

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки**

Кафедра комп'ютеризованих систем управління

«Допущений до захисту»

Завідувач кафедри

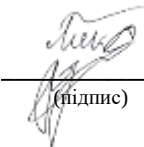
 Черно О.О.
«16» 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «бакалавр»

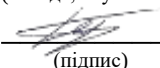
на тему: «Інформаційна інфраструктура офісного середовища»

Виконав: студент 4341 групи


(підпис) **Борисов О.Ю.**

Керівник роботи:

доцент кафедри КСУ, к.т.н., доцент
(посада, науковий ступень вчене звання)


(підпис) **Герасін О.С.**

м. Миколаїв – 2025 р.

ННІ автоматики і електротехніки
Кафедра комп'ютеризованих систем управління
Рівень вищої освіти бакалавр

Спеціальність **151 Автоматизація та комп'ютерно-інтегровані технології**

(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри КСУ
 **Черно О.О.**
« 05 » 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Б о р и с о в О л е к с і й Ю р і й о в и ч

(прізвище, ім'я, по батькові)

1. Тема
роботи: Інформаційна інфраструктура офісного середовища

керівник роботи Герасін Олександр Сергійович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "23" 04 2025р. № УЧ-343

2. Строк подання студентом
роботи 09.06.2025

3. Вихідні дані до роботи Розробити інформаційну інфраструктуру офісного середовища для двоповерхового офісу з 10 працівниками, яка включає логічну сегментацію мережі, налаштування основних серверних служб, централізоване управління доступом, організацію віддаленого підключення та засобів моніторингу, з урахуванням вимог масштабованості, інформаційної безпеки та охорони праці.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Огляд сучасного стану проблеми побудови інформаційної інфраструктури робочого середовища офісу.
Апаратні компоненти інформаційної інфраструктури офісного середовища.
Програмні компоненти інформаційної інфраструктури робочого середовища офісу.
Охорона праці.

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

Актуальність, об'єкт і предмет дослідження

Мета і завдання дослідження

Основи інформаційної інфраструктури

Апаратне та програмне забезпечення

Аналіз апаратної інфраструктури

Аналіз програмної інфраструктури

Моніторинг і безпека

Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
<i>Охорона праці</i>	<i>Герасін О.С., доцент каф. КСУ</i>	29.04.2025	12.05.2025

7. Дата видачі завдання: «11» 02 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки кваліфікаційної роботи	Строк виконання	Примітка
1	Огляд сучасного стану проблеми побудови інформаційної інфраструктури робочого середовища офісу	14.03.2025	виконано
2	Апаратні компоненти інформаційної інфраструктури офісного середовища	04.04.2025	виконано
3	Програмні компоненти інформаційної інфраструктури робочого середовища офісу	29.04.2025	виконано
4	Охорона праці	12.05.2025	виконано

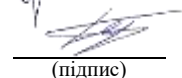
Студент


(підпис)

Борисов О.Ю.

(прізвище та ініціали)

Керівник роботи


(підпис)

Герасін О.С.

(прізвище та ініціали)

АНОТАЦІЯ

Обсяг кваліфікаційної роботи становить 88 сторінок, у роботі 44 рисунків, 11 таблиць та 25 використаних джерел.

У кваліфікаційній роботі розроблено інформаційну інфраструктуру офісного середовища на базі сучасних апаратних і програмних засобів.

Проведено аналіз вимог до мережевої інфраструктури, спроектовано топологію мережі типу "зірка" з використанням комутаторів Cisco Catalyst 2960-S та сервера Supermicro 6016T-URF. Реалізовано сегментацію трафіку за допомогою VLAN, налаштовано серверні служби (DHCP, DNS, Active Directory) та групові політики для управління користувачами. Впроваджено VPN на базі WireGuard і систему моніторингу Zabbix для забезпечення безпеки та контролю стану мережі. Розроблено заходи з охорони праці, включаючи ергономічні стандарти та навчання персоналу. Проведено експериментальне тестування системи, яке підтвердило її стабільність, безпеку та масштабованість.

Ключові слова: інформаційна інфраструктура, офісне середовище, мережева топологія, Cisco Catalyst, Supermicro, VLAN, VPN, Zabbix, охорона праці.

ABSTRACT

The qualification paper consists of 88 pages and includes 44 figures, 11 tables, and 25 references.

The qualification work presents the development of an information infrastructure for an office environment based on modern hardware and software tools.

An analysis of the requirements for the network infrastructure was conducted, and a star topology network was designed using Cisco Catalyst 2960-S switches and a Supermicro 6016T-URF server. Traffic segmentation was implemented using VLANs, and server services (DHCP, DNS, Active Directory) as well as Group Policies for user management were configured. A VPN based on WireGuard and the Zabbix monitoring system were implemented to ensure network security and status monitoring. Occupational safety measures were developed, including ergonomic standards and staff training. Experimental testing of the system confirmed its stability, security, and scalability.

Keywords: information infrastructure, office environment, network topology, Cisco Catalyst, Supermicro, VLAN, VPN, Zabbix, occupational safety.

Вступ.....	8
РОЗДІЛ 1 ОГЛЯД СУЧАСНОГО СТАНУ ПРОБЛЕМИ ПОБУДОВИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ РОБОЧОГО СЕРЕДОВИЩА ОФІСУ ..	10
1.1. Загальні відомості та основні вимоги до інформаційної інфраструктури офісу.....	10
1.2. Апаратне та програмне забезпечення офісних комп'ютерних мереж.....	13
1.3. Методи та засоби системної інженерії для підвищення ефективності офісних середовищ.....	20
1.4. Висновки до розділу 1.....	24
РОЗДІЛ 2 АПАРАТНІ КОМПОНЕНТИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ОФІСНОГО СЕРЕДОВИЩА	26
2.1. Проектування логічної схеми мережі.....	26
2.2. Вибір мережевого обладнання.....	31
2.3. Розподіл IP-адресації для компонентів мережі	50
2.4. Планування розташування обладнання інфраструктури офісу.....	51
2.5. Висновки до розділу 2.....	54
РОЗДІЛ 3 ПРОГРАМНІ КОМПОНЕНТИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ РОБОЧОГО СЕРЕДОВИЩА ОФІСУ	56
3.1. Запуск і налаштування серверів офісної мережі.....	56
3.2. Особливості групових політик та управління користувачами	60
3.3. Налаштування міжмережевого екрану та VPN	61
3.4. Засоби забезпечення моніторингу та безпеки мережі	67
3.5. Аналіз результатів роботи запропонованої інформаційної інфраструктури офісного середовища.....	70
3.6. Висновки до розділу 3.....	73
РОЗДІЛ 4 ОХОРОНА ПРАЦІ	76
4.1. Загальні положення охорони праці	76
4.2. Аналіз небезпечних та шкідливих факторів, що впливають на людину при розгортанні інформаційної інфраструктури офісного середовища	76
4.3. Заходи з техніки безпеки, що необхідно провести для зменшення або усунення впливу шкідливих факторів при розгортанні інформаційної інфраструктури офісного середовища	78
4.4. Висновки до розділу 4.....	81
ВИСНОВКИ.....	82
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	83

ДОДАТОК А.....	85
ДОДАТОК Б	86
ДОДАТОК В.....	87
ДОДАТОК Г	88

ВСТУП

У сучасному світі інформаційні технології відіграють ключову роль у забезпеченні ефективної діяльності офісних структур, організацій та підприємств. Зростаючі обсяги цифрових даних, широке використання віддаленої роботи, необхідність забезпечення захищеного доступу до інформаційних ресурсів і злагодженої взаємодії співробітників висувають нові вимоги до організації внутрішньої інформаційної інфраструктури. Стабільність, безпека, масштабованість і керованість інформаційних систем стали визначальними чинниками для підтримки робочих процесів в офісному середовищі.

Однак, незважаючи на значну кількість досліджень у сфері організації комп'ютерних мереж та інформаційної безпеки, питання комплексного проектування й впровадження офісної інформаційної інфраструктури на практиці часто вирішуються фрагментарно. Це стосується як вибору технічних і програмних засобів, так і методів адміністрування, управління доступом, резервного копіювання та підтримки продуктивності. Актуальність цієї теми зумовлена також потребою у типових рішеннях, які можна адаптувати до офісів різного масштабу з урахуванням сучасних вимог.

У наукових і технічних публікаціях аналізуються окремі аспекти інформаційної інфраструктури — від побудови локальних мереж до реалізації політик безпеки, управління користувачами та моніторингу систем. Проте цілісних рішень, що охоплюють весь цикл розробки та впровадження офісної ІТ-інфраструктури — від аналізу потреб до тестування результатів — у відкритому доступі обмаль, що й визначило вибір напрямку цього дослідження.

Метою даної роботи є розробка та впровадження ефективної інформаційної інфраструктури для офісного середовища, яка відповідає б сучасним вимогам щодо продуктивності, безпеки, масштабованості та зручності управління.

Для досягнення поставленої мети передбачено виконання таких завдань:

- визначити основні вимоги до інформаційної інфраструктури офісного типу;
- схарактеризувати ключові апаратні та програмні компоненти таких систем;

- розробити загальну концепцію побудови інфраструктури для типового офісу;
- встановити принципи організації доступу, адміністрування та забезпечення захисту інформації;
- розкрити результати оцінки працездатності побудованої системи та сформулювати практичні рекомендації.

Об'єктом дослідження є процес організації інформаційної інфраструктури в офісному середовищі, а предметом – підходи до її структурного, функціонального й організаційного формування із забезпеченням надійності, керованості та безпеки.

Результати дослідження апробовано під час моделювання інформаційного середовища умовного офісу, а основні підходи обговорювалися в межах навчальних консультацій і практичних занять.

Застосування сучасних технологій та методів дозволить створити надійну, масштабовану та ефективну інформаційну інфраструктуру, яка забезпечить стабільну роботу офісних процесів.

РОЗДІЛ 1

ОГЛЯД СУЧАСНОГО СТАНУ ПРОБЛЕМИ ПОБУДОВИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ РОБОЧОГО СЕРЕДОВИЩА ОФІСУ

1.1. Загальні відомості та основні вимоги до інформаційної інфраструктури офісу

Інформаційна інфраструктура в офісному середовищі є важливою для ефективного функціонування сучасних бізнесів. Ця інфраструктура включає апаратні засоби, програмне забезпечення та мережеві елементи, які сприяють безперебійному обміну даними, централізованому контролю ресурсів та надійному захисту даних. Спосіб організації цієї інфраструктури безпосередньо впливає на те, як добре працюють співробітники, наскільки гладко працюють робочі процеси та як швидко компанія може реагувати на зміни на ринку.

Через комп'ютерні мережі користувачі отримують доступ до різноманітних функцій, таких як швидкий обмін даними, послуги електронної пошти, управління процесами здалека та оптимальне використання фізичних ресурсів. Наприклад, дозволяючи кільком користувачам користуватися принтерами та дисковими зберігання спільно, ресурси використовуються ефективніше. Крім того, наявність централізованих баз даних та додатків сприяє кращій командній роботі та співпраці.

За територією охоплення телекомунікаційні мережі, що використовуються в Інтернеті речей, можна розділити на 4 основні типи:

1. Особиста мережа PAN (Personal Area Network) формується «навколо» людини та зазвичай об'єднує всі її особисті пристрої, такі як телефони, смартфони, ноутбуки, гарнітури тощо. У випадку з IoT така мережа будується навколо пристрою, а не навколо людини, і об'єднує різноманітні "речі".

2. Локальна мережа LAN (Local Area Network) зазвичай охоплює невелику територію, таких як будинки, офіси або підприємства. Також до цього типу мереж можна віднести мережу контролерів CAN (Controller Area Network), яка призначена для з'єднання різних виконавчих пристроїв та датчиків всередині певного підприємства.

3. Міська мережа MAN (Metropolitan Area Network) – поєднує користувачів і локальні мережі в межах якогось міста, є мережею, що в масштабі більша за LAN, але менша за WAN.

4. Глобальна мережа WAN (Wide Area Network) – з'єднує користувачів і мережі, розташовані на великих відстанях, від сотень до тисяч кілометрів.

Ієрархічну структуру комп'ютерних мереж представлено на Рис.1.1.

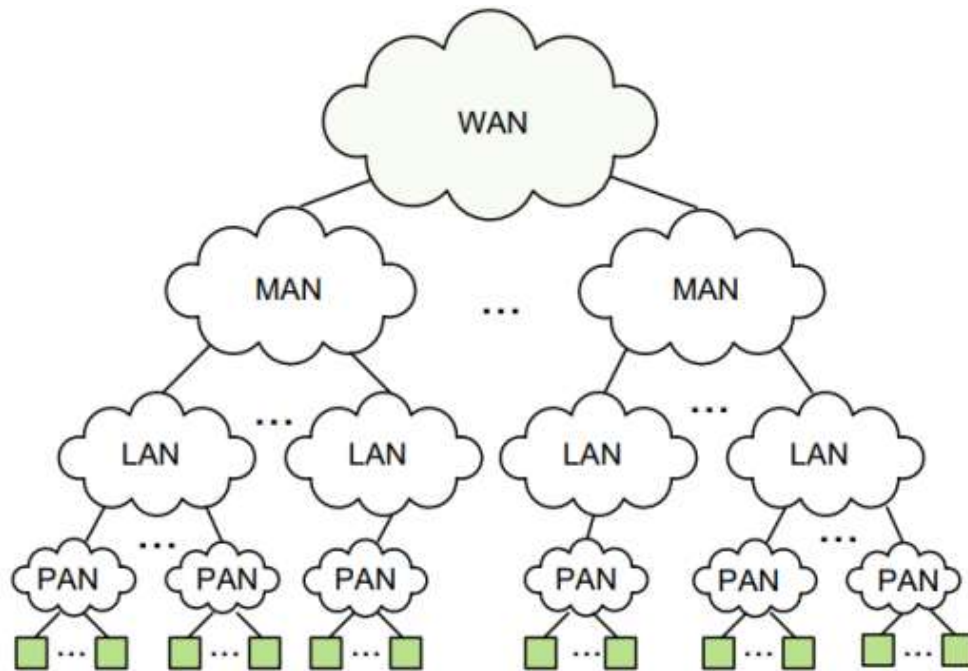


Рис.1.1 - Ієрархія комп'ютерних мереж

Інформаційні системи (ІС) є сутністю засобів зв'язку, які допомагають у зборі, збереженні, обробці, пошуку, надсиланні та представленні даних, адаптованих до конкретних цілей. Ці системи складаються з кількох інтегральних частин: людей, які ними користуються, вказівок щодо того, як вони повинні використовуватися, фактичних наборів даних, фізичних пристроїв для зберігання та обробки цих даних та програмного забезпечення для роботи цих пристроїв.

Кожна інформаційна система має життєвий цикл, який починається з її створення та продовжується з її постійним розвитком. Цей життєвий цикл поділений на відмінні фази: визначення того, що потрібно, розробка ідеї або плану, складання детальної специфікації, проектування системи, втілення її на практиці та подальше обслуговування. Кожна фаза має свій набір цілей і залучає різних зацікавлених сторін: системні аналітики визначають вимоги, програмісти будують систему та кінцеві користувачі використовують її. Підхід до розробки системи —

чи то це проста послідовна модель крок за кроком, повторюваний цикл вдосконалень чи динамічніша спіральна модель — впливає на те, наскільки адаптивним є процес розробки та як добре він може впоратися зі змінами по ходу справ. Стандартні способи використання цих інформаційних систем часто показані у діаграмі на кшталт Рис.1.2. [1]

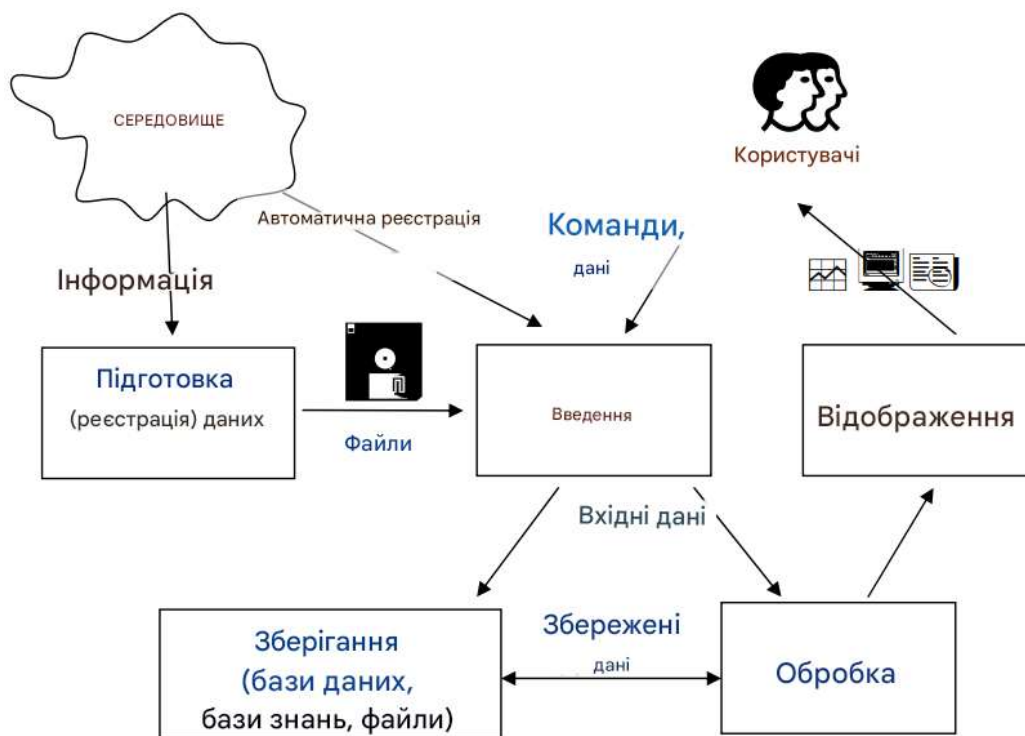


Рис.1.2 – Процес обробки даних

Під час розробки інформаційних систем необхідно дотримуватися основних принципів, зокрема системного підходу, постійного вдосконалення, забезпечення взаємодії, стандартизації та економічної ефективності. Методологія їх створення передбачає контроль складності проектування, чітке окреслення меж створюваної системи та забезпечення високої якості як кінцевого продукту, так і процесу його розробки. Планування розвитку інформаційної системи спрямоване на максимальну відповідність бізнес-завданням та підвищення ефективності їх реалізації шляхом оптимізації технологічних процесів. Важливо уникати помилок, які можуть виникнути через перенесення існуючих управлінських проблем у нову систему, оскільки це ускладнює її подальшу модернізацію. У процесі планування необхідно проаналізувати поточний стан системи, порівняти його з очікуваними результатами та визначити пріоритетні напрямки для автоматизації [2].

