разі короткочасного зникнення електроенергії.

Таким чином, інтеграція активного обладнання дозволяє повноцінно реалізувати функціонування локальної мережі та забезпечити всі потреби офісу в надійній цифровій інфраструктурі.

РОЗДІЛ 3
РОЗРОБКА ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Процес розробки локальної комп'ютерної мережі підприємства охоплює декілька послідовних етапів – від вибору оптимальної топології та визначення вимог до інфраструктури до підбору активного обладнання, проектування схеми підключень, розробки плану IP-адресації та впровадження заходів інформаційної безпеки.

У результаті проведеного аналізу було визначено, що найбільш раціональною для офісу є топологія типу «зірка» (рис. 4.1), яка забезпечує простоту адміністрування, гнучкість у розширенні та високу відмовостійкість. Центральним вузлом мережі виступає керований гігабітний комутатор, до якого підключаються всі робочі станції, сервери, точки доступу Wi-Fi, NAS-сервери та IP-телефони. Для організації доступу до Інтернету, а також для маршрутизації трафіку між різними сегментами мережі використовується сучасний маршрутизатор із функціями фаєрволу, підтримкою VLAN та сервісів резервування.

Важливим етапом проектування стало формування детальної схеми фізичних та логічних підключень. Передбачено окремі сегменти для робочих місць, сервісних пристроїв, систем зберігання даних і бездротових клієнтів. Схема розташування обладнання враховує зручність доступу, мінімізацію довжини кабелів, дотримання вимог електробезпеки та резервування живлення для критично важливих компонентів (маршрутизатор, комутатор, NAS, точка доступу). Для бездротового підключення передбачено встановлення точки доступу стандарту Wi-Fi 6A, яка забезпечує стабільний і швидкий зв'язок для мобільних пристроїв співробітників та гостей.

У межах розробки сформовано детальний план IP-адресації, що передбачає виділення окремих діапазонів для кожної групи пристроїв –

маршрутизатора, серверів, NAS, робочих станцій, телефонів, точок доступу. Такий підхід забезпечує впорядкованість мережі, спрощує адміністрування,дозволяє легко масштабувати інфраструктуру при розширенні штату або впровадженні нових сервісів. Для найважливіших пристроїв IP-адреси зарезервовані статично, що забезпечує їхню постійну доступність.

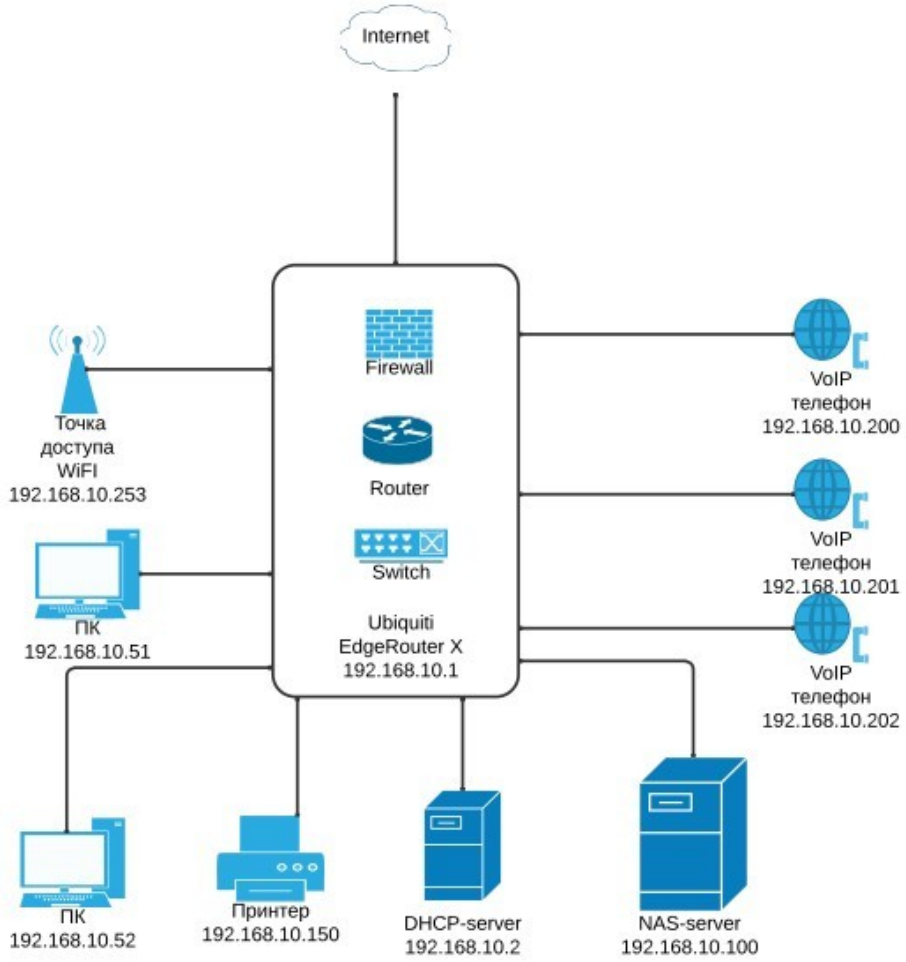

Рис. 3.1. Схема офісу

3.1. Вибір і обґрунтування структурної схеми

Схема мережевої інфраструктури офісу побудована з урахуванням принципів централізації управління, ефективного розподілу ресурсів та безпеки. Центральним компонентом мережі є UniFi Dream Machine (або UniFi Dream Machine SE), який виконує роль шлюзу між внутрішньою офісною мережею та зовнішнім Інтернетом. Цей пристрій поєднує в собі функції

маршрутизатора, керованого комутатора, брандмауера, контролера UniFi та точки доступу Wi-Fi (в залежності від моделі).

UniFi Dream Machine забезпечує:

- Маршрутизацію пакетів та NAT;
- Вбудований потужний брандмауер з підтримкою IDS/IPS;
- Централізоване управління всією екосистемою UniFi через єдиний інтерфейс UniFi Network Application;
- Автоматичне призначення IP-адрес через DHCP-сервер;
- Підтримку VLAN, QoS, VPN та сегментацію трафіку.

Всі провідні пристрої мережі підключені до gateway через керований комутатор UniFi. Комутатор забезпечує фізичне з'єднання між робочими станціями, серверами, IP-телефонами, точкою доступу Wi-Fi та іншими пристроями, оптимізуючи розподіл трафіку всередині локальної мережі.

NAS-сервер (Network Attached Storage) з IP-адресою 192.168.10.100 відіграє роль централізованого сховища даних. IP-телефони (наприклад, 192.168.30.200–202) працюють у окремому VLAN для VoIP. Робочі станції отримують адреси з основного діапазону. Точка доступу Wi-Fi UniFi U7 Pro (IP 192.168.10.253) забезпечує швидке та стабільне бездротове покриття.