Топологія являє собою конфігурацію фізичних зв'язків між вузлами мережі. Вибір певної топології визначає характеристики роботи мережі. Рівень ефективності інформаційної інфраструктури в офісному середовищі напряму залежить від правильної організації мережевої топології. Вона визначає способи з'єднання між мережевими пристроями (сервери, маршрутизатори, комутатори, робочі станції), особливості передачі даних, а також рівень відмовостійкості та можливості розширення мережі.

Існує широкий спектр варіантів побудови мережеских з'єднань. Основні топології включають:

1. Шину
2. Зірку
3. Кільце

Окрім базових структур, існують додаткові варіанти топологій, які формуються шляхом комбінування основних. До них належать:

1. Подвійне кільце
2. Сотова топологія
3. Решітка
4. Дерево
5. Сніжинка
6. Повнозв'язна структура

Такі варіанти можуть бути віднесені до гібридних або змішаних топологій, але деякі з них, наприклад, "Дерево", отримали власні унікальні назви. [3]

1.2. Апаратне та програмне забезпечення офісних комп'ютерних мереж

У сучасному офісному середовищі робота комп'ютерних мереж ґрунтується на взаємодії апаратного та програмного забезпечення, що забезпечує стабільність, ефективність і безпеку інформаційної інфраструктури. До апаратних елементів належать фізичні пристрої, зокрема сервери, маршрутизатори, комутатори та кабельні системи. Програмне забезпечення, зі свого боку, включає операційні системи, мережеві інструменти, засоби для моніторингу та захисту. У цьому розділі детально аналізуються основні характеристики апаратного та програмного

забезпечення, а також обґрунтовується вибір програм, які будуть застосовуватися в межах цієї роботи.

Комп'ютерна мережа являє собою набір апаратних і програмних ресурсів, з'єднаних каналами передачі даних, що дозволяє обмінюватися інформацією та спільно використовувати ресурси. Завдяки її впровадженню вдається оптимізувати робочі процеси, централізувати управління та гарантувати безперебійний доступ до важливих даних. Ефективність мережі залежить від правильного вибору апаратних компонентів та їхньої сумісності з програмними рішеннями. Офісні мережі мають бути гнучкими та масштабованими, щоб підтримувати як локальні, так і віддалені робочі процеси.

Одним із ключових завдань системного адміністратора є вибір апаратних і програмних засобів, які формують інформаційну систему офісу. Від компетентності адміністратора залежить оптимальність підбраного обладнання та програмного забезпечення (ПЗ), що має відповідати як функціональним вимогам, так і фінансовим можливостям організації. У цьому підрозділі розглядаються основні аспекти вибору мережевого обладнання, зокрема маршрутизаторів Wi-Fi, з урахуванням їхньої продуктивності, вартості та функціональних характеристик. Метою є надання рекомендацій щодо оптимального вибору, який забезпечить стабільну роботу інформаційної інфраструктури офісу. Для побудови мережі в офісному приміщенні, розрахованому на певну кількість працівників, потрібно використати різне технічне оснащення [4].

Це включає:

- Пристрої для маршрутизації та комутації, які забезпечують рух даних;
- Кабельні дроти в бухтах та необхідні витратні матеріали;
- З'єднувальні кабелі, роз'єми, мережеві порти, панелі розподілу;
- Телекомунікаційні стійки з висувними відділеннями;
- Кріпильні елементи та допоміжні деталі.

Для стабільної роботи мережі в офісі рекомендується обирати пристрої від відомих брендів, які мають високий рівень надійності. Правильне налаштування всіх частин системи допомагає зменшити ризик технічних проблем та непередбачених витрат на обслуговування.

Перед початком монтажу мережі з нуля важливо спланувати шляхи прокладання кабелів. Пошкодження комунікацій під час робіт може спричинити серйозні ускладнення. Щоб уникнути цього, використовують спеціальні прилади для перевірки прихованої проводки, які дозволяють визначити місце розташування кабелів.

Якщо такого приладу немає, орієнтуються на розміщення електричних розеток та вимикачів, хоча цей метод не забезпечує високої точності. Щоб знизити ризик ушкодження силових або мережевих ліній, кабелі в офісі прокладають прямими лініями з кутами в 90°. Система структурованого кабелювання передбачає використання скручених пар, які підключаються через модульні конектори. Всі комунікації обов'язково маркуються, що значно полегшує технічне обслуговування, модернізацію та розширення мережі.

Після завершення прокладання кабелів та встановлення обладнання виконується етап конфігурації. Підключається доступ до інтернету, встановлюється серверне програмне забезпечення (наприклад, Windows Server), налаштовується робота бухгалтерських систем (1С) та інших корпоративних сервісів.

Основні елементи інформаційної інфраструктури офісу включають сервери Рис.1.3, маршрутизатори, комутатори Рис.1.4, кабельну систему Рис.1.5 та відповідне програмне забезпечення. Сервери виконують завдання зберігання даних, адміністрування баз даних, забезпечення роботи поштових служб та підтримки мережевих сервісів, таких як DHCP, DNS і Active Directory. Вони дозволяють централізовано зберігати документи, контролювати доступ до корпоративних програм і забезпечувати безпечний обмін інформацією в межах мережі [5].

Комутатори відіграють вирішальну роль у функціонуванні локальної мережі, оскільки забезпечують підключення пристроїв та розподіл трафіку. Завдяки їм можна об'єднати в єдину систему комп'ютери, принтери, сервери та інші пристрої, забезпечуючи при цьому високу швидкість передачі даних. Моделі з підтримкою технології PoE (Power over Ethernet) дозволяють жити такі пристрої, як точки

доступу Wi-Fi чи IP-камери, без додаткових джерел живлення, що спрощує встановлення обладнання та знижує витрати.

Кабельна інфраструктура є невід'ємною частиною мережі й може включати коаксіальні кабелі, виту пару або оптоволоконні лінії – вибір залежить від конкретних потреб. Основними критеріями при виборі кабельної системи є необхідна пропускна здатність мережі, відстань передачі сигналу та умови експлуатації.

Сучасні кабельні системи базуються на технології, відомій як вита пара. Цей кабель складається з кількох дротів, скручених між собою попарно та поміщених у спільну захисну оболонку. Вита пара буває двох основних типів: екранована та неекранована.

Екранована вита пара (STP, Shielded Twisted Pair) — це конструкція зі скручених дротів, додатково захищених спеціальною опліткою, що оберігає від зовнішніх електромагнітних перешкод.

Неекранована вита пара (UTP, Unshielded Twisted Pair) — як зрозуміло з назви, не має додаткового екранування, що робить її простішою та дешевшою у виробництві.

Для повного огляду варто згадати й інші види кабелів, що використовуються в мережах:

Коаксіальний кабель складається з центральної мідної жили, огорнутої екранувальною опліткою. Сьогодні він рідко застосовується в локальних мережах, оскільки поступився місцем витій парі через її переваги в гнучкості та ефективності.

Оптоволоконний кабель використовує оптичне волокно як основу для передачі даних. Він вирізняється високою швидкістю, стійкістю до перешкод і застосовується там, де потрібна максимальна пропускна здатність та надійність зв'язку.

Таким чином, вита пара залишається основою сучасних кабельних систем, тоді як коаксіальні та оптоволоконні кабелі виконують свої специфічні функції залежно від потреб мережі.



Рис.1.3 - Сервери



Рис.1.4 - Комутатор

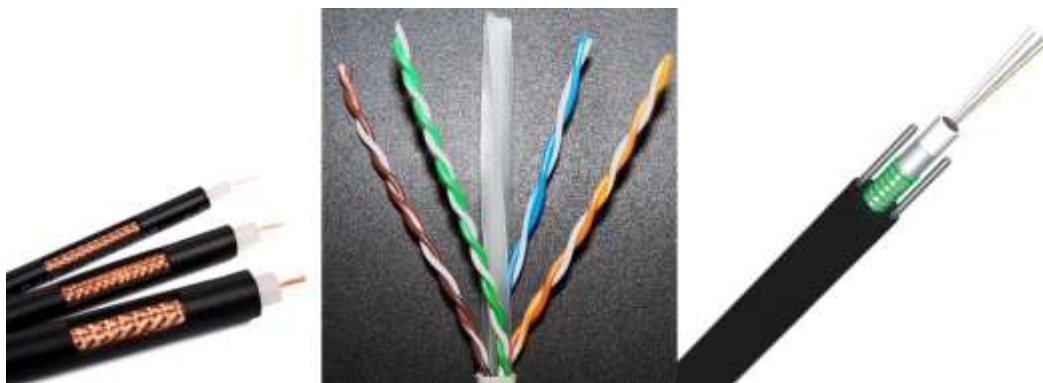


Рис.1.5 – Клоаксальний, вита пара, оптоволоконний кабель

Ethernet є однією з найпоширеніших технологій для організації локальних комп'ютерних мереж (LAN), яка здобула популярність завдяки своїй простоті впровадження та економічній доцільності. Вона функціонує на фізичному рівні мережевої моделі OSI і стала стандартом для корпоративних мережних інфраструктур.

Ethernet підтримує різні стандарти швидкості, від 10 мегабітів за секунду до 10 гігабітів за секунду. Для з'єднань зазвичай використовуються два типи кабелів:

мідна вита пара або оптоволоконний кабель. Це забезпечує гнучкість у виборі залежно від потреб мережі.

Хоча Ethernet є дротяною технологією, мережі на його основі можуть інтегруватися з бездротовими рішеннями, такими як Wi-Fi, створюючи комплексні системи зв'язку. Це дозволяє поєднувати переваги обох підходів для більшої гнучкості. На сьогоднішній день існують такі класи технології Ethernet [6]:

- 10 Base XX - передача зі швидкістю до 10 Мбіт/с;
- 100 Base XX - передача зі швидкістю до 100 Мбіт/с;
- 1000 Base XX - передача зі швидкістю до 1000 Мбіт/с;
- 10 GBase XX - передача зі швидкістю до 10 Гбіт/с.

Таблиця 1.1

Характеристики сімейства технологій Ethernet

	Ethernet	FastEthernet	GigabitEthernet	10 Gigabit Ethernet
Швидкість, Мбіт/с	10	100	1000	10000
Середа передачі	Скручена пара, коаксіальний кабель, оптоволоконно	Скручена пара, оптоволоконно	Оптоволоконно, скручена пара	Скручена пара, оптоволоконно
Стандарти для реалізації	10 Base2 10 BaseT 10 Base5 10 Base FL 10 Base F	100 Base TX 100 Base T4 100 Base-FX 100 Base-SX 100 Base T2	1000 Base-TX 1000 Base-LX 1000 Base-SX 1000 Base-CX 1000 Base-T	10 GBase CX4 10 GBase SR 10 GBase LR 10 GBase SW 10 GBase T
Топологія	Шина, зірка	Зірка	Зірка	Зірка

Апаратне забезпечення повинно відповідати вимогам щодо продуктивності, надійності та енергоефективності. Наприклад, для офісного приміщення, де функціонує 10 робочих місць, доцільно використовувати один високопродуктивний сервер, маршрутизатор середнього рівня та декілька комутаторів, що забезпечать ефективний розподіл мережевого трафіку.

Програмне забезпечення для офісних мереж відіграє вирішальну роль у керуванні апаратними ресурсами, автоматизації процесів роботи та забезпеченні захисту даних. Воно поділяється на кілька основних категорій, кожна з яких має специфічні функції для підтримки ефективної роботи мережі.

Операційні системи. Операційна система є базовим рівнем, який забезпечує взаємодію між апаратною частиною комп'ютера та програмами, що на ньому працюють. У межах створеної інфраструктури для серверів обрано операційну систему Windows Server 2012, оскільки вона пропонує широкі можливості для адміністрування мережі, інтеграції з Active Directory та реалізації групових політик. Це рішення дозволяє централізовано регулювати доступ користувачів, автоматизувати розподіл IP-адрес за допомогою DHCP та гарантувати стабільну роботу служби DNS.

Для робочих станцій основною операційною системою стане Windows 10. Вона вирізняється зручним інтерфейсом, має вбудовані засоби безпеки, зокрема Windows Defender, і забезпечує сумісність із більшістю програм, які використовуються в офісному середовищі.

Мережеві служби управління. Для забезпечення ефективного функціонування мережі необхідно застосовувати спеціалізовані служби:

DHCP (Динамічний протокол конфігурації хоста): Цей протокол автоматично призначає IP-адреси підключеним пристроям, зменшуючи потребу в ручному налаштуванні мережі. У рамках реалізації проєкту сервер на базі Windows Server 2012 виконуватиме функції DHCP-сервера.

DNS (Система доменних імен): Забезпечує перетворення доменних імен на відповідні IP-адреси, що пришвидшує доступ до мережевих ресурсів. Крім того, інтеграція DNS із Active Directory підвищує ефективність роботи мережевої інфраструктури.

Active Directory: Це служба каталогів, розроблена компанією Microsoft, яка дає змогу централізовано керувати користувачами, групами та підключеними пристроями. У нашій мережі Active Directory буде основним інструментом для контролю доступу.

Інструменти моніторингу та безпеки. Для контролю стану мережевої інфраструктури та забезпечення безпеки використовуватимуться такі інструменти:

Zabbix: Це система моніторингу з відкритим кодом, призначена для аналізу продуктивності серверів, мережевого обладнання та інших пристроїв. Вона дозволяє в реальному часі відстежувати параметри, такі як навантаження на

процесор, використання оперативної пам'яті та мережевий трафік, а також створювати детальні звіти.

Event Viewer: Потужний інструмент автоматизації та адміністрування від Microsoft, який застосовуватиметься для аналізу журналів безпеки, перевірки конфігурації мережі та виявлення можливих відхилень.

Таблиця 1.2

Огляд програмного забезпечення

Категорія	Програма	Призначення
Операційна система (сервер)	Windows Server 2012	Управління мережею, підтримка служб DHCP, DNS, Active Directory
Операційна система (клієнт)	Windows 10	Забезпечення робочого середовища для користувачів
Моніторинг	Zabbix	Відстеження продуктивності мережі та обладнання
Безпека та аналіз	Event Viewer	Автоматизація адміністрування та аналіз логів безпеки
Прикладне ПЗ	Microsoft Office Suite	Виконання офісних завдань (документи, таблиці, презентації)

Фізичні компоненти мережі визначають її матеріальну основу та характеристики, тоді як програмні інструменти забезпечують оптимальне та ефективне використання цієї мережі. Наприклад, сервер на базі Windows Server 2012 може одночасно виконувати роль DHCP- та DNS-сервера, тоді як Zabbix дозволяє адміністратору в реальному часі стежити за навантаженням системи чи виникненням збоїв. У свою чергу, Event Viewer надає можливість швидкого аналізу журналів безпеки, що є надзвичайно важливим для захисту від потенційних загроз.

1.3. Методи та засоби системної інженерії для підвищення ефективності офісних середовищ

Системна інженерія являє собою всеосяжний метод, який застосовується для створення, впровадження та адміністрування складних систем, зокрема тих, що становлять основу інформаційної інфраструктури офісних приміщень. Її головна

мета полягає в забезпеченні максимальної ефективності, надійності та здатності до розширення таких систем. У контексті офісних комп'ютерних мереж системна інженерія зосереджується на вирішенні типових проблем, таких як перевантаження мережі, нестабільність Wi-Fi-з'єднання та різноманітні ризики для безпеки. Використання спеціалізованих методів і технологій сприяє оптимізації робочих процесів і підвищенню загальної продуктивності.

Перевантаження комп'ютерних мереж часто виникає через одночасне підключення великої кількості пристроїв або передачу значних обсягів даних. Наприклад, це може відбуватися під час проведення відеоконференцій або виконання резервного копіювання, що призводить до затримок у передачі даних і погіршення роботи системи. Проблеми зі слабким сигналом Wi-Fi зазвичай проявляються в приміщеннях із товстими стінами, численними перешкодами або недостатньою кількістю точок доступу. Це може створювати труднощі для стабільного з'єднання, особливо для працівників, які працюють віддалено. Ризики для безпеки включають несанкціонований доступ, зараження вірусами, фішингові атаки та витік конфіденційної інформації. Особливо небезпечною ситуація стає, коли до корпоративної мережі підключаються пристрої без належного захисту, наприклад, гостьові ноутбуки, що становить загрозу для інформаційних ресурсів компанії.

Для вирішення цих проблем системна інженерія передбачає використання низки ефективних інструментів. Одним із таких є механізм якості обслуговування (QoS), який дозволяє розподіляти мережевий трафік залежно від рівня пріоритетності. Наприклад, критичні сервіси, такі як відеозв'язок або телефонія, отримують перевагу в доступі до ресурсів, тоді як менш важливі процеси, як завантаження файлів, мають нижчий пріоритет. Це допомагає уникнути значних затримок у години пікового навантаження. Ще одним важливим елементом є брандмауери, які підвищують рівень захисту системи, блокуючи потенційно небезпечні IP-адреси та обмежуючи доступ із неавторизованих джерел відповідно до встановлених правил безпеки.

Окрім базових рішень, системна інженерія також включає вдосконалення мережевої інфраструктури шляхом оптимізації її топології та впровадження

технологій сегментації, таких як VLAN (віртуальні локальні мережі). Це дозволяє рівномірно розподіляти трафік між різними групами користувачів, значно зменшуючи навантаження на мережеве обладнання. Для централізованого керування правами доступу, налаштуваннями користувачів та груп широко застосовується Active Directory, що значно спрощує адміністрування системи та допомагає обмежити доступ до конфіденційної інформації, мінімізуючи ризики витоку даних.

Підвищення безпеки офісної мережі досягається також через впровадження технології VPN (віртуальних приватних мереж), яка забезпечує шифрування віддалених підключень, та регулярне оновлення програмного забезпечення для усунення потенційних вразливостей. Одним із критично важливих аспектів захисту інформації є організація процесів резервного копіювання, що дозволяє уникнути втрати даних у разі збоїв або кібератак. Автоматизоване збереження інформації на незалежних носіях або в хмарних сховищах значно підвищує рівень захисту корпоративних даних. Додатково, використання спеціалізованих інструментів моніторингу, таких як Zabbix, дає можливість у реальному часі відстежувати стан мережі, виявляти перевантаження або проблеми зі зниженням пропускної здатності та оперативно реагувати на потенційні загрози.

Важливим аспектом системної інженерії є використання моделей під час проектування складних систем, таких як офісні комп'ютерні мережі. Моделі відіграють ключову роль у забезпеченні того, щоб кінцева система відповідала вимогам і очікуванням користувачів. Для цього необхідно дотримуватися таких вимог:

1. Моделі мають бути відображенням майбутньої реальності. Щоб це забезпечити, необхідно:
 - зробити моделі зрозумілими для користувачів, щоб вони могли легко сприймати інформацію та брати участь у процесі розробки;
 - залучати користувачів до створення системи: усі компоненти інформаційної системи, які стосуються їхньої діяльності, мають бути розглянуті та узгоджені з ними;

- розробляти моделі на основі порівняння поточного стану ("як є") з бажаним ("як має бути"), що дозволяє чітко визначити цілі та напрямки вдосконалення.

2. Кожна модель повинна бути завершеною і логічно цілісною. Це означає, що кожна модель має містити всі необхідні елементи для повного опису певного аспекту системи та не містити суперечностей у своїй структурі.

3. Система моделей має бути всебічною. Між моделями не повинно виникати розбіжностей, для чого вони мають послідовно пов'язуватися одна з одною, а їхні складові частини — гармоніювати між собою. Це забезпечує цілісність проекту та узгодженість усіх компонентів системи.

Таблиця 1.3

Чинники, що впливають на якість інформаційної системи

	Відповідність очікуванням/вимогам користувачів	Гнучкість -Розширюваність -Можливості супроводу	Універсальність
Якість конструкції	-Ступінь відповідності очікуванням/вимогам користувачів -Зміна вимог у процесі розробки	-Незалежність частоти (висока внутрішня зв'язаність компонент кожної частини, низький ступінь залежності частоти для від одного) -Нормалізація структури даних -Структурність процесів обробки даних	-Використання стандартних технологій та систем запису -Наявність зрозумілої документації та конструкції в цілому -Контроль змін
Якість виготовлення	-Продуктивність -Доступність описаних проектних рішень -Кількість помилок -Кількість ненормальних завершень	-Модульність -Структурний код	-Використання стандартних технологій та систем запису -Читання коду -Контроль змін

Використання моделей у системній інженерії дозволяє не лише візуалізувати майбутню систему, а й виявляти потенційні проблеми на ранніх етапах розробки,

що значно знижує ризики та витрати на виправлення помилок у майбутньому. Наприклад, моделювання мережі з урахуванням розміщення точок доступу Wi-Fi та розподілу трафіку через VLAN може заздалегідь показати можливі "вузькі місця" і допомогти оптимізувати інфраструктуру ще до її фізичного впровадження.

Основними принципами системної інженерії є цілісність, ієрархічність та адаптивність, що означає розгляд усіх компонентів мережевої інфраструктури як єдиної системи. Наприклад, проблему перевантаженості мережі можна вирішити не лише за допомогою QoS, а й завдяки правильному розташуванню точок доступу Wi-Fi з урахуванням особливостей приміщення. Аналогічно, зниження рівня кіберзагроз можливе не лише за рахунок використання брандмауерів, а й шляхом проведення навчання персоналу та впровадження політик складних паролів у Active Directory.

Ефективність зазначених методів підтверджується їх широким застосуванням у корпоративних мережах. Наприклад, завдяки QoS затримки у передачі даних у години пікового навантаження можуть скоротитися на 30–50%, а використання Active Directory здатне зменшити час, необхідний для адміністрування користувачів, удвічі порівняно з ручним управлінням. Таким чином, системна інженерія забезпечує комплексний підхід до оптимізації офісного середовища, дозволяючи ефективно управляти ресурсами, підвищувати рівень безпеки та забезпечувати стабільну роботу мережевої інфраструктури. Використання таких технологій, як QoS, брандмауери, Active Directory, Zabbix та VPN, у поєднанні з моделюванням, сприяє побудові надійних, безпечних і продуктивних комп'ютерних мереж, що є ключовим фактором успішної роботи сучасних організацій.

1.4. Висновки до розділу 1

У першому розділі роботи проведено детальний огляд сучасного стану проблем, пов'язаних із формуванням інформаційної інфраструктури для офісних умов. Було проаналізовано ключові складові такої інфраструктури, зокрема сервери, маршрутизатори, комутатори, кабельні системи та програмне забезпечення, які відіграють вирішальну роль у її функціонуванні. Досліджено, що

правильний вибір топології мережі, а також відповідного апаратного та програмного забезпечення є критично важливим для забезпечення стабільної роботи, високої продуктивності та надійного захисту офісної мережі.

Окрім того, було вивчено основні труднощі, які можуть виникати під час впровадження та управління корпоративними мережами. Зокрема, виявлено проблеми, пов'язані з перевантаженням мережевого трафіку через інтенсивне використання, слабким сигналом Wi-Fi через фізичні перешкоди чи недостатню кількість точок доступу, а також із загрозами кібербезпеки через еволюцію методів атак. Для вирішення цих питань розглянуто підходи системної інженерії, зокрема використання технології QoS для пріоритизації трафіку, впровадження міжмережевих екранів для захисту від зовнішніх загроз, а також застосування моніторингових інструментів, таких як Zabbix, для контролю стану мережевої інфраструктури.

На основі проведеного аналізу визначено головну мету роботи — створення ефективної та захищеної офісної мережі, яка сприятиме стабільному функціонуванню інформаційної інфраструктури, оптимізації бізнес-процесів та підвищенню продуктивності працівників. Для досягнення цієї мети сформульовано такі ключові завдання:

1. Провести аналіз існуючих методів побудови комп'ютерних мереж і обрати оптимальні рішення для офісного середовища.
2. Вибрати відповідне апаратне та програмне забезпечення, яке відповідатиме вимогам продуктивності, масштабованості та безпеки.
3. Оптимізувати процеси маршрутизації, розподілу IP-адрес та управління доступом до мережевих ресурсів.
4. Впровадити механізми централізованого адміністрування та групові політики для автоматизації керування користувачами та пристроями.
5. Оцінити ефективність запропонованих рішень та розробити рекомендації для їх подальшого вдосконалення.
6. Реалізація цих завдань сприятиме створенню надійної та гнучкої інформаційної інфраструктури, яка відповідатиме сучасним вимогам і стандартам, застосовуваним до офісних мереж.

РОЗДІЛ 2

АПАРАТНІ КОМПОНЕНТИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ОФІСНОГО СЕРЕДОВИЩА

2.1. Проектування логічної схеми мережі

Проектування логічної схеми мережі є одним із ключових етапів створення інформаційної інфраструктури офісного середовища. Цей процес охоплює організацію віртуальних локальних мереж (VLAN) а також маршрутизацію для забезпечення ефективного обміну даними, безпеки та зручності адміністрування. У рамках цього підpunkту розглядається структура мережі для двоповерхового офісу з різними відділами, кожен із яких має свої функціональні особливості та вимоги до доступу до мережевих ресурсів. Основною метою є створення логічної схеми, яка забезпечить стабільність роботи, ізоляцію трафіку між відділами, можливість масштабування та безпечний віддалений доступ до корпоративних даних.

Логічну схему офісної мережі побудовано у середовищі Cisco Packet Tracer, як показано на Рис.2.6 [7].

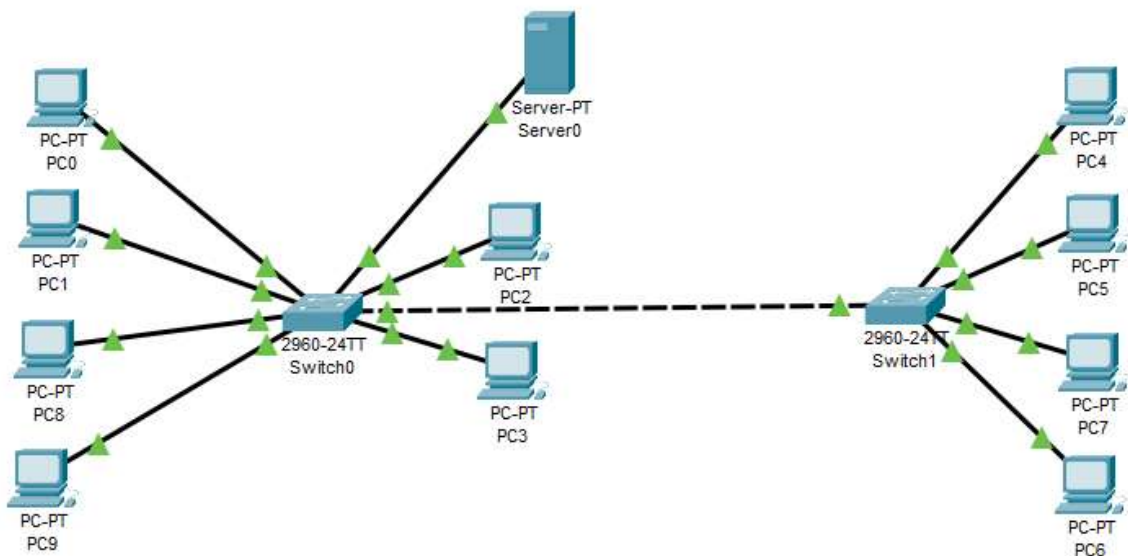


Рис.2.6 – Схема мережі

Для розробки логічної схеми мережі використано програмне забезпечення Cisco Packet Tracer, яке є стандартним інструментом для моделювання мережевих топологій і перевірки їхньої працездатності. У створеній схемі використано наступне обладнання: 10 персональних комп'ютерів (ПК), 1 сервер та 2 свічі. Такий набір пристроїв дозволяє реалізувати всі необхідні функції мережі, включаючи підключення робочих станцій та зв'язок із зовнішніми мережами. Мережа поділена

на кілька логічних сегментів за допомогою технології VLAN, яка дозволяє ізолювати трафік і підвищити безпеку. Кожен відділ офісу має власну VLAN, що забезпечує чітке розділення робочих груп і зменшує ймовірність несанкціонованого доступу до даних. Структура VLAN виглядає так:

- *VLAN 2 (adm):* призначена для адміністративно-фінансового відділу, який розташований на першому та другому поверхах. На першому поверсі у відділі працюють два співробітники (наприклад, бухгалтер і кадровик), які використовують два ПК, а на другому поверсі — ще два (юрист і адміністратор), також із двома ПК.

- *VLAN 3 (op):* охоплює операційний відділ на першому поверсі, де два співробітники (логіст і спеціаліст із закупівель) використовують два ПК.

- *VLAN 4 (it):* створена для ІТ-відділу на першому поверсі з двома ПК для системного адміністратора та спеціаліста технічної підтримки.

- *VLAN 5 (prodaga):* включає відділ продажів і маркетингу на другому поверсі, де два співробітники (менеджери з продажу та маркетолог) працюють із двома ПК.

- *VLAN 6 (server):* Один сервер розміщений у зоні ІТ-відділу та виконує функції DHCP, DNS і Active Directory, забезпечуючи централізоване управління мережею. Два свічі слугують для підключення всіх пристроїв на кожному поверсі, утворюючи основу топології "зірка". Розподіл IP-адрес виконано в межах підмережі 192.168.0.0/24, що забезпечує достатню кількість адрес для всіх пристроїв і простоту конфігурації. У Cisco Packet Tracer кожен пристрій отримав унікальну IP-адресу, враховуючи його роль у мережі. Детальний розподіл виглядає так:

- *Перший поверх:*
 - Адміністративно-фінансовий відділ (VLAN 2): 192.168.2.1–192.168.2.2 для двох ПК.
 - Операційний відділ (VLAN 3): 192.168.3.1–192.168.3.2 для двох ПК.
 - ІТ-відділ (VLAN 4): 192.168.4.1–192.168.4.2 для двох ПК.
 - Сервер (VLAN 6): 192.168.6.1
- *Другий поверх:*

- Адміністративно-фінансовий відділ (VLAN 2): 192.168.2.3–192.168.2.4 для двох ПК.
- Відділ продажів і маркетингу (VLAN 5): 192.168.5.1–192.168.5.2 для двох ПК.

Для підтвердження працездатності спроектованої логічної схеми мережі було проведено симуляцію в програмному комплексі Cisco Packet Tracer. Модель відтворювала топологію «зірка», що включає два комутатори Cisco Catalyst 2960-S, сервер Supermicro (IP-адреса 192.168.6.1) та десять робочих станцій, розподілених між VLAN 2–5. Зокрема, VLAN 2 об'єднує робочі станції ПК 1 (IP-адреса 192.168.2.1) і ПК 4 (IP-адреса 192.168.2.4), розташовані на різних поверхах офісу та підключені до відповідних комутаторів через порти, що належать до цього VLAN (див. Додаток А). Додавання робочих станцій робітників до VLAN відбувається завдяки консольному програмуванню комутатора (див. Додаток Б). Налаштування транкових портів між комутаторами Switch0 і Switch1 забезпечувало передачу трафіку між VLAN (див. Додаток В).

У ході симуляції було змодельовано передачу даних між ПК 1 і ПК 4 у межах VLAN 2 для перевірки коректності сегментації трафіку, стабільності з'єднань та працездатності мережевої інфраструктури. Процес передачі імітувався шляхом відправлення пакета даних від ПК 1 до ПК 4, що дозволило відстежити маршрут і час проходження через мережу. Результати, відображені в панелі симуляції Cisco Packet Tracer, показали, що пакет успішно передався від ПК 1 через Switch0 до Switch1, а потім до ПК 4 із загальною затримкою, яка не перевищувала 0,006 секунди (див. Рис. 2.7). Події в журналі симуляції підтвердили послідовність обробки: відправлення пакета з ПК 1 (0,000 с), передача через Switch0 (0,001–0,003 с), маршрутизація через транковий порт до Switch1 (0,004–0,005 с) і доставка до ПК 4 (0,006 с). Відсутність конфліктів IP-адрес та помилок у передачі свідчить про правильність конфігурації DHCP-сервера та розподілу адрес у діапазоні 192.168.2.0/24.

Сегментація VLAN 2 забезпечила ізоляцію трафіку, що підтверджено спробою відправлення пакета з ПК 1 до пристрою в іншому VLAN (наприклад, ПК 5 у VLAN 3), яка була заблокована без додаткових правил маршрутизації. Це

підкреслює ефективність запропонованої топології та налаштувань для підвищення безпеки мережі.

Отже, результати симуляції підтверджують коректність проектування логічної схеми мережі, її готовність до реального впровадження та потенціал для подальшого розширення. Для візуалізації процесу передачі даних наведено схему топології з позначенням маршруту пакета (Рис. 2.7 – 2.8).

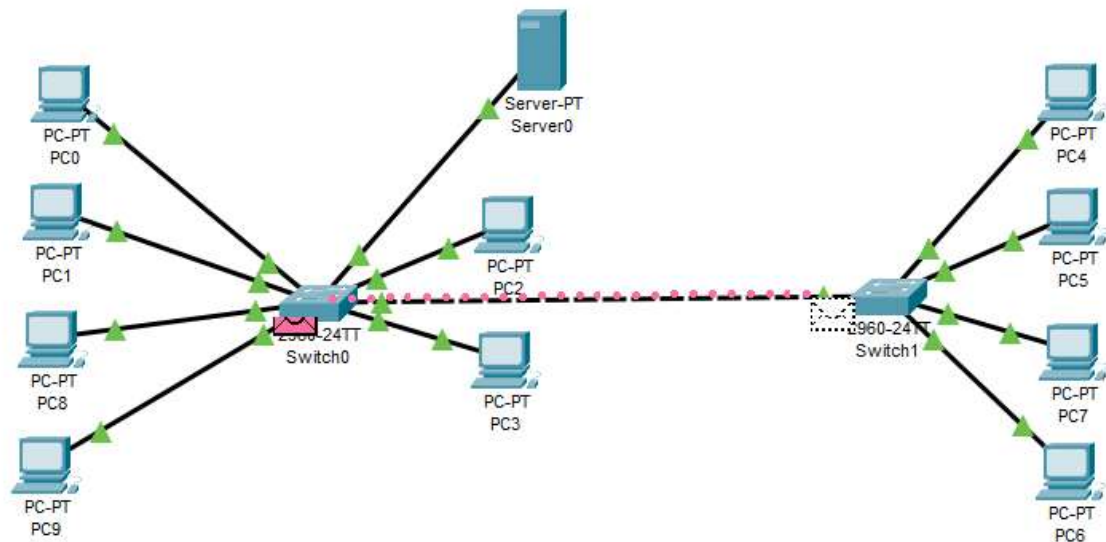


Рис.2.7 – Логічна схема мережі з симуляцією передачі даних між ПК 1 і ПК 4 у VLAN 2

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.000	--	PC0	ARP
	0.001	PC0	Switch0	ARP
	0.002	Switch0	PC1	ARP
	0.002	Switch0	Switch1	ARP
	0.003	Switch1	PC4	ARP
	0.003	Switch1	PC5	ARP
	0.004	PC4	Switch1	ARP
	0.005	Switch1	Switch0	ARP
	0.006	Switch0	PC0	ARP
	0.006	--	PC0	ICMP

Рис.2.8 – Журнал подій у симуляційному режимі Cisco Packet Tracer

Для автоматизації призначення IP-адрес сервер налаштовано як DHCP-сервер, який динамічно розподіляє адреси в межах зазначених діапазонів. Це дозволяє легко додавати нові пристрої без необхідності ручного введення параметрів, що особливо зручно для ноутбуків, які можуть використовуватися

віддалено або в різних зонах офісу. Топологія мережі обрана у вигляді "зірки", що є оптимальним рішенням для невеликого офісу з двома поверхами. У центрі кожного поверху розташовано свіч, до якого підключені всі ПК, ноутбуки та сервер. Перший свіч на першому поверсі з'єднує пристрої VLAN 2, 3 і 4, а також VLAN 6 сервера, тоді як другий свіч на другому поверсі обслуговує VLAN 2 і 5. У Cisco Packet Tracer ця топологія дозволяє легко візуалізувати зв'язки між пристроями та перевірити їхню працездатність.