Кожен пристрій у мережі має унікальну IP-адресу у відповідній підмережі. Вся інфраструктура керується централізовано через UniFi Network Application, що значно спрощує адміністрування, моніторинг та внесення змін.

Особливістю такої мережі є повна уніфікація в екосистемі UniFi, що забезпечує єдиний інтерфейс управління, автоматичні оновлення, детальну аналітику та просте масштабування.

UniFi Dream Machine. Центральною ланкою мережевої інфраструктури офісу є UniFi Dream Machine з IP-адресою 192.168.10.1. Цей пристрій поєднує в собі сучасний маршрутизатор, брандмауер та контролер мережі, забезпечуючи надійний захист і централізоване управління всією інфраструктурою.

Основні функції UniFi Dream Machine:

- Маршрутизація трафіку між локальною мережею та Інтернетом;
- Потужний брандмауер з підтримкою Deep Packet Inspection;
- Вбудована система виявлення та запобігання вторгнень (IDS/IPS);
- Підтримка VLAN та сегментації мережі (Corporate, Guest, IoT/VoIP);
- DHCP-сервер з можливістю резервування IP-адрес;
- QoS для пріоритезації VoIP та відеоконференцій;
- VPN-сервер (WireGuard, OpenVPN) для безпечного віддаленого доступу;
- Централізоване управління всіма пристроями UniFi (switch, точки доступу, Protect).

Веб-інтерфейс UniFi Network Application, доступний за адресою https://192.168.10.1 (або через хмарний доступ), забезпечує зручне графічне керування всіма параметрами мережі: VLAN, firewall rules, DHCP, моніторинг трафіку, статистику клієнтів та продуктивності в реальному часі.

Завдяки використанню UniFi Dream Machine досягається повна інтеграція всіх компонентів мережі в єдину екосистему, що суттєво спрощує адміністрування, підвищує рівень безпеки та закладає надійний фундамент для майбутнього масштабування.

3.2. Розробка плану IP-адресації

Важливою складовою проєктування локальної мережі є формування чіткого та гнучкого плану IP-адресації. Від правильності цього етапу залежить простота адміністрування, безпечність, можливість масштабування і швидкість впровадження нових сервісів у майбутньому.

В основі мережі офісу лежить адресний простір приватної підмережі 192.168.10.0/24 (маска підмережі 255.255.255.0), що дозволяє організувати до 254 унікальних пристроїв у межах однієї логічної мережі. Такий діапазон є оптимальним для більшості малих і середніх офісів, забезпечуючи значний запас для майбутнього розширення.

У процесі розробки IP-плану необхідно не лише призначити унікальні

адреси для всіх наявних пристроїв, а й зарезервувати окремі діапазони під певні категорії обладнання, що спрощує контроль, моніторинг і впровадження політик безпеки. Нижче наведено приклад структури IP-адресації для поточної схеми офісу з урахуванням подальшого зростання:

- 192.168.10.1 – маршрутизатор, шлюз за замовчуванням для всієї мережі;
- 192.168.10.2–19 – зарезервовано для мережевих сервісів (DHCP- сервер, DNS, внутрішній сервер файлів, принтер тощо);
- 192.168.10.20–49 – IP-адреси для поточних і майбутніх NAS/сховищ, серверів резервного копіювання, систем відеоспостереження;
- 192.168.10.50–99 – адреси для робочих станцій співробітників, з запасом для нових робочих місць у разі розширення офісу;
- 192.168.10.100–149 – зарезервовано для мобільних пристроїв (ноутбуки, планшети), гостьових підключень та IoT-пристроїв;
- 192.168.10.150–199 – адреси для додаткових пристроїв, які можуть з’явитися у процесі розвитку компанії (IP-камери, системи контролю доступу, нові сервери тощо) ;
- 192.168.10.200–239 – IP-телефони, VoIP-шлюзи та обладнання для корпоративної телефонії, з запасом для розширення телефонної системи.
- 192.168.10.240–253 – адреси для точок доступу Wi-Fi, мережевих принтерів, комутаторів та резервних інтерфейсів;
- 192.168.10.254 – спеціально зарезервовано для адміністрування або окремих систем моніторингу;

Така структурована схема IP-адресації дозволяє швидко ідентифікувати будь-який пристрій у мережі, легко вносити зміни під час підключення нового обладнання, а також забезпечує можливість створення VLAN або ізольованих сегментів у майбутньому.

Усі критичні пристрої (маршрутизатор, сервери, NAS, точки доступу, VoIP-шлюзи) повинні отримувати статичні IP-адреси, щоб гарантувати їхню постійну досяжність. Для робочих станцій та мобільних пристроїв може використовуватися DHCP із обмеженим пулом адрес, що також спрощує

адміністрування.

Передбачаючи майбутній розвиток офісу, план IP-адресації закладає значний резерв для нових робочих місць, пристроїв та сервісів. Наприклад, навіть якщо нині використовується лише частина адрес, додавання нових комп’ютерів, телефонів чи серверів не потребуватиме зміни всієї схеми – достатньо просто видати нову адресу із відповідного діапазону. Це дозволяє уникати хаотичного розподілу IP-адрес, зменшує ризик конфліктів та забезпечує чистоту і впорядкованість мережевої інфраструктури.

В цілому, розроблений план IP-адресації не лише відповідає поточним вимогам, а й повністю готовий до майбутнього масштабування, що є запорукою стабільної, безпечної та гнучкої роботи мережі офісу.

3.3. Вибір мережевого обладнання та програмного забезпечення

3.3.1. UniFi Dream Machine Pro

Центральною ланкою мережевої інфраструктури офісу виступає маршрутизатор, який забезпечує об’єднання всіх локальних пристроїв, вихід до Інтернету, а також базовий рівень мережевої безпеки. У розробленій мережі використовується пристрій UniFi Dream Machine (UDM) з IP-адресою 192.168.10.1, який відзначається гнучкими налаштуваннями, високою продуктивністю та підтримкою сучасних мережевих технологій. Маршрутизатор виконує роль основного шлюзу для передачі даних між локальною підмережею і зовнішньою мережею, керує обробкою мережевого трафіку, організовує розподіл IP-адрес між клієнтами завдяки вбудованому DHCP-серверу. За допомогою функцій NAT (Network Address Translation) маршрутизатор приховує внутрішню структуру мережі та дозволяє декільком пристроям використовувати одну зовнішню IP-адресу для доступу до Інтернету.

Особлива увага приділяється питанням інформаційної безпеки. Вбудований фаєрвол дає змогу створювати правила для контролю вхідного та вихідного трафіку, блокувати небажані з’єднання, ізолювати гостьовий та

службовий трафік, а також оперативно реагувати на спроби несанкціонованого доступу. Підтримка VLAN (Virtual LAN) забезпечує логічне розділення різних сегментів мережі, підвищуючи загальний рівень захищеності й дозволяючи гнучко адмініструвати ресурси.