Переваги "зірки" включають [8]:

- *простоту розширення*: додавання нових пристроїв можливе шляхом підключення до свіча без зміни всієї структури;
- *надійність*: вихід із ладу одного ПК не впливає на роботу інших;
- *централізоване управління*: свічі дозволяють налаштовувати VLAN і контролювати трафік із однієї точки.

На першому поверсі свіч розміщений у серверній шафі поруч із IT-відділом, що полегшує доступ для адміністраторів. Сервер (192.168.6.1) розташований там же і підключений до цього свіча, виконуючи функції управління мережею.

На другому поверсі другий свіч розміщений у зручному місці для підключення ПК і ноутбуків, а також із можливістю додавання точки доступу Wi-Fi для бездротового зв'язку.

Схема, створена в Cisco Packet Tracer, включає всі згадані пристрої: 10 ПК розподілені між відділами на двох поверхах, 1 сервер забезпечує централізоване управління, а 2 свічі формують основу топології.

У програмі також налаштовано базові параметри, такі як IP-адреси, VLAN і правила маршрутизації, що дозволяє протестувати мережу перед фізичною реалізацією.

Логічна схема інтегрується з програмними компонентами, такими як Active Directory для управління користувачами та DNS для швидкого доступу до ресурсів. Кожен ПК і ноутбук зареєстрований у домені, що дозволяє застосовувати групові політики для обмеження доступу залежно від ролі співробітника.

Наприклад, бухгалтер із VLAN 2 матиме доступ до фінансових баз даних, а маркетолог із VLAN 5 — лише до рекламних матеріалів.

Отже, логічна схема мережі, спроектована в Cisco Packet Tracer, забезпечує ефективну організацію інформаційної інфраструктури офісу. Використання VLAN ізолює трафік між відділами, а маршрутизація через два роутери забезпечує зв'язок із зовнішніми мережами. Набір із 10 ПК, 1 сервера і 2 свічів відповідає потребам офісу та дозволяє легко масштабувати мережу в майбутньому.

Таблиця 2.4

Розподіл IP адресації

Відділ	Поверх	Кількість ПК	IP-діапазон	VLAN	Назва VLAN
Сервер	1	-	192.168.6.1	6	server
Адмін-фінансовий	1/2	4	192.168.2.1–2.4	2	adm
Операційний	1	2	192.168.3.1–3.2	3	op
ІТ	1	2	192.168.4.1–4.2	4	it
Відділ продажів та маркетингу	2	2	192.168.5.1–0.2	5	prodaga

2.2. Вибір мережевого обладнання

Сучасний ринок пропонує широкий асортимент апаратного та програмного забезпечення, що відрізняється за технічними параметрами, вартістю та функціональними можливостями. Таке різноманіття створює певні труднощі під час вибору, оскільки адміністратору необхідно враховувати не лише поточні потреби офісу, але й можливості масштабування системи в майбутньому. У минулому проблема вибору часто була відсутньою через обмежену кількість доступних рішень, що змушувало використовувати наявне обладнання незалежно від його відповідності вимогам. Сьогодні ж завдання вибору ускладнене через велику кількість альтернатив, що потребує ретельного аналізу характеристик і співвідношення ціни та якості [9].

Аналіз вибору свитча. Ринок мережевого обладнання пропонує широкий асортимент пристроїв від різних виробників, таких як Cisco, TP-Link, D-Link, Ubiquiti та інших, що відрізняються за технічними характеристиками, вартістю та функціональними можливостями.

Вибір конкретної моделі для офісу середнього розміру, де передбачається використання кількох комп'ютерів, сервера та підключення до зовнішніх мереж, вимагає врахування таких параметрів, як пропускна здатність, підтримка технологій VLAN і PoE, надійність, масштабованість, простота управління та економічна доцільність. Для порівняння, я розглянув кілька популярних моделей комутаторів, які могли б бути застосовані в такому офісі, і поясню, чому Cisco Catalyst 2960-S виявився кращим вибором.

Першою моделлю для аналізу є Cisco Catalyst 2960-S [10], який характеризується пропускною здатністю до 176 Гбіт/с і швидкістю пересилання пакетів до 41,7 Mpps, що значно перевищує потреби невеликого офісу, але забезпечує запас продуктивності для майбутнього зростання. Цей комутатор оснащений 24 або 48 портами Ethernet 10/100/1000 Мбіт/с, підтримує PoE для живлення пристроїв, таких як точки доступу Wi-Fi чи IP-камери, а також має 4 SFP-порти для оптоволоконного підключення, що дозволяє інтегрувати його в гібридні мережі з високошвидкісними магістралями.

Функціональність Cisco включає підтримку VLAN для сегментації трафіку між різними групами користувачів, QoS для пріоритизації критичного трафіку, такого як відеоконференції чи голосовий зв'язок, і базову маршрутизацію рівня 2+, що додає гнучкості в управлінні мережею. Надійність пристрою підтверджується високим показником MTBF (понад 300 000 годин) і репутацією Cisco як лідера в корпоративному сегменті, а технологія FlexStack дозволяє об'єднати до 4 комутаторів у стек, що ідеально для масштабування офісу при збільшенні кількості робочих місць чи додаванні нових зон.

Управління здійснюється через професійний інтерфейс командного рядка (CLI), веб-інтерфейс і підтримує SNMP для інтеграції з системами моніторингу, що забезпечує зручність адміністрування. Вартість Cisco Catalyst 2960-S коливається в середньому діапазоні (\$500–\$1000 для refurbished моделей у 2025 році), що робить його дорожчим за бюджетні альтернативи, але виправданим для офісів, де стабільність і продуктивність є пріоритетом.

Другою моделлю для порівняння є TP-Link TL-SG3428, який пропонує пропускну здатність до 56 Гбіт/с і ту ж швидкість пересилання пакетів (41,7 Mpps),

що достатньо для базових офісних потреб, але значно поступається Cisco при високих навантаженнях. Він має 24 порти Gigabit Ethernet і 4 SFP-порти, а в деяких модифікаціях підтримує PoE, що робить його схожим на Cisco за базовими характеристиками.

TP-Link підтримує VLAN, QoS і STP, але його функціональність обмежена порівняно з Catalyst 2960-S, зокрема відсутністю стекування та менш розвиненими можливостями маршрутизації. Надійність цього комутатора середня, з MTBF близько 200 000 годин, що нижче, ніж у Cisco, а управління здійснюється переважно через веб-інтерфейс із базовим CLI, що може бути недостатньо для складних мереж. Вартість TP-Link становить \$150–\$250, що робить його привабливим для бюджетних проєктів, але економія на якості компонентів може призвести до частих збоїв при інтенсивному використанні.

Третьою моделлю є D-Link DGS-1210-28 із пропускну здатністю 56 Гбіт/с і швидкістю пересилання 41,7 Mpps, що аналогічно TP-Link і підходить для невеликих офісів із помірним трафіком. Він оснащений 24 портами Gigabit Ethernet і 4 SFP-портами, з опціональною підтримкою PoE, але не пропонує стекування чи розширених функцій маршрутизації.

Функціональність включає VLAN, QoS і базові ACL, але поступається Cisco за гнучкістю налаштувань. Надійність D-Link також середня (MTBF 200 000–250 000 годин), а управління обмежене веб-інтерфейсом із мінімальним CLI, що ускладнює інтеграцію з професійними системами моніторингу. Вартість моделі становить \$200–\$300, що позиціонує її в бюджетному сегменті, але, як і у випадку з TP-Link, нижча ціна супроводжується компромісами в довговічності та продуктивності.

Четвертою альтернативою можна розглядати Ubiquiti UniFi Switch USW-24, який має пропускну здатність 52 Гбіт/с і 24 порти Gigabit Ethernet із підтримкою PoE на деяких портах, а також 2 SFP-порти. Цей комутатор інтегрується з екосистемою UniFi, що забезпечує зручне централізоване управління через UniFi Controller, але не підтримує CLI в традиційному розумінні, що може бути незручним для адміністраторів, звиклих до Cisco.

Ubiquiti пропонує VLAN і QoS, але поступається за продуктивністю (52 Гбіт/с проти 176 Гбіт/с у Cisco) і не має стекування, хоча його ціна (\$200–\$400) є конкурентною.

Тепер поясню, чому Cisco Catalyst 2960-S був обраний для моєї мережі. По-перше, для офісу з кількома групами користувачів, де потрібна ізоляція трафіку, наприклад, між фінансовими працівниками, операційним відділом і технічною підтримкою, Cisco ідеально підходить завдяки високій пропускну здатності 176 Гбіт/с і розширеній підтримці VLAN, що забезпечує безпечний і ефективний розподіл ресурсів.

По-друге, підтримка PoE є ключовою для живлення точок доступу Wi-Fi чи інших пристроїв, таких як IP-телефони, і Cisco забезпечує це на всіх портах із достатньою потужністю, тоді як у TP-Link і D-Link ця функція доступна лише в дорожчих модифікаціях, що може збільшити загальні витрати.

По-третє, висока продуктивність і надійність Cisco гарантують стабільну роботу мережі навіть при одночасному підключенні великої кількості пристроїв і в умовах пікових навантажень, таких як передача великих обсягів даних чи потокового відео, що є важливим для сучасного офісу.

По-четверте, інтеграція з системами управління, такими як серверні служби чи інструменти моніторингу, значно спрощується завдяки підтримці SNMP і професійному CLI, що робить Cisco кращим вибором для адміністрування складних мереж із централізованим контролем.

Хоча TP-Link і D-Link дешевші, їхня нижча пропускну здатність (56 Гбіт/с) і відсутність стекування роблять їх менш придатними для офісів із перспективою зростання, а Ubiquiti, хоч і зручний у керуванні через власну платформу, не пропонує такої ж продуктивності та гнучкості конфігурації, як Cisco.

Крім того, Cisco Catalyst 2960-S має технологію EnergyWise, яка знижує енергоспоживання в періоди низького навантаження, що є додатковою перевагою для офісу, орієнтованого на ефективність і економію ресурсів.

Економічна доцільність вибору Cisco полягає не лише в початковій вартості, а й у довгостроковій перспективі: вища надійність і підтримка оновлень

зменшують ризик простоїв і витрати на заміну обладнання, що особливо важливо для бізнес-процесів, де мережа відіграє критичну роль.

Таким чином, Cisco Catalyst 2960-S вирізняється як оптимальне рішення, яке поєднує високу продуктивність, підтримку сучасних технологій, таких як VLAN, PoE і QoS, надійність і гнучкість управління, відповідаючи потребам офісної мережі, де стабільність, безпека і можливість розширення є ключовими пріоритетами.

Мережевий комутатор, обраний для проєкту, представлено на Рис.2.9.



Рис.2.9 - Світч Cisco Catalyst 2960 S

Аналіз вибору компонентів сервера

Аналіз корпусу. Обраний корпус Supermicro 6016T-URF [11] у форм-факторі 1U з можливістю розміщення чотирьох накопичувачів розміром 3,5 дюйма є спеціалізованим рішенням для компактних серверних систем, призначених для встановлення в стандартні 19-дюймові стійки центрів обробки даних.

Висота 1U (44,45 мм) забезпечує максимальну щільність розміщення серверів у стійці, що дозволяє економити фізичний простір, зменшувати витрати на оренду площі та оптимізувати інфраструктуру дата-центру. Корпус підтримує гарячу заміну дисків (hot-swap), що дає змогу замінювати накопичувачі без вимкнення системи, підвищуючи її доступність і зменшуючи час простою.

Сумісність із материнською платою MBD-X10DRD-iNT забезпечується завдяки стандартним розмірам (ширина 437 мм, глибина до 650 мм) та відповідним конекторам для підключення живлення й даних.

У порівнянні з корпусами 2U, такими як Supermicro 825TQ-R720LPB, які дозволяють розмістити до восьми 3,5-дюймових дисків і мають більше простору для додаткових плат розширення чи покращеного охолодження, 1U модель поступається за гнучкістю, але виграє за компактністю. Для задач, де не потрібна

велика кількість накопичувачів чи слотів PCIe, а пріоритетом є економія місця, 6016T-URF є ідеальним вибором.

Корпус оснащений двома резервованими блоками живлення (зазвичай 650 Вт або 700 Вт у платиновому стандарті енергоефективності), що забезпечує безперебійну роботу навіть у разі відмови одного блоку, а також знижує ризик перебоїв у живленні, що критично для серверів із цілодобовим режимом роботи.

Система охолодження в 1U корпусі базується на кількох високошвидкісних вентиляторах (зазвичай 40 мм), які створюють потужний повітряний потік для відведення тепла від двох процесорів, оперативної пам'яті та накопичувачів. Хоча це може підвищувати рівень шуму порівняно з 2U чи 4U корпусами, для дата-центрів із централізованою системою кондиціонування це не є проблемою.

Вибір саме 6016T-URF може бути зумовлений його доступністю на ринку, підтримкою Supermicro як надійного бренду та оптимальним співвідношенням ціни й функціональності для базової серверної конфігурації.

Зовнішній вигляд корпусу сервера, використаного у проєкті, зображено на Рис.2.10.



Рис.2.10 – Корпус сервера 6016T-URF Supermicro 1U 4x3,5

Аналіз оперативної пам'яті. Оперативна пам'ять у цій конфігурації представлена шістьма модулями DDR4R-2133 LRDIMM M386A4G40DM0-CPB від Samsung, кожен із яких має ємність 32 ГБ, що в сумі дає 192 ГБ [12]. Тип LRDIMM (Load-Reduced DIMM) обрано через його здатність підтримувати високу щільність пам'яті при використанні меншої кількості слотів, що є ключовою перевагою для серверів у компактному 1U форм-факторі, де фізичний простір обмежений.

Частота 2133 МГц обрана як стандартна для серверних систем на базі процесорів Intel Xeon E5-2600 v4, що забезпечує стабільну роботу без необхідності зниження продуктивності через обмеження контролера пам'яті чи несумісність із вищими частотами.

Порівняно з RDIMM (Registered DIMM), LRDIMM має нижче енергоспоживання при великих об'ємах пам'яті завдяки буферу, який зменшує навантаження на контролер процесора, а також дозволяє уникати затримок при високій завантаженості шини пам'яті.

Модулі Samsung M386A4G40DM0-CPB належать до серверного класу, підтримують ECC (Error-Correcting Code), що забезпечує виявлення й виправлення однобітових помилок і виявлення двобітових, що є стандартом для серверів, де надійність і точність даних є пріоритетними.

Об'єм 192 ГБ дозволяє ефективно виконувати багатозадачні операції, обробляти великі набори даних у реальному часі, підтримувати численні віртуальні машини чи працювати з базами даних, що потребують значних ресурсів пам'яті. У порівнянні з модулями на 2400 МГц, вибір 2133 МГц може бути обґрунтований нижчою вартістю, меншим тепловиділенням і ширшою доступністю на момент закупівлі.

Використання шести модулів замість восьми також сприяє рівномірному розподілу навантаження між двома процесорами, що покращує продуктивність у двопроцесорній конфігурації.

Вигляд модулів оперативної пам'яті, які застосовуються у сервері, показано на Рис.2.11.



Рис.2.11 – Оперативна пам'ять сервера 32 DDR4R-2133 LRDIMM
M386A4G40DM0-CPB Samsung x6

Аналіз накопичувачів. Для зберігання даних я обрав два твердотільних накопичувачі Intel DC S3520 Series SSDSC2BB240G7 об'ємом 240 ГБ кожен із форм-фактором 2,5 дюйма та інтерфейсом SATA 6 Гбіт/с [13].

Вибір двох накопичувачів замість одного більшого (наприклад, 480 ГБ) продиктований необхідністю забезпечення надлишковості через налаштування RAID 1 (дзеркалювання), де дані дублюються на обох дисках, що дозволяє системі продовжувати роботу без втрати інформації в разі відмови одного SSD. Це рішення підвищує надійність сервера, що є критично важливим для задач, де недопустимі перерви в роботі чи втрата даних, наприклад, для зберігання баз даних, логів чи конфігураційних файлів.

Альтернативно, накопичувачі можуть бути використані окремо: один для операційної системи (наприклад, Linux чи Windows Server), а другий для прикладних даних чи кешу, що забезпечує загальну ємність 480 ГБ і розподіляє навантаження для підвищення швидкості доступу.

Серія Intel DC S3520 базується на технології 3D MLC NAND, яка поєднує високу витривалість (до 0,3 DWPD – записів на день протягом 5 років) і стабільну продуктивність, із швидкістю послідовного читання до 450 МБ/с і запису до 380 МБ/с. Ці показники достатні для більшості серверних навантажень, таких як веб-хостинг, обробка транзакцій чи аналітика, хоча й поступаються NVMe-накопичувачам, які можуть досягати 2000 МБ/с читання і 1500 МБ/с запису.