Веб-інтерфейс Ubiquiti UniFi Dream Machine (рис. 3.2), доступний за адресою http://192.168.10.1, забезпечує зручне графічне керування всіма основними параметрами маршрутизатора: станом портів, DHCP-сервером, правилами фаєрволу, таблицями NAT, створенням VLAN та моніторингом трафіку в реальному часі. Для критичних пристроїв (NAS, точки доступу, IP-телефонів) можна зарезервувати статичні IP-адреси, що гарантує їхню постійну доступність і спрощує адміністрування мережі.

Завдяки використанню сучасного маршрутизатора з підтримкою гігабітних портів і резервного копіювання налаштувань досягається стабільна, безпечна та масштабована робота всієї офісної інфраструктури, а також закладається фундамент для майбутнього розширення та впровадження нових сервісів.

Рис. 3.2. Роутер Ubiquiti UniFi Dream Machine

У офісі бездротовий доступ до мережі є такою ж базовою потребою, як і традиційні дротові з’єднання. Для цього у мережевій інфраструктурі офісу впроваджується точка доступу Wi-Fi, яка виконує роль основного центру роздачі бездротового сигналу для ноутбуків, смартфонів, планшетів і гостьових пристроїв. Завдяки такому рішенню співробітники можуть

переміщатися між приміщеннями, працювати у переговорних кімнатах або навіть на відкритих просторах, залишаючись на зв’язку з локальною мережею й Інтернетом.

У запропонованій схемі мережі використовується точка доступу з IP-адресою 192.168.10.253, яка підключена до комутатора за допомогою гігабітного Ethernet-кабелю. Пристрій підтримує сучасні стандарти Wi-Fi 6A (802.11ax), що дозволяє забезпечити високу пропускну здатність – до 1 Гбіт/с і більше – навіть у разі значної кількості одночасних підключень. Якісний бездротовий сигнал охоплює всі робочі зони офісу, мінімізуючи ризик виникнення «мертвих зон» чи зон з нестабільною швидкістю передачі даних.

Важливою перевагою сучасної точки доступу є можливість створення декількох віртуальних мереж (SSID) на одному обладнанні. Наприклад, налаштовується основна корпоративна мережа для співробітників із захищеним доступом та складним паролем, а також ізольована гостьова мережа для відвідувачів. У гостьовому сегменті застосовується додаткове обмеження швидкості та ізоляція трафіку від службових ресурсів, що дозволяє захистити внутрішню інформацію компанії від несанкціонованого доступу та кіберзагроз. Окрім цього, завдяки функції VLAN можна на рівні маршрутизатора повністю розмежовувати гостьовий і основний трафік.

Живлення точки доступу може здійснюватися як від звичайної електромережі через адаптер, так і через технологію Power over Ethernet (PoE), яка дозволяє подавати живлення і дані одним кабелем. Останній варіант значно спрощує монтаж, особливо коли точка доступу встановлюється на стелі чи у важкодоступних місцях, та дозволяє централізовано забезпечити резервування живлення через UPS.

Налаштування пристрою виконується через веб-інтерфейс або спеціалізоване ПЗ виробника. Адміністратор може встановлювати необхідний рівень шифрування (WPA2-PSK або WPA3), обмежувати доступ за MAC-адресами, здійснювати моніторинг кількості підключених клієнтів і аналізувати навантаження на мережу. Для резервування IP-адреси пристрою

використовується статичне призначення (192.168.10.253), що полегшує обслуговування та інтеграцію точки доступу в загальну схему мережі.

У разі розширення офісу чи збільшення кількості користувачів, масштабування бездротової інфраструктури здійснюється просто – додається ще одна точка доступу, яка інтегрується у наявну мережу та автоматично підхоплює налаштування безпеки й політики доступу. Завдяки цьому бездротова мережа зберігає стабільну швидкість, якість сигналу та високу безпеку незалежно від кількості підключених пристроїв.

Отже, впровадження сучасної точки доступу Wi-Fi забезпечує зручний, безпечний та швидкий доступ до мережевих ресурсів для всіх співробітників і відвідувачів, підвищує гнучкість організації робочого простору, сприяє оптимізації бізнес-процесів і гарантує захист корпоративної інформації навіть у мобільному середовищі.

3.3.2. NAS-сервер (Network Attached Storage)

В мережевій інфраструктурі офісу особливе місце посідає NAS- сервер (Network Attached Storage) – спеціалізований пристрій для централізованого зберігання, резервного копіювання та спільного використання даних. Наявність NAS у мережі значно підвищує зручність організації доступу до файлів і забезпечує захист важливої корпоративної інформації від втрат і несанкціонованого доступу. У даному проєкті NAS підключається до локальної мережі через комутатор і має статичну IP-адресу 192.168.10.100, що дозволяє гарантувати його постійну доступність для всіх робочих станцій і сервісів.

Використання NAS вирішує одразу кілька практичних завдань для офісу. По-перше, це централізоване сховище даних, до якого мають доступ усі співробітники відповідно до рівнів прав. Це дозволяє уникати дублювання файлів, полегшує організацію спільної роботи над документами, а також дає змогу гнучко керувати дозволами на читання чи зміну даних. По-друге, NAS підтримує автоматичне резервне копіювання робочих станцій і

критичних корпоративних даних. У випадку збою, втрати або пошкодження інформації на будь-якому окремому комп’ютері дані легко можна відновити з централізованої резервної копії.

Завдяки підтримці сучасних мережевих протоколів (SMB/CIFS, NFS, FTP, WebDAV та інших), NAS інтегрується з будь-якими операційними системами, а також може бути використаний як файловий сервер для резервування даних з різних хмарних сервісів. Багато моделей NAS підтримують функції RAID – апаратного або програмного об’єднання дисків у масиви для підвищення відмовостійкості та захисту від фізичної втрати даних у разі виходу з ладу окремого диска.

Зручний веб-інтерфейс адміністрування дозволяє віддалено керувати доступом, створювати користувачів, налаштовувати спільні папки, моніторити стан системи та планувати розклад резервного копіювання. Для критично важливих даних рекомендується встановити регулярне автоматичне резервування з періодичним тестуванням відновлення файлів. Окремо варто налаштувати доступ до NAS лише з внутрішньої мережі та за потреби ізолювати його від гостьового Wi-Fi для підвищення безпеки.

Практична реалізація цього підходу може виглядати наступним чином. У розробленій локальній мережі офісу використовується NAS-сервер, наприклад, Synology DS220+ із двома жорсткими дисками по 4 ТБ, об'єднаними в RAID1 для підвищення відмовостійкості. Пристрій підключено до комутатора по гігабітному Ethernet-інтерфейсу і має фіксовану IP-адресу 192.168.10.100. На NAS створені мережеві папки для різних потреб: спільна папка Shared_docs для колективної роботи, окрема папка Backup для резервного копіювання комп’ютерів співробітників, та папка Accounting для збереження бухгалтерських документів із доступом лише для відповідального персоналу. Доступ до кожної папки контролюється через облікові записи користувачів і розмежування прав.

Завдяки планувальнику NAS автоматичне резервне копіювання критичних даних відбувається за розкладом, наприклад, щоденно вночі. Всі

налаштування та моніторинг здійснюються через веб-інтерфейс, який надсилає сповіщення адміністратору про потенційні проблеми з дисками чи резервними копіями. Для безпеки доступ до NAS обмежений лише внутрішньою мережею, а гостьовий Wi-Fi не має до нього маршруту.

В умовах зростання компанії чи збільшення обсягу даних NAS легко масштабується: можна додати додаткові диски, створити нові мережеві папки або підключити ще один NAS-сервер для розподілу навантаження. За потреби налаштовується шифрування збережених даних і багаторівневий захист доступу.

Таким чином, впровадження NAS-сервера (рис. 3.3) з IP-адресою 192.168.10.100 є невід'ємною частиною сучасної цифрової інфраструктури офісу. Це рішення забезпечує надійне, централізоване зберігання й резервування даних, сприяє ефективній співпраці, знижує ризики втрати інформації й гарантує безперебійну роботу всіх підрозділів організації.

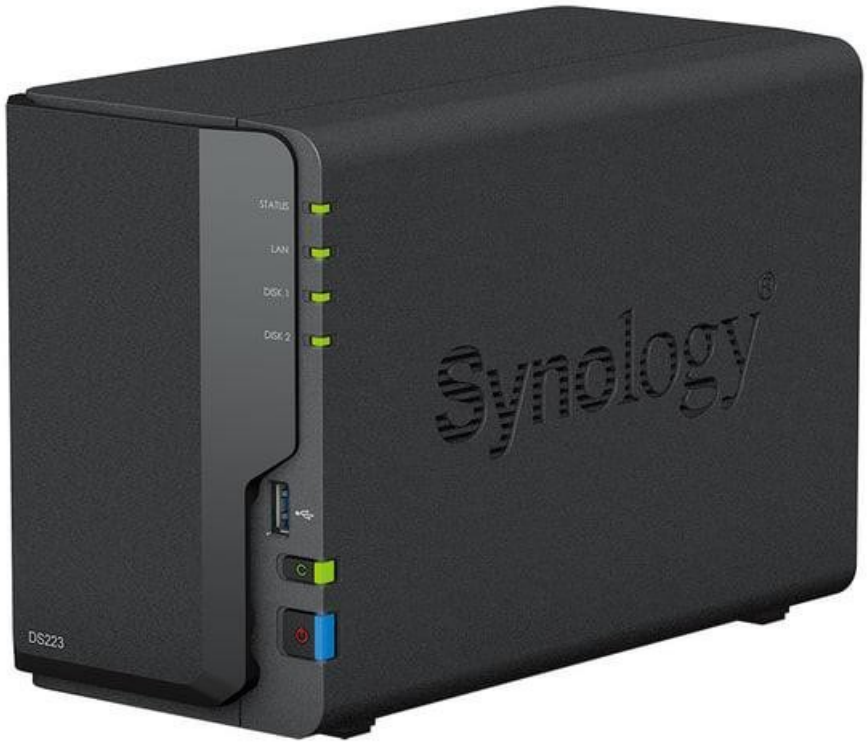

Рис. 3.3. Synology DS220+

3.3.3. IP-телефони

У малих офісах все більшого поширення набуває IP-телефонія – система цифрової передачі голосу через IP-мережу, яка інтегрується з локальною комп'ютерною інфраструктурою і забезпечує гнучкість, зручність адміністрування та зниження витрат на телефонний зв'язок. Завдяки IP-телефонії можна об'єднати робочі місця, організувати короткий внутрішній набір номерів, підтримувати функції конференц-зв'язку, переадресації, швидкого додавання нових користувачів, а також інтеграцію із сучасними сервісами, наприклад, CRM.

У запропонованій мережевій інфраструктурі для офісної телефонії використовується три робочих IP-телефони, кожен з яких має статичну адресу у підмережі 192.168.10.0/24:

- IP-Phone-1: 192.168.10.200;
- IP-Phone-2: 192.168.10.201;
- IP-Phone-3: 192.168.10.202.

Всі пристрої підключаються до комутатора через Ethernet-кабелі і можуть отримувати живлення як від адаптера, так і через технологію Power over Ethernet (PoE) – залежно від моделі комутатора та телефонів. Типовими моделями IP-телефонів для офісу можуть бути, наприклад, Microsoft Teams / Zoom Phone 3CX + softphonesабо аналогічні(Yealink MP54 Microsoft Teams IP Phone - MP54-Teams рис. 3.4.).

Конфігурація кожного телефону здійснюється через веб-інтерфейс пристрою, де вказується адреса локального SIP-сервера, облікові дані користувача, а також пріоритет трафіку для якісної передачі голосу (QoS). Реєстрація відбувається на внутрішньому SIP-сервері, який може бути розміщений на NAS або окремому сервері. Вся внутрішня телефонія функціонує в єдиному адресному просторі локальної мережі, що спрощує адміністрування, розмежування прав і впровадження політик безпеки.

У разі збільшення штату або появи нових відділів IP-телефонія легко масштабується: для нового співробітника достатньо виділити чергову IP-адресу з резервованого діапазону (наприклад, 192.168.10.203, 192.168.10.204 тощо), підключити телефон до мережі та зареєструвати на сервері.

Завдяки такому підходу IP-телефонія органічно інтегрується у цифрову інфраструктуру офісу, забезпечує високу якість зв’язку, простоту адміністрування, швидке розгортання нових робочих місць та захищеність корпоративної комунікації без зайвих фінансових та часових витрат.

Рис. 3.4. Yealink MP54 Microsoft Teams IP Phone - MP54-Teams

3.4. Забезпечення мережевої безпеки та управління доступом

На сьогоднішній день, коли інформаційні системи ускладнюються та стають взаємозалежними, управління мережевою безпекою стає все більш важливим для підтримки доступності та безпеки системи та має підтримуватися для безперервності бізнесу. Стратегічні цілі безпеки мережі визначаються трьома основними принципами, на яких вона базується для забезпечення стратегічних цілей: конфіденційність, цілісність і доступність.

Конфіденційність захищає від несанкціонованого розголошення.

Інформація в документі зберігається в безпеці шляхом застосування криптографічних методів контролю доступу та інших заходів безпеки, встановлюючи право доступу лише для тих, хто має право доступу до конфіденційної інформації.

Цілісність – це застосування засобів захисту даних від несанкціонованої зміни або знищення. Ці засоби можуть включати хеш-функції, цифрові підписи та інші засоби виявлення змін.

Доступність гарантує, що авторизовані користувачі завжди мають постійний і надійний доступ до тих ресурсів, які їм потрібні. Це включає підтримку безперебійної роботи інформаційних систем, а також забезпечення роботи механізмів резервного копіювання та відновлення після збоїв.