Вибір SATA замість NVMe зумовлений сумісністю з материнською платою без потреби в додаткових контролерах чи адаптерах, а також нижчою вартістю й енергоефективністю (споживання близько 3,5 Вт у режимі запису).

Форм-фактор 2,5 дюйма ідеально інтегрується в корпус 6016T-URF через адаптери для 3,5-дюймових відсіків, що забезпечує гнучкість монтажу й економію простору.

У порівнянні з HDD (наприклад, 1 ТБ 7200 об/хв), SSD мають значно вищу швидкість доступу (IOPS до 68 000 для читання), нульовий час пошуку й відсутність рухомих частин, що підвищує їхню надійність і знижує ризик механічних поломок.

Вибір саме Intel DC S3520 також пояснюється їхньою репутацією в сегменті дата-центрів, підтримкою апаратного шифрування AES-256 і захистом від втрати даних при перебоях живлення, що додає ще один рівень безпеки для серверних застосувань.

Твердотільний накопичувач (SSD), що використовується у складі серверної системи, представлено на Рис.2.12.

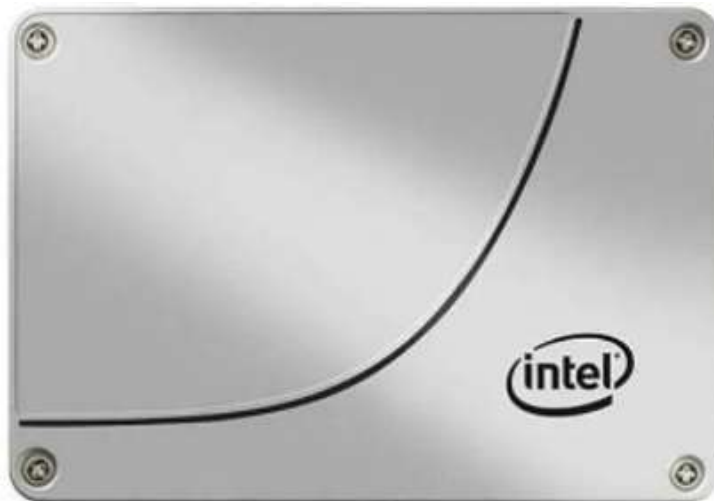


Рис.2.12 – SSD накопичувач 240 SATA 2,5 SSD Intel DC S3520 Series
SSDSC2BB240G7

Аналіз материнської плати та процесорів. Материнська плата Supermicro MBD-X10DRD-iNT [14] із двома сокетом LGA 2011-3 підтримує процесори Intel Xeon серії E5-2600 v3/v4 [15], має вісім слотів DIMM для пам'яті DDR4 із частотами від 1600 до 2400 МГц, вбудовані контролери SATA 6 Гбіт/с (10 портів), а також два порти 10GbE (маркування iNT), що забезпечує високошвидкісне мережеве підключення без додаткових карт розширення. Ця плата є основою для двопроесорної конфігурації, забезпечуючи оптимальну сумісність із обраними компонентами.

Два процесори Intel Xeon E5-2697A v4, кожен із 16 ядрами та 32 потоками, дають загалом 32 ядра і 64 потоки, що робить систему надзвичайно потужною для паралельних обчислень. Базова частота 2,6 ГГц із турбо-режимом до 3,6 ГГц, кеш третього рівня 40 МБ на процесор і підтримка технологій Hyper-Threading, VT-x і VT-d роблять їх ідеальними для задач віртуалізації, обробки великих даних чи наукових симуляцій.

У порівнянні з E5-2697 v4 (18 ядер, 2,3 ГГц, 45 МБ кешу), E5-2697A v4 має вищу базову частоту, що підвищує продуктивність у задачах із високим навантаженням на одне ядро, таких як веб-сервери чи потокова обробка. Порівняно з E5-2699 v4 (22 ядра, 2,2 ГГц, 55 МБ кешу), обраний процесор є економічнішим за вартістю й тепловиділенням (TDP 145 Вт), уникаючи надлишкової потужності для задач, які не потребують максимальної кількості ядер.

Плата підтримує до 1 ТБ пам'яті при використанні 3DS LRDIMM, що забезпечує запас для майбутнього масштабування, а вбудовані мережеві адаптери 10GbE дозволяють підключатися до сучасних інфраструктур із високою пропускнуою здатністю, що важливо для передачі великих обсягів даних у реальному часі. Обмеження 1U корпусу виключають використання повнорозмірних плат розширення, але вбудовані функції MBD-X10DRD-iNT компенсують це, роблячи її оптимальною для компактного сервера.

На Рис.2.13 Рис.2.14 відповідно зображено процесор, що використовується у сервері, та материнську плату, сумісну з обраною апаратною конфігурацією.



Рис.2.13 – Материнська плата сервера MBD-X10DRD-iNT Supermicro Dual socket 8 DIMM slots 2400/2133/1866/1600MHz ECC DDR4 SDRAM



Рис.2.14 – Процесор сервера E5-2697A v4 Хеон

Порівняльні таблиці.

Таблиця 2.5

Порівняння процесорів

Процесор	Ядра	Потоки	Базова частота	Турбо (макс.)	Кеш L3	Споживання (TDP)	Ціна (USD)
E5-2697A v4	16	32	2,6 ГГц	3,6 ГГц	40 МБ	145 Вт	1500
E5-2697 v4	18	36	2,3 ГГц	3,6 ГГц	45 МБ	145 Вт	1600
E5-2699 v4	22	44	2,2 ГГц	3,6 ГГц	55 МБ	145 Вт	2000

Таблиця 2.6

Порівняння пам'яті

Тип пам'яті	Ємність	Частота	Ранг	Споживання	Ціна за модуль (USD)
LRDIMM (Samsung)	32 ГБ	2133 МГц	4Rx4	15 Вт	300
RDIMM	32 ГБ	2133 МГц	2Rx4	12 Вт	250

Таблиця 2.7

Порівняння накопичувачів

Накопичувач	Ємність	Інтерфейс	Швидкість читання	Швидкість запису	Ціна (USD)
Intel DC S3520 SSD	240 ГБ	SATA 6 Гбіт/с	450 МБ/с	380 МБ/с	100
Intel DC S3520 480 ГБ	480 ГБ	SATA 6 Гбіт/с	450 МБ/с	380 МБ/с	200

NVMe SSD (аналог)	240 ГБ	NVMe	2000 МБ/с	1500 МБ/с	150
----------------------	--------	------	-----------	-----------	-----

Аналіз вибору компонентів ПК.

Аналіз процесора. Обраний процесор Intel Core i3-6100 [16] належить до шостого покоління процесорів Skylake, випущеного у 2015 році, і базується на архітектурі 14 нм. Він оснащений двома ядрами та чотирма потоками завдяки технології Hyper-Threading, має базову частоту 3,7 ГГц без підтримки турбо-режиму, кеш третього рівня об'ємом 3 МБ і тепловий пакет (TDP) 51 Вт.

Цей процесор призначений для сокету LGA 1151 і сумісний із материнською платою Asus B150M-C, що використовує чипсет Intel B150. Вибір Core i3-6100 обґрунтований його достатньою продуктивністю для базових задач, таких як офісна робота (робота з документами, таблицями, браузером), перегляд мультимедіа, легке програмування чи навчання, при цьому він має низьке енергоспоживання, що зменшує вимоги до блоку живлення та охолодження.

У порівнянні з чотириядерними моделями, такими як Core i5-6400 (4 ядра, 4 потоки, базова частота 2,7 ГГц, турбо до 3,3 ГГц, TDP 65 Вт), i3-6100 поступається в багатопотоковій продуктивності, але виграє за ціною та енергоефективністю, що робить його оптимальним для бюджетних систем без потреби в інтенсивних обчисленнях.

Порівняно з молодшою моделлю, наприклад Pentium G4400 (2 ядра, 2 потоки, 3,3 ГГц, 3 МБ кешу), Core i3-6100 пропонує перевагу Hyper-Threading, що дозволяє ефективніше обробляти кілька задач одночасно, наприклад, запуск браузера з кількома вкладками паралельно з текстовим редактором чи IDE для програмування.

Відсутність розгону (немає індексу "К") відповідає чипсету B150, який не підтримує оверклокінг, що додатково знижує тепловиділення та спрощує систему охолодження.

Core i3-6100 також підтримує набір інструкцій SSE4.1/4.2, AVX і AVX2, що забезпечує сумісність із сучасним програмним забезпеченням, включно з легкими графічними редакторами чи емуляторами.

Вибір саме цієї моделі був зумовлений її доступністю на вторинному ринку, низькою вартістю на момент складання конфігурації та достатньою продуктивністю для задач, які не потребують високої обчислювальної потужності, таких як робота з базами даних невеликого обсягу чи веб-розробка.

На Рис.2.15 зображено процесор Core i3-6100, який використовується в офісному персональному комп'ютері для забезпечення базової продуктивності при виконанні повсякденних завдань.



Рис.2.15 – Процесор офісного ПК Core i3 6100

Аналіз оперативної пам'яті. Оперативна пам'ять представлена одним модулем Kingston KVR26N19S6/8 об'ємом 8 ГБ типу DDR4 із частотою 2666 МГц [17]. Модуль належить до серії ValueRAM, яка розроблена для базових систем і не має радіаторів чи функцій розгону, що відповідає потребам бюджетного ПК.

Частота 2666 МГц є стандартною для DDR4 і сумісна з материнською платою Asus B150M-C, хоча чипсет B150 офіційно підтримує пам'ять до 2133 МГц, тому реальна частота може бути обмежена до цього значення без ручного налаштування BIOS.

Об'єм 8 ГБ є мінімально достатнім для комфортної роботи в сучасних операційних системах, таких як Windows 10 чи Linux-дистрибутиви (Ubuntu, Fedora), дозволяючи запускати браузер із кількома вкладками, офісні програми та легкі IDE, наприклад Visual Studio Code чи PyCharm у базовому режимі.

У порівнянні з конфігурацією з двома модулями по 4 ГБ у двоканальному режимі, один модуль 8 ГБ поступається за пропускну здатністю (одноканальний режим замість двоканального), але виграє за простотою встановлення та можливістю майбутнього розширення, оскільки материнська плата має два слоти DIMM, і додавання другого модуля 8 ГБ дозволить досягти 16 ГБ у двоканалі.

Відсутність ECC (Error-Correcting Code) типова для споживчої пам'яті й не є недоліком для ПК, де критична надійність даних не є пріоритетом, на відміну від серверів. Модуль Kingston KVR26N19S6/8 має затримки CL19, що є середнім показником для бюджетної пам'яті, і напругу 1,2 В, що забезпечує енергоефективність і сумісність із процесором Skylake.

Вибір одного модуля замість двох може бути зумовлений обмеженням бюджетом або наміром поступового апгрейду, а вибір Kingston як бренду пояснюється його репутацією надійного виробника з низьким відсотком браку.

У порівнянні з DDR3 (наприклад, 1600 МГц), DDR4 на 2666 МГц забезпечує вищу пропускну здатність (до 21,3 ГБ/с теоретично), що покращує загальну швидкодію системи, особливо при роботі з інтегрованою графікою, яка використовує системну пам'ять.

Оперативну пам'ять Kingston KVR26N19S6/8, що застосовується в офісному ПК для забезпечення стабільної роботи користувацьких застосунків, представлено на Рис.2.16.

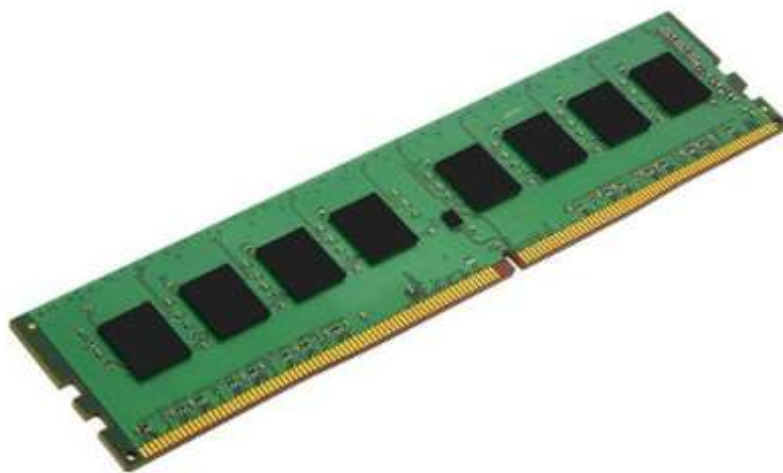


Рис.2.16 - Оперативна пам'ять офісного ПК Kingston KVR26N19S6/8

Аналіз материнської плати. Материнська плата Asus B150M-C виконана у форм-факторі Micro-ATX (mATX) із розмірами 24,4 x 21,8 см і базується на чипсеті Intel B150 [18], призначеному для систем середнього рівня на базі процесорів Skylake (6-е покоління).

Плата має два слоти DIMM із підтримкою до 32 ГБ DDR4 пам'яті (максимум 2133 МГц без розгону), один слот PCIe x16 для відеокарти (версія 3.0), два слоти PCIe x1 для додаткових карт розширення (наприклад, звукової чи мережевої), шість портів SATA 6 Гбіт/с для накопичувачів і один слот M.2 для SSD (з обмеженням до SATA M.2, без підтримки NVMe).

Вибір B150M-C обґрунтований її компактністю, що ідеально підходить для корпусу Mini-Tower, та достатньою функціональністю для базової конфігурації без надлишкових можливостей, таких як розгін чи підтримка SLI/CrossFire, які відсутні в чипсеті B150.

У порівнянні з чипсетом H170 (4 слоти DIMM, більше ліній PCIe), B150 є дешевшим і простішим, що відповідає бюджетному підходу до складання ПК.

Плата оснащена вбудованим звуковим кодеком Realtek ALC887 (7.1-канальний звук), мережевим контролером Realtek RTL8111H (Gigabit Ethernet) і базовими відеовиходами (VGA, DVI-D, HDMI), що забезпечують підключення монітора до інтегрованої графіки Intel UHD Graphics 530 без потреби в дискретній відеокарті.

Наявність портів USB 3.0 (4 штуки) і USB 2.0 (2 штуки) на задній панелі та підтримка додаткових портів через фронтальні роз'єми корпусу роблять плату зручною для підключення периферії, наприклад миші, клавіатури, флеш-накопичувачів чи зовнішніх дисків.

Відсутність розгінних функцій і обмеження частоти пам'яті до 2133 МГц не є недоліком для даної конфігурації, оскільки процесор i3-6100 не підтримує розгін, а пам'ять на 2666 МГц може працювати на нижчій частоті без суттєвих втрат продуктивності.

Вибір Asus як бренду пояснюється якістю складання, стабільністю роботи BIOS (UEFI із графічним інтерфейсом) і тривалим терміном служби, що робить

B150M-C оптимальною основою для довгострокового використання в бюджетному ПК.

На Рис.2.17 зображено материнську плату Asus B150M-C, яка використовується в офісному ПК та забезпечує підтримку базових апаратних компонентів для виконання щоденних завдань.



Рис.2.17 – Материнська плата офісного ПК Asus B150M-C

Аналіз відеокарти. Відеокарта в цій конфігурації є інтегрованою – Intel UHD Graphics 530, вбудованою в процесор Core i3-6100. Цей графічний чип базується на архітектурі Skylake GT2, має 24 виконавчих блоки (EU), базову частоту 350 МГц із динамічним розгоном до 1000 МГц і використовує системну пам'ять DDR4 як відеопам'ять (до 1,7 ГБ із загальних 8 ГБ). UHD Graphics 530 підтримує DirectX 12, OpenGL 4.4 і апаратне декодування відео H.265/HEVC, що дозволяє переглядати 4K-контент, працювати з базовими графічними редакторами (Photoshop у легкому режимі) чи запускати старі або невимогливі ігри (наприклад, CS:GO на низьких налаштуваннях із 30-40 FPS).

Вибір інтегрованої графіки замість дискретної відеокарти, наприклад NVIDIA GTX 1050 (2 ГБ GDDR5, 75 Вт), пояснюється економією бюджету, зниженням енергоспоживання та відсутністю потреби в додатковому охолодженні чи потужнішому блоці живлення. У порівнянні з UHD Graphics 630 (Coffee Lake, 7-е покоління), UHD 530 має дещо нижчу продуктивність, але для задач без значного

графічного навантаження (офісна робота, перегляд відео, веб-серфінг) різниця несуттєва.

Відеовиходи на материнській платі (HDMI, DVI-D, VGA) дозволяють підключати один монітор із роздільною здатністю до 4096x2304 при 24 Гц (HDMI) або 1920x1200 при 60 Гц (DVI-D), що достатньо для стандартних дисплеїв. Відсутність дискретної відеокарти обмежує можливості для сучасних ігор чи роботи з 3D-графікою, але для цілей ПК, орієнтованого на продуктивність у базових задачах, інтегроване рішення є виправданим. Продуктивність графіки залежить від швидкості пам'яті, тому один модуль DDR4 на 2666 МГц дещо знижує її потенціал порівняно з двоканальним режимом, але це не критично для неігрових сценаріїв.

Аналіз корпусу. Корпус CaseCom GN-1718-500 у форм-факторі Mini-Tower із вбудованим блоком живлення на 500 Вт є компактним рішенням для бюджетних систем [19]. Розміри корпусу (приблизно 352 x 175 x 410 мм) дозволяють розмістити материнську плату Micro-ATX, один 3,5-дюймовий відсік для HDD, один 2,5-дюймовий для SSD і обмежений простір для додаткових вентиляторів (зазвичай один 80 мм або 120 мм спереду чи ззаду).