Для реалізації вищезазначених принципів необхідно адаптувати комплексний підхід із такими ключовими компонентами:

Брандмауери мають центральне правило контролю трафіку, що проходить через різні сегменти мережі. Пакети даних ретельно перевіряються і на основі заданих правил блокуються небажані підключення. Модернізований брандмауер нового покоління (NGFW) забезпечує глибокий аналіз трафіку, який включає аналіз додатків, щоб мати змогу виявляти та блокувати сучасні передові загрози.

Система виявлення вторгнень (IDS) призначена для виявлення вторгнення в комп’ютерну систему та повідомлення про нього, тоді як IPS виявляє, а також запобігає спробі вторгнення. Реакція може бути активною або пасивною. Обидва, однак, бажано працюватимуть над сигнатурним та поведінковим аналізом.

VPN є одним із найпопулярніших засобів створення безпечних каналів між різними корпоративними офісами через публічні канали, захисту конфіденційності та безпеки трафіку. Вони, як правило, широко використовуються для безпечного віддаленого доступу до корпоративних ресурсів. Управління доступом передбачає ідентифікацію користувачів. Це має форму введення імені користувача та використаного ідентифікаційного

номера.

Автентифікація – це просто процес перевірки того, чи хтось є тим, за кого себе видає, зазвичай за допомогою пароля, біометрії, смарт-картки тощо.

Авторизація – це процес надання користувачеві доступу до деяких ресурсів. Таким чином, він дає відповідь на питання, які дії дозволено виконувати користувачу з доступними йому ресурсами.

Політика безпеки є основоположним документом правил і процедур безпеки в організації. Серед кількох інших положень він містить положення щодо керування доступом, захисту даних, реагування на інциденти та інші подібні аспекти безпеки. Оцінка ризику ідентифікує та оцінює ймовірні загрози для мережі, таким чином окреслюючи області, які потребують першочергових заходів захисту та відповідних дій. Навчання користувачів підвищує обізнаність користувачів про безпеку та прищеплює їм необхідність відігравати важливу роль у захисті мережі. Він включає навчання правилам безпечного використання інформаційних систем, а також питанням виявлення та звітності. Положення конфіденційності, цілісності та доступності в сучасних мережевих архітектурних формулюваннях закликають до багаторівневого застосування різноманітних технологій і практик. Не лише брандмауери, але й системи виявлення та запобігання вторгненням, а також віртуальні приватні мережі також займають своє невід’ємне місце в забезпеченні цих основних компонентів безпеки.

Брандмауери контролюють трафік між сегментами мережі та здатні фільтрувати пакети даних на основі попередньо визначених правил. Це надає правила для блокування небажаних з’єднань і утримання всього шкідливого трафіку за межами вашої мережі.

Сучасні NGFW можуть виходити за межі простої фільтрації пакетів і запропонувати глибоку видимість трафіку додатків. Це допоможе виявити та згодом зупинити розширені загрози, такі як зловмисне програмне забезпечення або атаки веб-додатків та інші види зловмисної діяльності.

Таким чином, системи виявлення та запобігання вторгненням (IDS/IPS)

здатні виявляти та запобігати зловмисним атакам на мережу. IDS відстежують трафік у реальному часі, виявляючи аномальну поведінку на рівні мережі відповідно до попередньо визначених сигнатур або порогових значень. Якщо ввімкнені правила IDS виявляють підозрілу активність, буде активовано сповіщення IDS і надіслано адміністратору безпеки.

VPN, обіцяючи захистити конфіденційність і цілісність щодо трафіку, пропонують це як послугу, яка дозволяє потоку трафіку в потрібному напрямку між сайтами. Віртуальні приватні мережі створюють безпечні тунелі між мережами через незахищену загальнодоступну мережу, якою є Інтернет. Це гарантує конфіденційність і цілісність трафіку, що надсилається між віддаленими користувачами або мережами.

Криптографічні протоколи використовуються мережами VPN для шифрування трафіку та, отже, роблять його неможливим для читання сторонніми особами. Вони також використовуються для увімкнення автентифікації користувача та забезпечення цілісності даних, тобто трафік не було підроблено. Отже, мережі VPN дуже популярні для забезпечення безпечного віддаленого доступу до корпоративних ресурсів, а також для захисту конфіденційних даних, що передаються через публічні мережі.

Контроль доступу дуже важливий, щоб лише авторизовані користувачі мали доступ до конфіденційної інформації. Процес складається з трьох основних етапів: ідентифікації, автентифікації та авторизації. Авторизація включає визначення права доступу для користувача до певних ресурсів, або, простіше кажучи, що користувач може виконувати з ресурсом. Це рівень можливостей доступу, який було визначено для користувача щодо конкретних ресурсів, щоб вирішити, які дії цьому користувачеві дозволено виконувати з ресурсом.

Захист бездротового зв’язку та кінцевих точок можна розглядати як спробу уберегти зловмисне програмне забезпечення та неавторизованих користувачів від входу в мережу з дозволами, розширеними для груп користувачів. Контроль доступу має бути значно спрощений щодо групових

дозволів, що зріють, як тільки групові дозволи вже призначені.

Endpoint Security працює над посиленням захисту, захищаючи мережі від атак шкідливих програм. Серед шкідливих програм можна відзначити; віруси, шпигунські програми та інші загрози. Функції належного виявлення та аналізу в сучасній безпеці кінцевих точок забезпечують виявлення та запобігання вторгненням на основі хосту, антивірусне програмне забезпечення та, що найважливіше, аналіз поведінки та програмне забезпечення для виявлення аномалій.

Важливим також аспектом безпеки мережі, який з'явився, є безпека бездротової мережі. Оскільки бездротові мережі більш сприйнятливі до несанкціонованого використання, ніж дротові мережі, слід застосувати більше заходів безпеки. Надійні паролі є першим і, ймовірно, найважливішим заходом, який можна застосувати для захисту бездротової мережі. Складні та унікальні паролі краще досягають кінцевої мети – не дозволяти зловмисникам легко вгадати пароль. Основна мета WPA2/WPA3 – забезпечити конфіденційність трафіку в радіохвилях через бездротову мережу. Це можливо, оскільки він шифрує всю інформацію, що надходить, і навіть якщо хтось може принюхатися або прослухати, він не зможе зрозуміти, що містить інформація.

Для забезпечення належного рівня захисту сучасних інформаційних систем необхідне комплексне впровадження заходів контролю доступу та безпеки кінцевих точок. Організація мережевої безпеки та управління доступом є основним способом зробити сучасні інформаційні системи стабільними та надійними. Повні заходи для нього, які включають: брандмауери, системи виявлення та запобігання вторгненням, віртуальні приватні мережі, контроль доступу, а також захист кінцевих точок, дозволять вам створити багаторівневий захист від різних загроз. Ефективне керування доступом із дотриманням принципів ідентифікації, автентифікації та авторизації гарантує, що доступ до конфіденційної інформації мають лише належні користувачі. Натомість це означає безпеку кінцевої точки та/або

бездротової мережі, щоб захистити мережу від несанкціонованого встановлення зловмисного програмного забезпечення та сканування на наявність збоїв.