Вбудований блок живлення на 500 Вт забезпечує достатню потужність для конфігурації з TDP процесора 51 Вт, інтегрованою графікою та одним SSD (споживання до 5 Вт), залишаючи запас для периферії (близько 100-150 Вт загального навантаження). У порівнянні з корпусами Mid-Tower, такими як Zalman Z3 Plus, Mini-Tower поступається за кількістю відсіків і можливостями охолодження, але виграє за компактністю та нижчою вартістю.

Блок живлення, імовірно, не сертифікований за стандартом 80 Plus, що вказує на базову ефективність (70-80%), але для системи без дискретної відеокарти чи великої кількості накопичувачів це не є проблемою. Наявність фронтальних портів USB (2.0 або 3.0 залежно від моделі) і аудіороз'ємів (3,5 мм) забезпечує зручність підключення зовнішніх пристроїв.

Корпус підходить для домашнього чи офісного використання, де важливі невеликі розміри та простота складання. Вибір CaseCom GN-1718-500 зумовлений

його низькою ціною, наявністю блоку живлення в комплекті та достатньою міцністю конструкції для захисту компонентів від пилу й механічних пошкоджень. Корпус офісного ПК CaseCom GN-1718-500 у форм-факторі Mini-Tower із блоком живлення на 500 Вт представлено на Рис.2.18.



Рис.2.18 – Корпус офісного ПК CaseCom GN-1718-500 Mini-Tower 500 Вт

Аналіз накопичувача. Твердотільний накопичувач Kingston A400 об'ємом 240 ГБ із форм-фактором 2,5 дюйма та інтерфейсом SATA 6 Гбіт/с є базовим рішенням для зберігання даних [20]. Він базується на контролері (імовірно Phison S11) і флеш-пам'яті TLC NAND, забезпечуючи швидкість послідовного читання до 500 МБ/с і запису до 350 МБ/с (залежно від обсягу кешу DRAM, якого в A400 немає, що знижує продуктивність при інтенсивному записі).

Об'єм 240 ГБ достатній для встановлення операційної системи (Windows 10 займає 20-30 ГБ), базового набору програм (офісні пакети, браузер, IDE) і зберігання невеликої кількості файлів (документи, фото, легкі проекти). У порівнянні з HDD (наприклад, WD Blue 1 ТБ, 7200 об/хв, 150 МБ/с), SSD A400 значно швидший (час доступу 0,1 мс проти 10 мс у HDD), безшумний і стійкий до вібрацій, що підвищує надійність системи.

Порівняно з преміальними SSD, такими як Samsung 860 EVO (500 МБ/с запис, DRAM-кеш), Kingston A400 поступається за витривалістю (TBW 80 ТБ проти 150 ТБ) і стабільністю при тривалому навантаженні, але виграє за ціною. Вибір SATA замість NVMe пояснюється сумісністю з материнською платою (M.2 слот підтримує лише SATA) і нижчою вартістю.

SSD A400 ідеально підходить для прискорення завантаження ОС (5-10 секунд проти 30-40 секунд на HDD) і роботи програм, що робить його оптимальним для бюджетного ПК.

На Рис.2.19 зображено SSD-накопичувач Kingston A400 об'ємом 240 ГБ, який використовується в офісному ПК для швидкого завантаження операційної системи та програм.



Рис.2.19 – SSD накопичувач офісного ПК Kingston A400 240 ГБ

Порівняльні таблиці.

Таблиця 2.8

Порівняння процесорів

Процесор	Ядра/Потоки	Частота	Кеш L3	TGP	Ціна (USD)
Core i3-6100	2/4	3,7 ГГц	3 МБ	51 Вт	50-70
Core i5-6400	4/4	2,7-3,3 ГГц	6 МБ	65 Вт	80-100
Pentium G4400	2/2	3,3 ГГц	3 МБ	54 Вт	30-40

Таблиця 2.9

Порівняння пам'яті

Модуль	Об'єм	Частота	Затримка	Ціна (USD)
Kingston KVR26N19S6/8	8 ГБ	2666 МГц	CL19	25-30
2x4 ГБ DDR4	8 ГБ	2133 МГц	CL15	30-35

Таблиця 2.10

Порівняння накопичувачів

Накопичувач	Об'єм	Швидкість читання/запису	TBW	Ціна (USD)
Kingston A400	240 ГБ	500/350 МБ/с	80 ТБ	25-30

Samsung 860 EVO	250 ГБ	550/520 МБ/с	150 ТБ	40-50
WD Blue HDD	1 ТБ	150/140 МБ/с	-	40-45

2.3. Розподіл IP-адресації для компонентів мережі

Розподіл IP-адрес у локальній мережі є важливим етапом проектування інформаційної інфраструктури офісу, оскільки він визначає стабільність зв'язку між пристроями, ефективність передачі даних та зручність адміністрування. У двоповерховому офісі з п'ятьма відділами (адміністративно-фінансовий, операційний, IT, продажів і маркетингу) мережа складається з 10 персональних комп'ютерів (ПК), 1 сервера та 2 комутаторів, об'єднаних у топологію "зірка" з сегментацією трафіку за допомогою VLAN [21].

Для організації мережі обрано приватний діапазон IPv4 192.168.0.0/24 з маскою 255.255.255.0, що забезпечує 254 доступні адреси (від 192.168.0.1 до 192.168.0.254, за винятком 192.168.0.0 як ідентифікатора мережі та 192.168.0.255 як широкомовної адреси), достатні для поточних потреб і майбутнього розширення. Оскільки роутерів у конфігурації немає, функції маршрутизації між VLAN і зв'язку із зовнішньою мережею виконуватиме комутатор із підтримкою рівня 3.

IP-адреси поділено на статичні для ключового обладнання та динамічні для робочих станцій: серверу, розташованому в зоні IT-відділу на першому поверсі, призначено статичну адресу 192.168.6.1 для виконання функцій DHCP, DNS і Active Directory; комутатор першого поверху отримав 192.168.0.251, комутатор другого поверху — 192.168.0.252, а шлюз за замовчуванням (зовнішній пристрій від провайдера) — 192.168.0.254.

Для робочих станцій адреси розподілено за VLAN: VLAN 2 (adm)-192.168.2.1-192.168.2.4 (2 ПК на першому поверсі, 2 на другому), VLAN 3 (op) -192.168.3.1-192.168.3.2 (2 ПК на першому поверсі), VLAN 4 (it)-192.168.4.1-192.168.4.2 (2 ПК на першому поверсі), VLAN 5 (prodaga)-192.168.5.1-192.168.5.2 (2 ПК на другому поверсі).

Сервер на адресі 192.168.6.1 налаштовано як DHCP-сервер для автоматизації призначення IP-адрес робочим станціям, що зменшує ручну працю адміністраторів

і спрощує підключення нових пристроїв. Сегментація за VLAN із чітким розподілом адрес підвищує безпеку, ізолюючи трафік між відділами (наприклад, ПК у VLAN 2 на 192.168.2.1 не має прямого доступу до ПК у VLAN 3 на 192.168.3.1 без правил маршрутизації), а топологія "зірка" з комутаторами на кожному поверсі полегшує управління та розширення мережі.

Ця схема відповідає потребам офісу, забезпечуючи стабільність завдяки статичним адресам для сервера та комутаторів, ефективність через автоматизацію DHCP і можливість масштабування за рахунок резервного діапазону, що робить її надійною основою для інформаційної інфраструктури.

2.4. Планування розташування обладнання інфраструктури офісу

Офіс складається з двох поверхів, на яких розміщені п'ять відділів: адміністративно-фінансовий (перший і другий поверхи), операційний (перший поверх), IT-відділ (перший поверх) та відділ продажів і маркетингу (другий поверх). Мережа побудована за топологією "зірка", де кожен поверх має свій комутатор, до якого підключені робочі станції відповідних відділів, а сервер із IP 192.168.6.1 розташований на першому поверсі в зоні IT-відділу для зручного доступу адміністраторів, дивитись (див. Додаток Г).

Серверна шафа компактного типу розміщується в зоні IT-відділу поблизу робочих місць системного адміністратора та спеціаліста технічної підтримки (VLAN 4), що забезпечує швидкий фізичний доступ до сервера та комутатора першого поверху для обслуговування, діагностики чи заміни обладнання, а також підвищує безпеку завдяки обмеженому доступу сторонніх осіб і полегшує організацію охолодження та вентиляції. Шафа вміщує сервер і комутатор, оснащена замикаючими дверима, перфорованими панелями для циркуляції повітря.



Рис.2.20 – Розташування серверної шафи в офісі

Кабельна інфраструктура базується на структурованій системі з використанням кабелів "вита пара" які забезпечують швидкість до 1 Гбіт/с на відстані до 100 метрів: на першому поверсі від шафи до робочих місць адміністративно-фінансового відділу (VLAN 2, IP 192.168.2.1–192.168.2.2, 2 ПК) прокладаються два кабелі довжиною 5–10 метрів, до операційного відділу (VLAN 3, IP 192.168.3.1–192.168.3.2, 2 ПК) — два кабелі такої ж довжини, до ІТ-відділу (VLAN 4, IP 192.168.4.1–192.168.4.2, 2 ПК) — два кабелі, підключені до комутатора в шафі, а сервер із комутатором з'єднаний патч-кордом (1–2 метри); на другому поверсі від комутатора (IP 192.168.0.252) до адміністративно-фінансового відділу (VLAN 2, IP 192.168.2.3–192.168.2.4, 2 ПК) і відділу продажів і маркетингу (VLAN 5, IP 192.168.5.1–192.168.5.2, 2 ПК) прокладаються по два кабелі довжиною 5–10 метрів.

Комутатор першого поверху з'єднується з комутатором другого поверху кабелем Cat6 через вертикальний кабельний канал або стельовий простір (10–15 метрів), а для підключення до зовнішнього шлюзу (IP 192.168.0.254) від комутатора першого поверху прокладається кабель до точки входу інтернет-з'єднання від провайдера біля входу в будівлю. Кабелі прокладаються в пластикових кабель-каналах уздовж стін або під фальшполом, маркуються на обох кінцях для зручності ідентифікації та обслуговування.



Рис.2.21 – Прокладання дроту між двома комутаторами

Комутатор першого поверху розташований у серверній шафі й обслуговує всі ПК першого поверху (VLAN 2, 3, 4) та зв'язок із другим поверхом, тоді як комутатор другого поверху розміщений у настінному боксі або на полиці в технічній зоні і обслуговує ПК другого поверху (VLAN 2, 5); обидва комутатори підтримують PoE, що дозволяє в майбутньому підключити точки доступу Wi-Fi без додаткових джерел живлення.



Рис.2.22 – Розташування комутатора на першому поверсі

Хоча мережа наразі використовує лише дротові з'єднання, передбачено можливість встановлення точок доступу Wi-Fi: на першому поверсі — у центрі або поблизу операційного відділу, на другому — у центрі або біля відділу продажів і маркетингу, із розміщенням на висоті 2–3 метри від підлоги, подалі від металевих конструкцій та джерел перешкод для стабільного сигналу.

Таким чином при плануванні було враховано розміщення серверної шафи в зоні IT-відділу, структуровану прокладку кабелів із маркуванням, розташування комутаторів на кожному поверсі та потенційні точки доступу Wi-Fi, забезпечуючи надійність, зручність експлуатації та можливість масштабування мережі.

2.5. Висновки до розділу 2

У ході дослідження досягнуто технічних характеристик, які відповідають сучасним вимогам до продуктивності, безпеки та адаптивності інформаційних систем. Зокрема, завдяки застосуванню топології "зірка" з двома комутаторами та поділу трафіку на VLAN (з 2 по 5) забезпечено чітке розділення даних між відділами, що підвищило безпеку й стабільність функціонування мережі.

Моделювання в Cisco Packet Tracer із 10 комп'ютерами, одним сервером і двома комутаторами підтвердило надійність зв'язків і легкість подальшого розширення системи. Зокрема, у рамках симуляції було відтворено передачу даних між ПК 1 (IP-адреса 192.168.2.1) і ПК 4 (IP-адреса 192.168.2.4), що належать до VLAN 2 і розташовані на різних поверхах офісу. Пакет даних успішно передавався від ПК 1 через комутатор Switch0 (IP 192.168.0.251) до Switch1 (IP 192.168.0.252) і далі до ПК 4 із загальною затримкою до 0,006 секунди, що свідчить про високу швидкість і стабільність з'єднання. Журнал подій симуляції показав послідовність обробки: відправлення пакета з ПК 1 (0,000 с), передача через Switch0 (0,001–0,003 с), маршрутизація через транковий порт до Switch1 (0,004–0,005 с) і доставка до ПК 4 (0,006 с). Ізоляція трафіку між VLAN підтверджена відсутністю доступу до пристроїв із інших VLAN без додаткових правил маршрутизації, а використання кабелів Cat6 забезпечило пропускну здатність до 1 Гбіт/с.

Обране обладнання стало запорукою високих технічних показників. Комутатори Cisco Catalyst 2960-S із пропускну здатністю до 176 Гбіт/с,

функціями PoE, QoS і тривалим часом безвідмовної роботи (MTBF понад 300 000 годин) гарантують стабільну передачу даних навіть у моменти максимального навантаження, а також дозволяють підключати Wi-Fi точки без додаткових джерел живлення.

Сервер, побудований на базі шасі Supermicro 6016T-URF із процесорами Intel Xeon E5-2697A v4 (32 ядра, 64 потоки, частота до 3,6 ГГц), 192 ГБ оперативної пам'яті DDR4 LRDIMM і твердотільними накопичувачами Intel DC S3520 (480 ГБ у конфігурації RAID 1), забезпечує значну обчислювальну потужність, надійне збереження інформації та швидкий доступ до неї.

Робочі станції на базі Intel Core i3-6100 з 8 ГБ RAM і SSD Kingston A400 (240 ГБ) відповідають вимогам офісних завдань, зберігаючи баланс між продуктивністю та вартістю. Система IP-адресації, побудована на діапазоні 192.168.0.0/24, із фіксованими адресами для сервера (192.168.6.1) і комутаторів (192.168.0.251–252), а також автоматичним розподілом адрес для робочих станцій через DHCP, створила умови для стабільної роботи мережі та її адаптивності. Залишений резерв адрес відкриває можливості для підключення додаткових пристроїв у майбутньому.

Розташування обладнання, зокрема серверної шафи в зоні IT-відділу, прокладка кабелів у структурованих каналах і підготовка до розміщення Wi-Fi точок із PoE, сприяли формуванню зручної, безпечної та функціональної інфраструктури з пропускною здатністю до 1 Гбіт/с і повним покриттям офісу.

Отже, розроблена апаратна структура забезпечує високу швидкість обробки даних (до 176 Гбіт/с, 41,7 Mpps), стійкість до збоїв (MTBF 200 000–300 000 годин, резервування RAID 1), захист інформації (VLAN) і потенціал для зростання (резерв адрес, можливість стекування комутаторів). Симуляція передачі даних у VLAN 2 додатково підтвердила ефективність топології «зірка», коректність сегментації трафіку та готовність мережі до експлуатації в реальних умовах. Ці параметри відповідають потребам сучасного офісного середовища, створюючи надійну основу для подальшого вдосконалення програмного забезпечення в наступних етапах роботи.

РОЗДІЛ 3

ПРОГРАМНІ КОМПОНЕНТИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ РОБОЧОГО СЕРЕДОВИЩА ОФІСУ

3.1. Запуск і налаштування серверів офісної мережі

Серверна інфраструктура є основним елементом управління інформаційними потоками в офісному середовищі. Вона дозволяє централізовано керувати користувачами, розподіляти IP-адреси, ідентифікувати пристрої в мережі та забезпечувати захищений доступ до ресурсів. Ключовими сервісами, що реалізуються на сервері, є Active Directory (AD), DHCP (Dynamic Host Configuration Protocol) та DNS (Domain Name System).

На першому етапі інсталяції виконується додавання ролей через менеджер серверів. Обираються необхідні служби, що забезпечують мережеву функціональність.

На Рис.3.23 показано процес вибору ролей під час встановлення серверних служб DHCP, DNS та Active Directory в середовищі Windows Server.

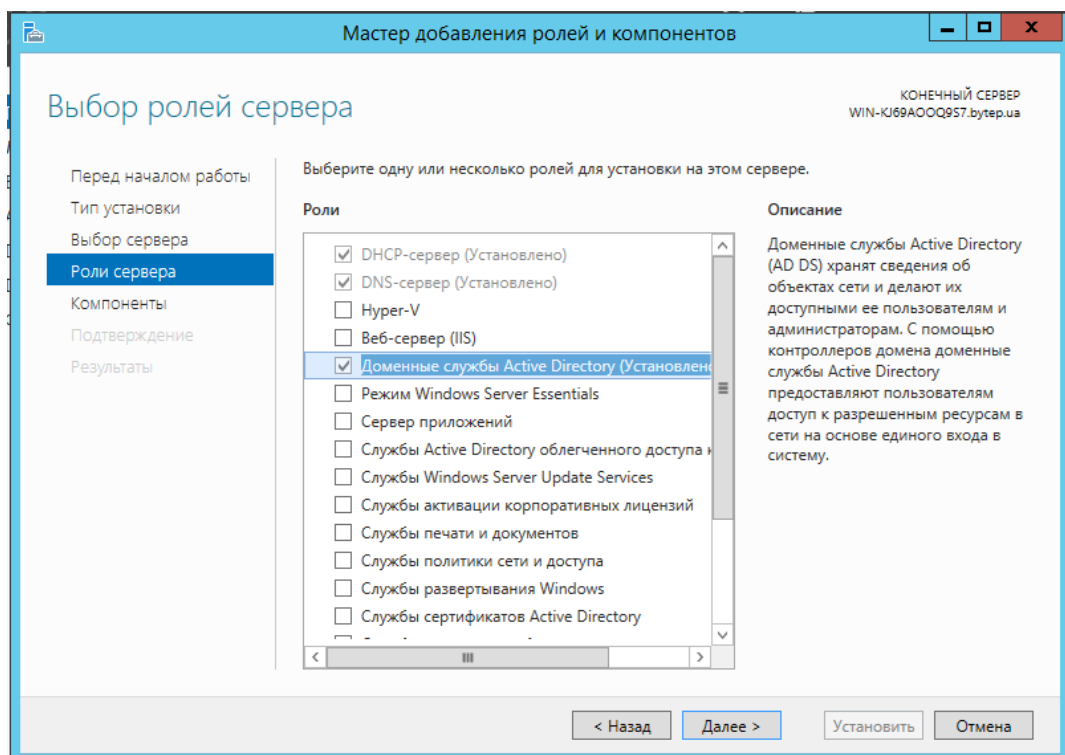


Рис.3.23 – Вибір ролей для встановлення DHCP, DNS та Active Directory

Після вибору ролей виконується налаштування домену — логічної структури, яка об'єднує всі об'єкти мережі під єдиним управлінням.