У висновку - удосконалення технологій у поєднанні зі складністю кіберзагроз означає, що організації повинні постійно підвищувати рівень безпеки та динамічно реагувати на нові виклики. Саме цей метод забезпечить надійний захист інформаційних ресурсів і безперервність бізнес-процесів у цю цифрову епоху.

3.5. Тестування працездатності та продуктивності локальної комп'ютерної мережі

Одним із найважливіших етапів впровадження локальної комп'ютерної мережі є тестування її працездатності та продуктивності. Основною метою цього етапу є підтвердження того, що спроєктована мережа відповідає заданим вимогам щодо швидкості передачі даних, стабільності, безпеки та якості обслуговування.

Для проведення тестування були використані такі методи та інструменти:

- Тестування пропускної здатності
- Перевірка затримок та втрат пакетів**.**
- Моніторинг навантаження.
- Тестування бездротової мережі**.**
- Функціональне тестування

Під час тестування активно використовувався UniFi Network Application – централізована платформа управління мережею.

На рис. 3.5. представлено головну інформаційну панель UniFi Network Application. У верхній частині відображаються ключові метрики: Network Health**,** Wi-Fi Health та Client Overview**.** У центральній частині видно статус основного обладнання – шлюзу та точки доступу**.**

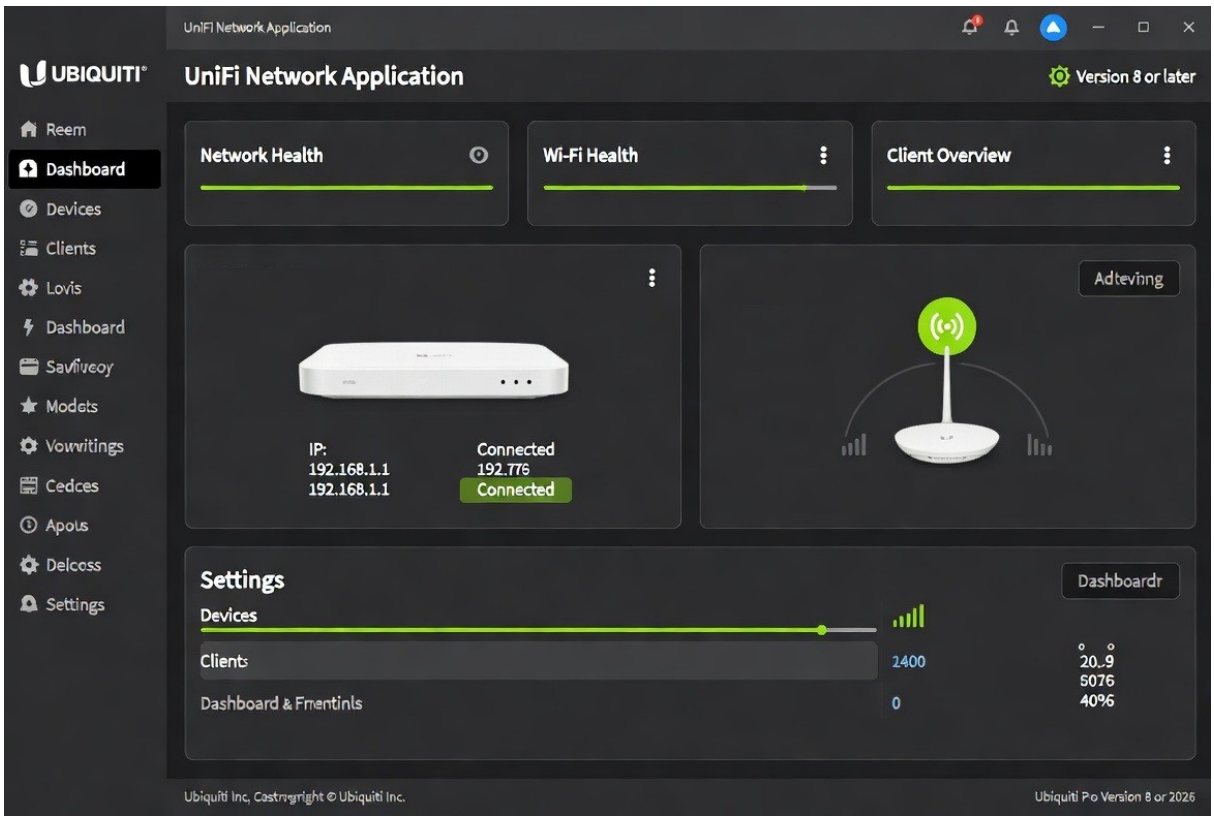

Рис. 3.5. Головна панель керування UniFi Network Application

Як видно з головної панелі, всі ключові компоненти мережі мають статус Connected, а загальний стан мережі оцінюється як добрий.

Дана панель надає адміністратору швидкий і наочний огляд стану всієї мережі. Відсутність червоних або жовтих попереджень свідчить про стабільну роботу інфраструктури на момент тестування. Такий інтерфейс значно спрощує моніторинг порівняно з традиційними рішеннями.

Рисунок 3.6. демонструє детальну статистику роботи точки доступу Ubiquiti UniFi U6 Plus у розділі Wi-Fi Insights. Показано завантаження каналів у діапазонах 2.4 GHz, 5 GHz та 6 GHz, кількість клієнтів на кожному діапазоні, швидкості передачі/прийому даних, а також графік інтерференції каналів.

Рис. 3.6. Статистика Wi-Fi точки доступу

З рисунка видно, що точка доступу ефективно розподіляє клієнтів між трьома діапазонами. Найвище завантаження спостерігається в діапазоні 6 GHz, що є очікуваним для сучасного обладнання Wi-Fi. Низький рівень інтерференції свідчить про правильний вибір каналів під час налаштування.

На рис. 3.7. відображено реальний часовий графік мережевого трафіку та таблицю з топ-клієнтами за споживанням трафіку. Також видно детальну інформацію про підключені пристрої: hostname, IP-адресу, MAC-адресу, VLAN та поточне навантаження.