Процес створення нового домену в середовищі Windows Server продемонстровано на Рис.3.24 [22].

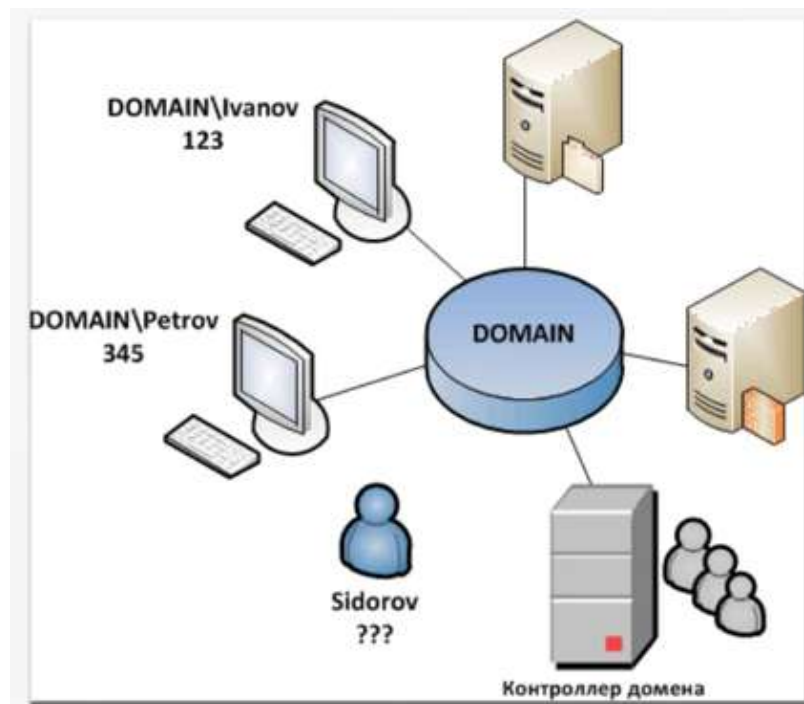


Рис.3.24 – Створення нового домену в середовищі Windows Server

Доменний контролер є сервером, що обслуговує функції Active Directory — базу даних, яка зберігає інформацію про облікові записи користувачів, комп'ютерів і політики безпеки. Процес його конфігурації включає вибір доменного імені та генерацію NetBIOS-імені — унікального скороченого ідентифікатора в межах мережі.

На Рис.3.25 зображено етап введення DNS-імені домену під час налаштування служби Active Directory.

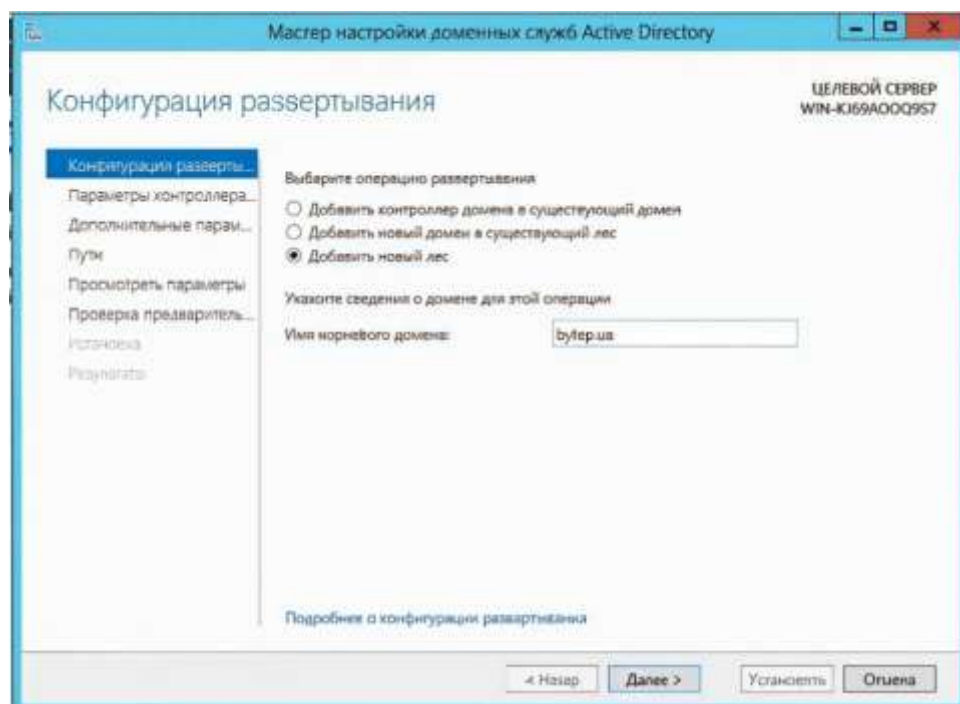


Рис.3.25 – Введення DNS-імені домену

Автоматичне створення NetBIOS-імені домену під час налаштування інфраструктури домену показано на Рис.3.26.

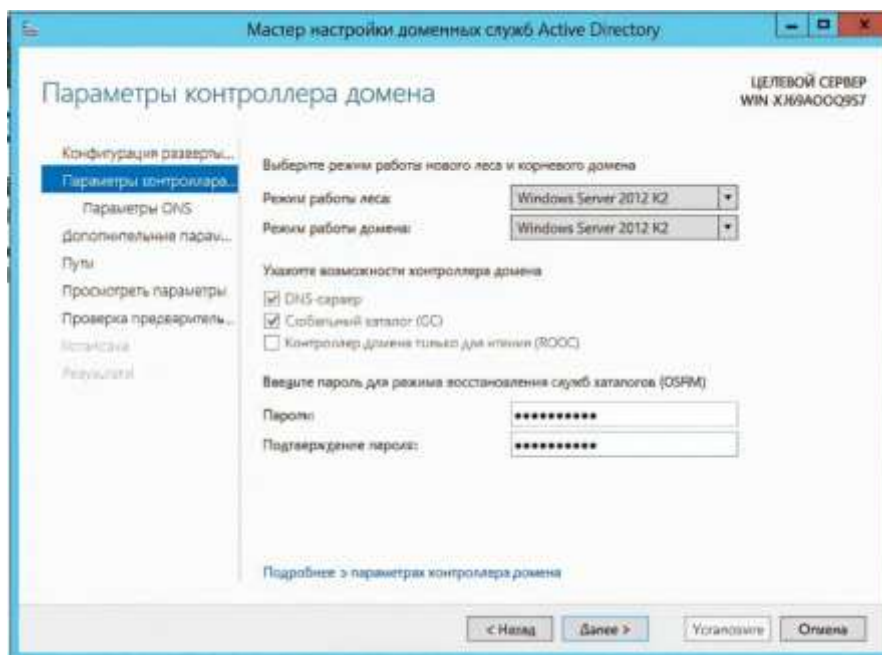


Рис.3.26 – Автоматичне створення NetBIOS-імені домену

Автогенерація NetBIOS імені. NetBIOS це унікальна 16 байтна адреса, яка використовується для ідентифікації ресурсів мережі. На Рис.3.27 продемонстровано завершальний етап налаштування контролера домену в середовищі Windows Server.

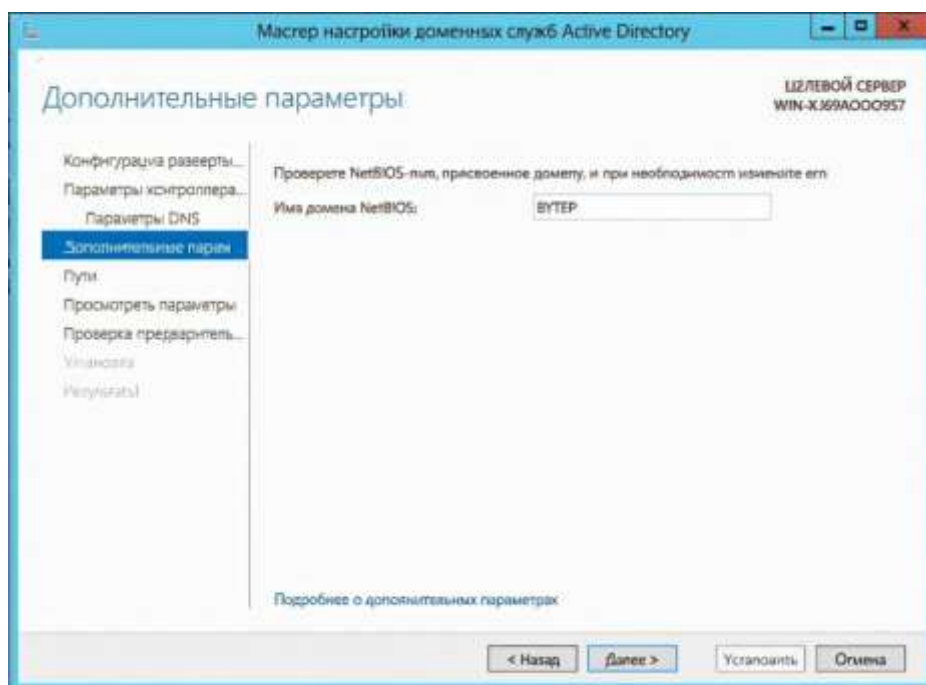


Рис.3.27 – Завершення налаштування контролера домену

Налаштування та встановлення пройшло успішно, що можна бачити на малюнку 3.28. Наш адміністраторський обліковий запис перейшов в AD і став частиною домену.

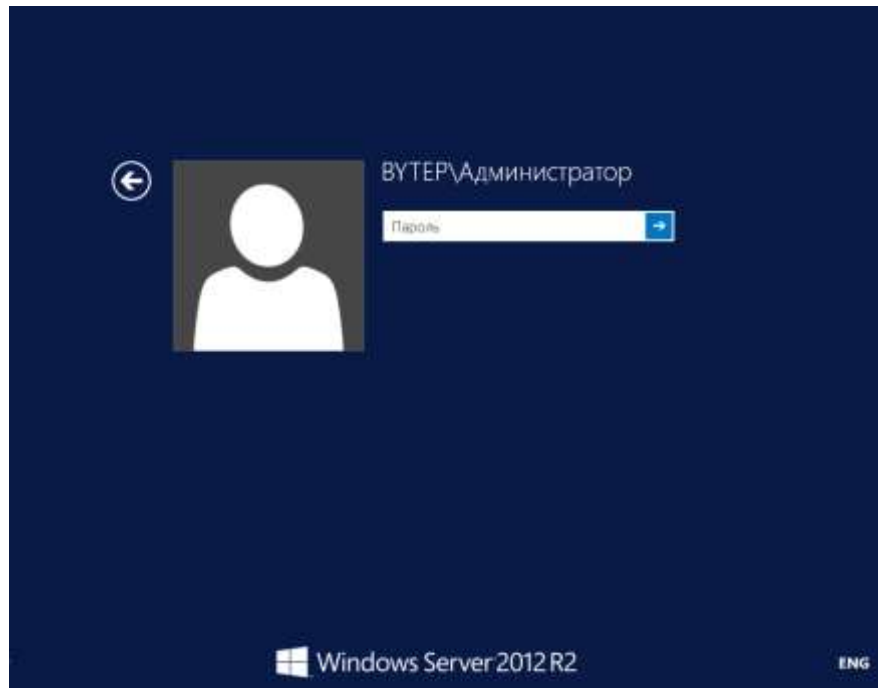


Рис.3.28 – Інформація про домен у системі (після входу адміністратора в домен)

Наступним кроком є налаштування DHCP-сервера, що дозволяє автоматизувати призначення IP-адрес користувачам та пристроям. Це зменшить ризик конфліктів адрес і спрощує адміністрування. Налаштування пулу IP-адрес для служби DHCP представлено на Рис.3.29.

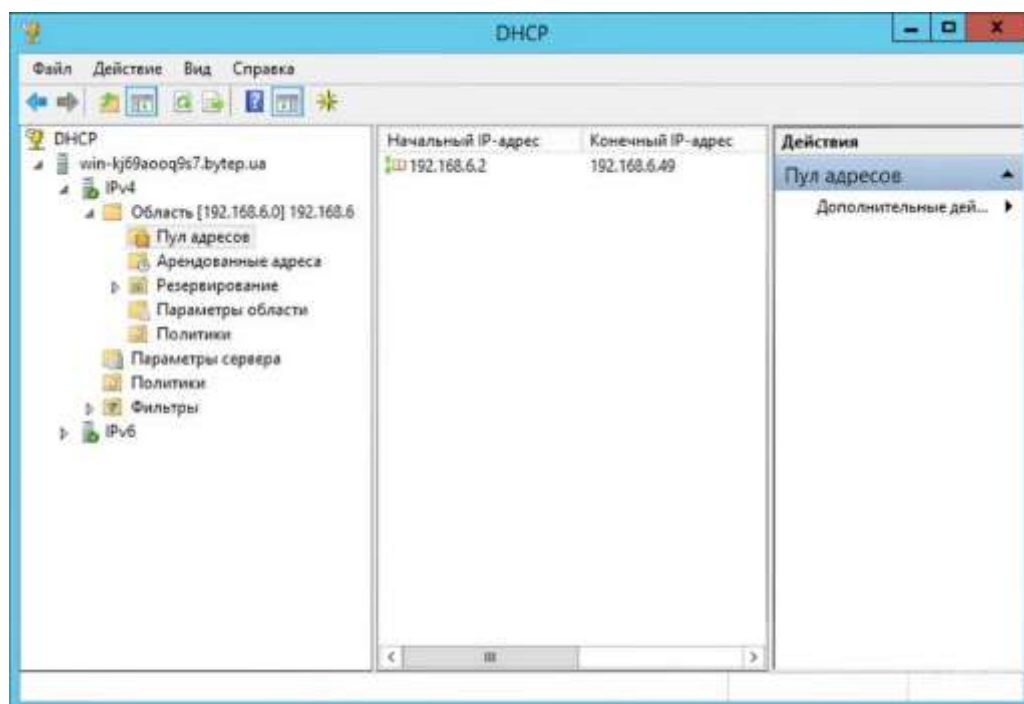


Рис.3.29 – Налаштування пулу адрес DHCP

DNS-сервер, своєю чергою, дозволяє перетворювати доменні імена в IP-адреси й навпаки. Це необхідно для зручної навігації в межах мережі, адже користувачам буде простіше працювати з іменами, ніж з цифровими адресами. На Рис.3.30 показано процес налаштування зон прямого та зворотного переглядів у службі DNS.

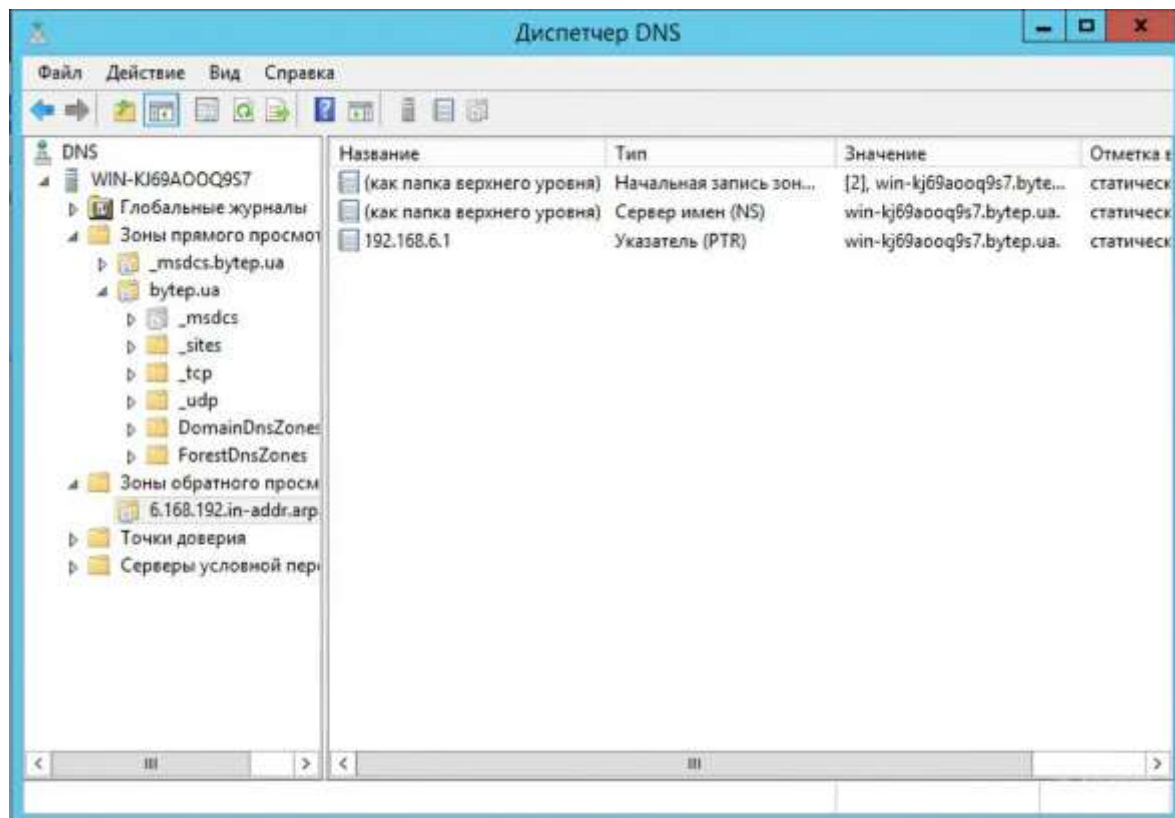


Рис.3.30 – Налаштування зон прямого та зворотного переглядів DNS

3.2. Особливості групових політик та управління користувачами

Централізоване управління користувачами — один із ключових елементів безпечної та ефективної офісної мережі. В основі цього підходу лежить використання групових політик (Group Policy) — потужного інструменту Microsoft, що дозволяє адміністраторам налаштовувати операційне середовище користувачів та комп'ютерів у доменній структурі.