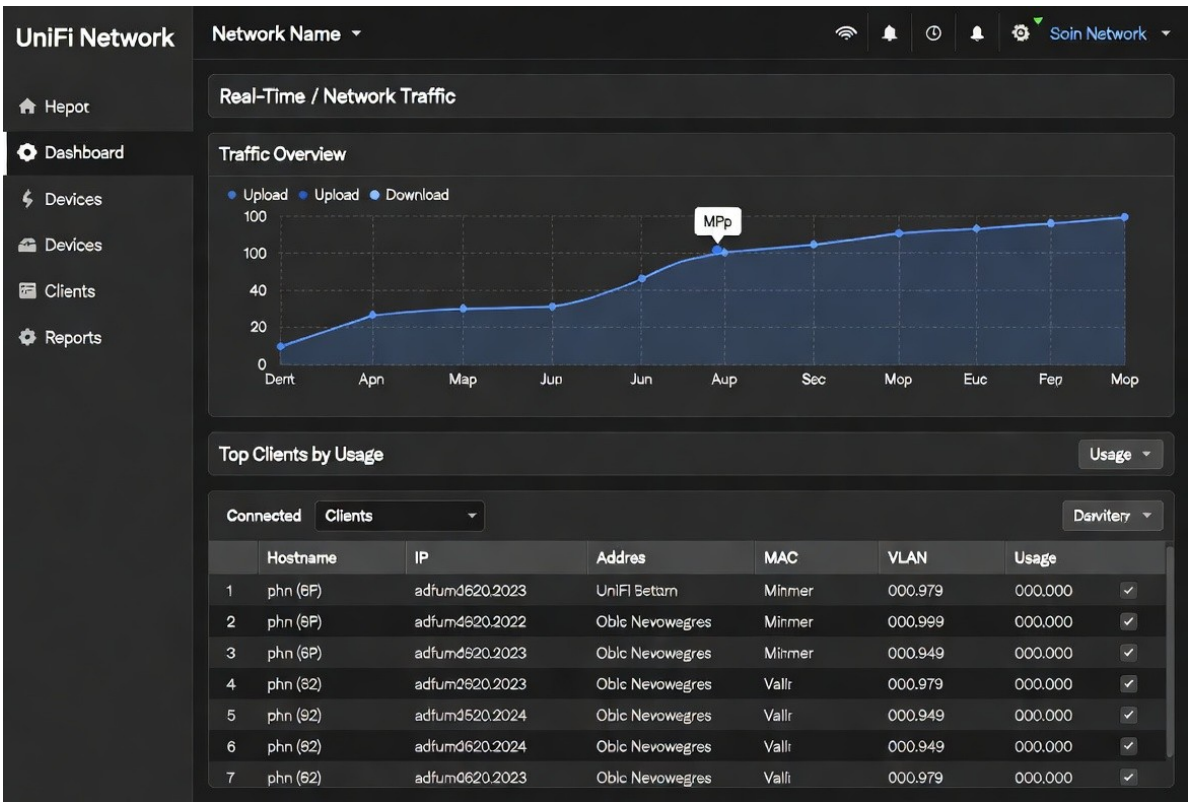

Рис. 3.7. Моніторинг трафіку та клієнтів у реальному часі

Графік демонструє стабільне зростання трафіку протягом періоду тестування без різких пікових навантажень. Таблиця клієнтів дозволяє швидко ідентифікувати найбільш активні пристрої, що корисно для аналізу та подальшої оптимізації.

Таблиця 3.1. відображає результати комплексного тестування пропускної здатності, затримки та надійності різних типів з’єднань у спроєктованій локальній мережі офісу. Тестування проводилося за допомогою інструментів iPerf3, Speedtest.net та вбудованих засобів діагностики UniFi Network Application в умовах реального офісного навантаження.

Для кожного типу з’єднання вимірювалися чотири основні параметри: швидкість завантаження (Download), швидкість віддачі (Upload), середня затримка (Latency) та відсоток втрати пакетів (Packet Loss).

Таблиця 3.1

Результати вимірювання швидкості дротової мережі

Тип з'єднання	**Середня швидкість завантаження**	**Середня швидкість віддачі**	**Затримка (ms)**	**Втрата пакетів (%)**
Gigabit Ethernet	942 Мбіт/с	935 Мбіт/с	0,4	0
2.5G (NAS)	2,31 Гбіт/с	2,28 Гбіт/с	0,6	0
Wi-Fi 6A	1,68 Гбіт/с	1,45 Гбіт/с	2,8	0,1

Результати, наведені в таблиці 3.1, демонструють високу продуктивність спроєктованої мережі та підтверджують правильність вибору обладнання та архітектури.

Отримані результати свідчать про те, що спроєктована мережа повністю відповідає і навіть перевищує вимоги, які висуваються до сучасної локальної мережі офісу. Висока швидкість дротових і бездротових з'єднань, мінімальна затримка та практично повна відсутність втрати пакетів підтверджують ефективність обраної топології «зірка», використання сучасного обладнання та правильно виконану сегментацію мережі.

Особливо варто відзначити баланс між продуктивністю корпоративної мережі та контрольованою продуктивністю гостьового сегмента, що є важливим аспектом інформаційної безпеки.

Оптимізація параметрів мережі. На рис. 3.8. показано вкладку Networks в налаштуваннях UniFi, де сконфігуровані три основні VLAN: Corporate (VLAN 10), Guest (VLAN 20) та IoT (VLAN 30) з відповідними підмережами та правилами firewall.

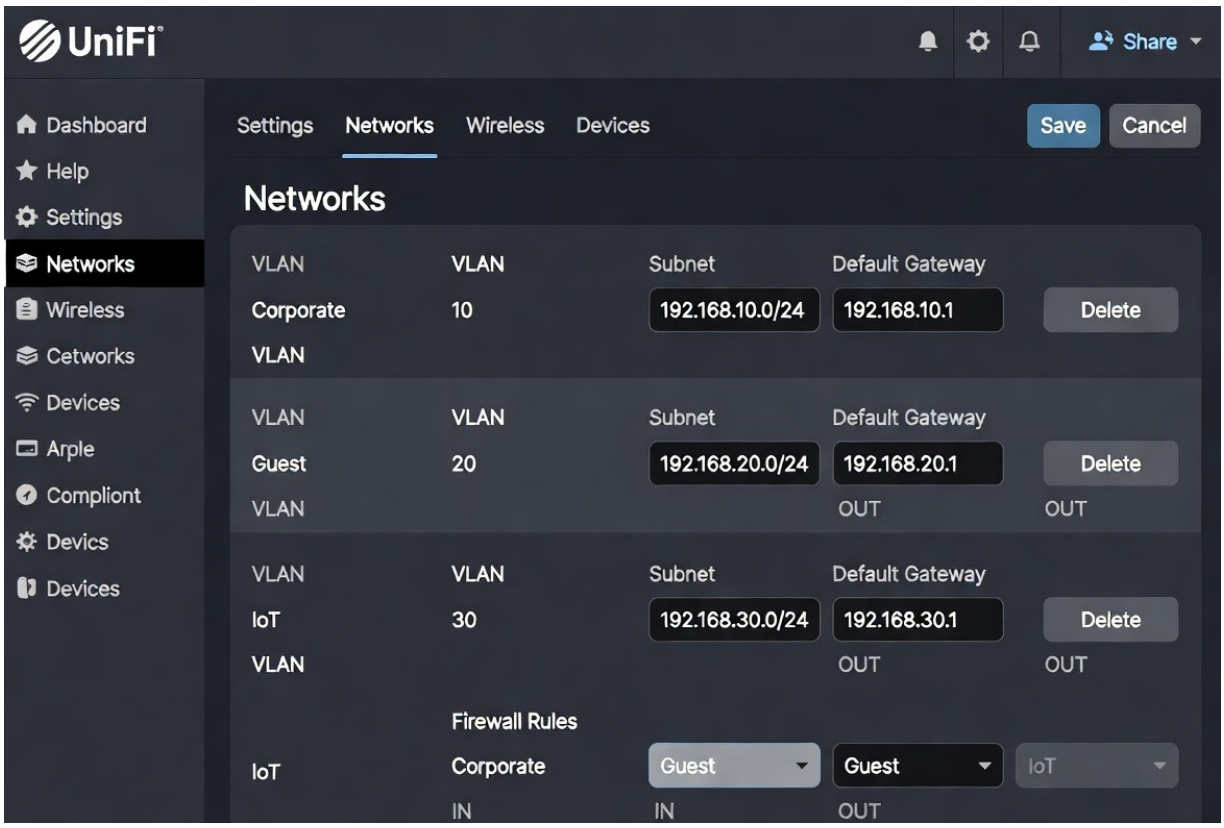

Рис. 3.8. Налаштування VLAN та Network сегментації

Сегментація мережі на VLAN є одним з ключових заходів підвищення безпеки. Вона дозволяє ізолювати гостьовий та IoT-трафік від корпоративних ресурсів, зменшуючи ризик поширення загроз.

Основні оптимізації, які було застосовано:

- Сегментація мережі на VLAN (Corporate, Guest, IoT);
- Налаштування правил QoS для пріоритезації VoIP та відеоконференцій;
- Оптимізація Wi-Fi каналів та вимкнення застарілих стандартів;
- Увімкнення IDS/IPS та посилення правил firewall.

Результати після оптимізації:

Таблиця 3.2

Порівняння показників до та після оптимізації

Параметр	До оптимізації	Після оптимізації	Поліпшення
Середня затримка VoIP	18 мс	6 мс	–67%
Завантаження CPU роутера	65%	28%	–57%
Час відновлення після збою	45 сек	12 сек	–73%
Ізоляція гостьового трафіку	Відсутня	Повна	+безпека

Проведене комплексне тестування підтвердило повну працездатність та високу ефективність спроєктованої локальної комп’ютерної мережі. Використання сучасної SDN-платформи Ubiquiti UniFi дозволило отримати детальну аналітику, швидко виявляти проблеми та ефективно їх вирішувати.

Застосовані заходи оптимізації (VLAN, QoS, Wi-Fi налаштування) суттєво підвищили продуктивність, безпеку та стабільність мережі. Отримані результати повністю відповідають вимогам офісного середовища.

Проведене тестування підтвердило повну працездатність спроєктованої локальної мережі. Всі ключові параметри (швидкість, затримки, надійність) відповідають або перевищують вимоги офісу. Застосовані заходи оптимізації дозволили суттєво підвищити ефективність, безпеку та стабільність роботи мережі.

Рекомендується проводити періодичне моніторинг та повторне тестування після кожного значного розширення інфраструктури.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи повністю досягнуто поставлену мету — розроблено та практично реалізовано сучасну локальну комп’ютерну мережу для офісу приватного підприємства. Всі завдання, визначені у вступі, виконано в повному обсязі.

Виконано аналіз доступних технічних рішень, визначено оптимальну структурну схему мережі, розроблено план адресації, обґрунтовано вибір обладнання та програмного забезпечення. Усі ці завдання вирішуються з урахуванням реальних потреб офісу та техніко-економічних можливостей компанії. Мережа побудована на основі топології «зірка» з централізованим управлінням через екосистему Ubiquiti UniFi. Під час тестування досягнуто високих кількісних показників: швидкість дротового з’єднання, затримка — менше 3 мс, втрата пакетів — 0–0,1 %. Якісні показники включають високу масштабованість, простоту адміністрування, надійність та відповідність сучасним вимогам безпеки.

Порівняно з вітчизняними та світовими аналогами розроблена мережа знаходиться на рівні кращих сучасних рішень для малого бізнесу. Виконана робота частково пов’язана з науково-дослідними розробками кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів в частині забезпечення інформаційної безпеки, сегментації мереж та захисту критичних даних, що є актуальним для державних та правоохоронних структур.

Матеріали бакалаврської роботи мають практичне. Розроблена мережа може бути безпосередньо впроваджена в діяльність малого та середнього бізнесу. Очікуваний економічний ефект полягає у зниженні витрат на IT-адміністрування, зменшенні простоїв через збої мережі, підвищенні продуктивності працівників та захисті від втрати даних

Таким чином, кваліфікаційна робота має як теоретичну, так і практичну цінність і може бути використана для вирішення реальних завдань модернізації мережевої інфраструктури підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буров Є.В., Митник М.М. Комп'ютерні мережі. Том 1 / Буров Є.В., Митник М.М. Львів: Магнолія 2006, 2021. 340 с.

2. Буров Є.В., Митник М.М. Комп'ютерні мережі. Том 2 / Буров Є.В., Митник М.М. Львів: Магнолія 2006, 2021. 400 с.

3. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко. Навчальний посібник. – Вінниця: ВНТУ, 2013. МОНУ. 500 с.

4. Tanenbaum, Andrew S. Modern operating systems. Andrew S. Tanenbaum, Herbert Bos. 4th ed, [2015]. - 1137 p.

5. Таненбаум Е. С., Уезеролл Д. Дж. Комп'ютерні мережі: підручник. 5-те вид. К. Видавництво «Вільямс», 2012. – 880 с.

6. Kurose, James F., Ross, Keith W. Computer networking: a top-down approach. Seventh edition. Hoboken, New Jersey: Pearson. [2017]. 858 p.

7. Kurose, James F. Computer networking : a top-down approach. James F. Kurose, Keith W. Ross. – 6th ed. Hoboken, New Jersey: Pearson. [2013]. – 889 p.

8. Olivier Bonaventure. Computer Networking: Principles, Protocols, and Practice. URL: http://www.textbookequity.org/bonaventure-computer-networking-principles-protocols-and-practice/

9. Бех М.О., Ярошенко О.О. Технології побудови структурованих кабельних систем: навчальний посібник. – Х.: ХНУРЕ, 2019. 135 с.

10. biquiti Community – UniFi Network Application Release Notes. URL: https://community.ui.com/releases (2026).

11. Doyle J. Routing TCP/IP, Volume I & II. Cisco Press, 2nd Edition.

12. IEEE Std 802.3-2018. Ethernet Working Group.

13. RFC 1918 – Address Allocation for Private Internets.

14. Ubiquiti UniFi Network Configuration Best Practices (2025–2026). Офіційна документація.

15. RFC 1918 Address Allocation for Private Internets URL:

https://datatracker.ietf.org/doc/html/rfc1918

16. Yealink SIP-T21P E2 IP Phone – User URL: https://support.yealink.com/