Групові політики: сутність і можливості

Групові політики — це набір правил, які застосовуються до облікових записів користувачів і комп'ютерів у середовищі Active Directory. Вони дозволяють автоматизувати:

- налаштування робочого столу;

- заборону доступу до певних елементів системи;
- встановлення обмежень на використання USB-пристроїв;
- призначення принтерів або мережевих дисків;
- застосування політик безпеки.

Автоматизація за допомогою GPO. Впровадження групових політик дозволяє значно зменшити час на налаштування кожного окремого комп'ютера. Наприклад, після додавання ПК до домену, він автоматично отримує всі параметри, передбачені політиками: від проксі-сервера до конфігурації брандмауера. Політики застосовуються через GPO (Group Policy Objects), які прив'язуються до об'єктів Active Directory — доменів, організаційних одиниць (OU) або груп. Це дозволяє створити ієрархічну структуру керування: наприклад, для всіх бухгалтерів можна застосувати обмеження на доступ до інтернету, а для IT-відділу — надати розширені права адміністратора.

Приклад використання в офісній мережі. У реалізованій мережевій моделі для кожного підрозділу офісу (бухгалтерія, IT, маркетинг) мною були створені окремі організаційні одиниці (OU). На кожному з них призначено відповідну GPO:

- OU "Бухгалтерія" — обмеження доступу до зовнішніх USB-накопичувачів, обов'язкова зміна пароля кожні 30 днів;
- OU "Маркетинг" — автоматичне підключення до загального мережевого ресурсу для зберігання рекламних матеріалів;
- OU "IT-відділ" — дозволи на встановлення ПЗ та доступ до службових інструментів адміністрування.

Таким чином, я не лише зменшує навантаження на ручну конфігурацію, але й забезпечує дотримання політик безпеки та уніфікацію середовища.

3.3. Налаштування міжмережевого екрану та VPN

Міжмережевий екран (брандмауер) і віртуальна приватна мережа (VPN) є ключовими для захисту офісної мережі та забезпечення безпечного віддаленого доступу. У цьому підпункті описано процес налаштування брандмауера на сервері з Windows та впровадження VPN за допомогою WireGuard для зручного і

безпечного підключення працівників. Для захисту мережі використано вбудований Windows Defender Firewall на сервері (IP 192.168.6.1).

Основні налаштування:

1. Увімкнено Windows Defender Firewall для всіх мережевих профілів (доменний, приватний, публічний).
2. Заблоковано всі вхідні підключення за замовчуванням, крім необхідних служб: DHCP (порт 67/UDP), DNS (порт 53/TCP і UDP), Active Directory (порт 445/TCP) і віддалений робочий стіл (порт 3389/TCP).
3. Відкриття порту 51820 UDP для VPN

Налаштування виконано через графічний інтерфейс Windows Defender Firewall із розширеними параметрами безпеки, як показано на Рис.3.31.

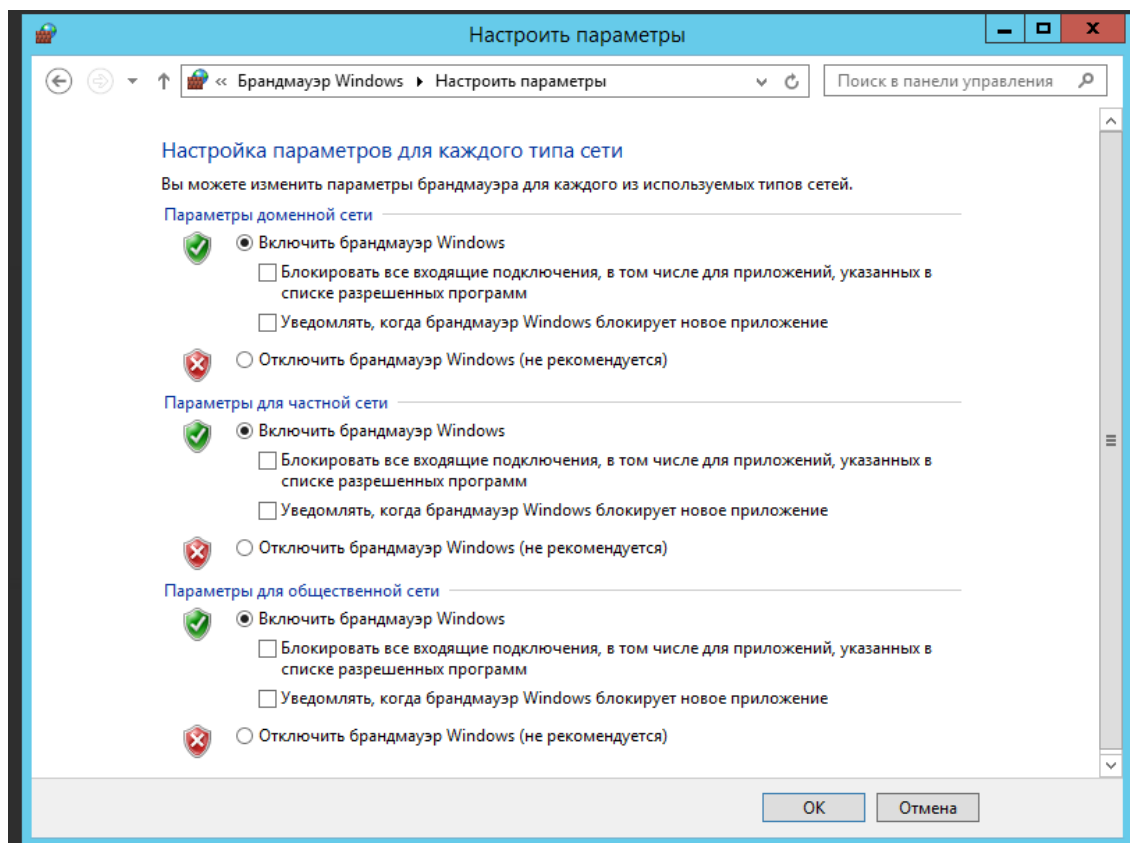


Рис.3.31 – Увімкнення Windows Defender Firewall для всіх мережевих профілів

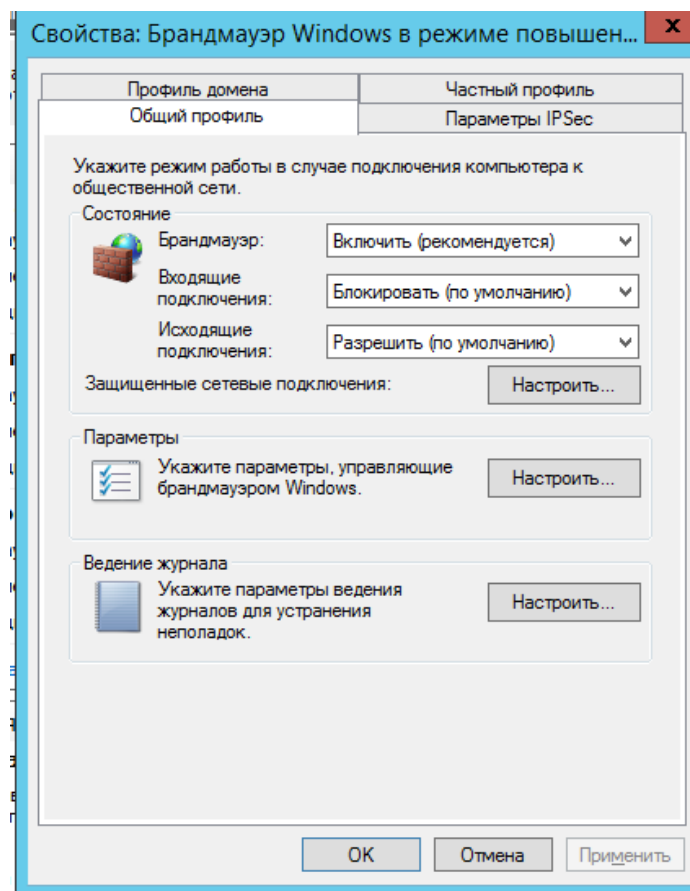


Рис.3.32 – Блокування всіх вхідних підключень

Правила для вхідних підключень						
Имя	Группа	Профиль	Включено	Локальный порт	Протокол	
✓ VPN UDP 51820		Все	Да	51820	UDP	
✓ RDP 3389		Все	Да	3389	TCP	
✓ AD 445		Все	Да	445	TCP	
✓ DHCP 67		Все	Да	67	UDP	
✓ TCP 53		Все	Да	53	TCP	
✓ UDP 53		Все	Да	53	UDP	

Рис.3.33 – Налаштування брандмауєра

Підключення клієнта до сервера за допомогою RDP. Для забезпечення віддаленого адміністрування та доступу до серверних ресурсів використовується протокол віддаленого робочого стола (Remote Desktop Protocol, RDP). Цей протокол дозволяє користувачам підключатися до графічного інтерфейсу сервера, виконувати адміністративні задачі, керувати файлами, службами та мережевими налаштуваннями. Щоб підключитися до сервера за допомогою RDP, на клієнтському комп'ютері з операційною системою Windows відкривається програма "Підключення до віддаленого робочого стола" (mstsc). У вікні підключення вказується IP-адреса сервера (у нашому випадку — 192.168.6.1), після чого вводяться облікові дані користувача, який має дозвіл на віддалений доступ.

Попередньо на сервері повинно бути:

- увімкнено службу "Remote Desktop Services".
- налаштовано виключення порту 3389/TCP у брандмауері.
- додано дозволи для користувачів у групу "Remote Desktop Users".

На Рис.3.34 показано приклад підключення клієнтського ПК до сервера через RDP.

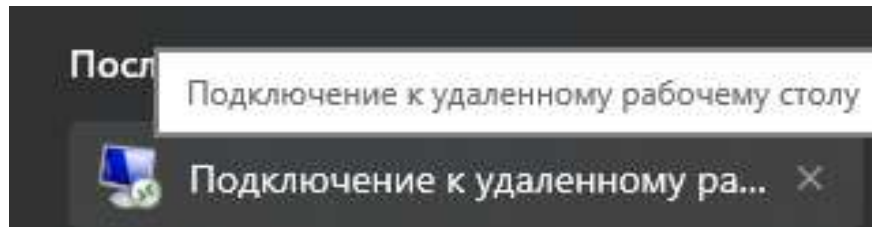


Рис.3.34 – Вікно програми "Підключення до віддаленого робочого столу"

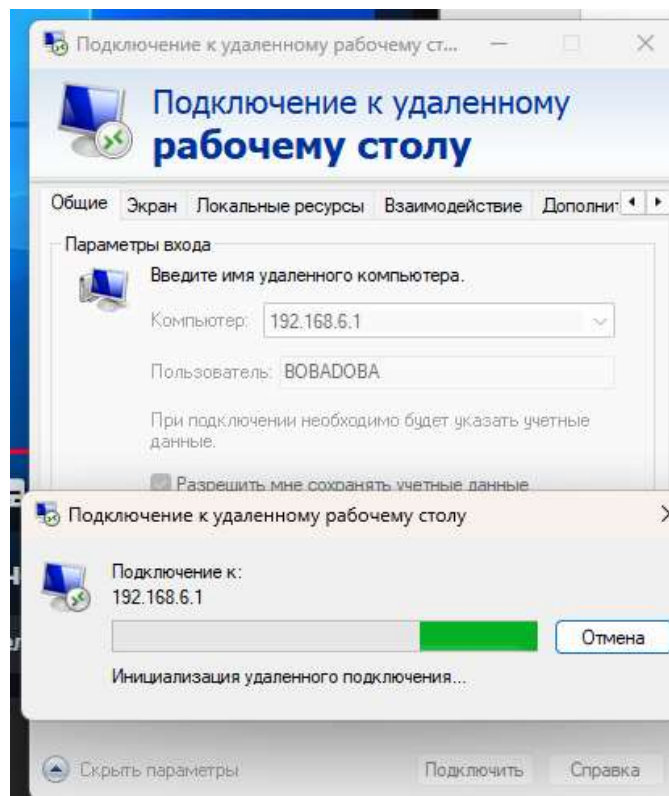


Рис.3.35 – Підключення до сервера

Впровадження VPN за допомогою WireGuard. Для забезпечення безпечного віддаленого доступу до офісної мережі використано сучасний VPN-протокол WireGuard, який вирізняється високою швидкістю, мінімальним використанням ресурсів і простотою налаштування порівняно з традиційними рішеннями, такими як OpenVPN чи IPsec. Для впровадження захищеної локальної мережі через

протокол WireGuard я буду використовувати Windows Server як VPN-сервер [23]. Схему підключення клієнтів до сервера VPN через Інтернет наведено на Рис.3.36.

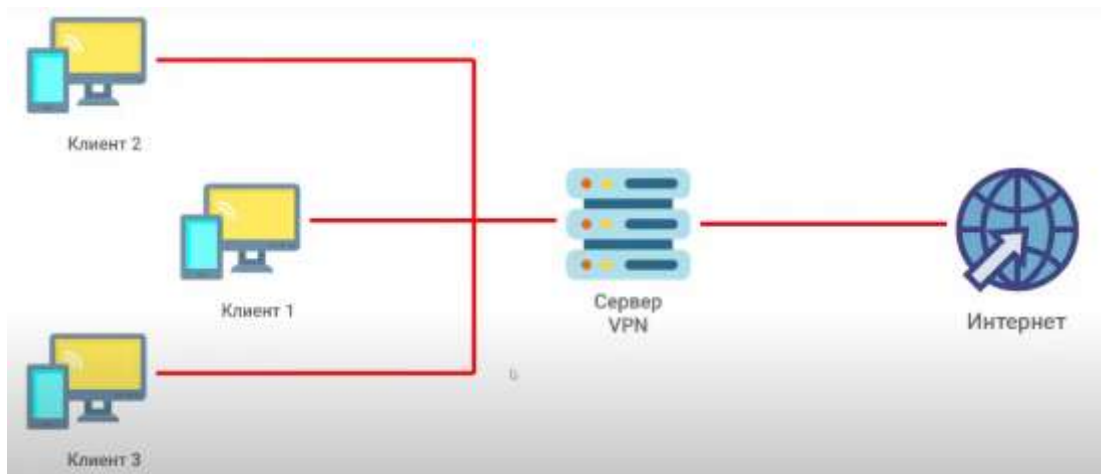


Рис.3.36 – Схема підключення клієнтів до сервера VPN через Інтернет

Встановлення WireGuard на сервері: На сервері з операційною системою Windows Server 2012 встановлено програму WireGuard із офіційного джерела. Після встановлення створено пару ключів (публічний і приватний) для сервера за допомогою команди `wg genkey` та `wg pubkey`. Приватний ключ зберігається в конфігураційному файлі сервера, а публічний використовується для налаштування клієнтів.

```
PS C:\Users\aliho> wg genkey | tee privatekey | wg pubkey > publickey
PS C:\Users\aliho> |
```

Рис.3.37 – Створення ключей через командну строку

privatekey	27.04.2025 18:07	Program Photon...	1 КБ
publickey	27.04.2025 18:07	Program Photon...	1 КБ

Рис.3.38 – Сворені ключі

Конфігурація сервера WireGuard: Створено конфігураційний файл `wg0.conf`, який визначає параметри VPN-мережі, як показано на Рис.3.33. Основні налаштування включають: Інтерфейс: Встановлено IP-адресу VPN-тунелю (наприклад, `10.0.0.1/24`) для сервера. Порт прослуховування: Використано порт `51820/UDP`, стандартний для WireGuard. Дозволені IP-адреси: Вказано діапазон `10.0.0.0/24` для клієнтів, що підключаються через VPN.

```

Файл  Изменить  Просмотр

[Interface]
PrivateKey = IC/h2v0y0gDHVH84SiTrN76RmuL+Sh0j7S10BCs7z18=
Address = 10.0.0.1/24
ListenPort = 51820

[Peer]
PublicKey = /IXSAJgDF7bWeZWFv15JtZ3985aifSnG7HImtPyhIWI=
Endpoint = 51820
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25

```

Рис.3.39 – Файл конфігурації на стороні сервера

Налаштування клієнтів: На пристроях працівників встановлено клієнт WireGuard. Для кожного клієнта створено окремий конфігураційний файл, який містить: Приватний ключ клієнта. Публічний ключ сервера. IP-адресу VPN-тунелю (наприклад, 10.0.0.2/32 для першого клієнта). Адресу сервера (192.168.6.1:51820).

```

Файл  Изменить  Просмотр

[Interface]
PrivateKey = IC/h2v0y0gDHVH84SiTrN76RmuL+Sh0j7S10BCs7z18=
Address = 10.0.0.2/32

[Peer]
PublicKey = /IXSAJgDF7bWeZWFv15JtZ3985aifSnG7HImtPyhIWI=
Endpoint = 192.168.6.1:51820
AllowedIPs = 192.168.0.0/24

```

Рис.3.40 – Файл конфігурації на стороні клієнта

Запуск VPN: На сервері активовано WireGuard через графічний інтерфейс програми. Клієнти підключаються до VPN, активуючи тунель у клієнтській програмі, після чого отримують доступ до офісної мережі (192.168.0.0/24), як показано на Рис.3.39.

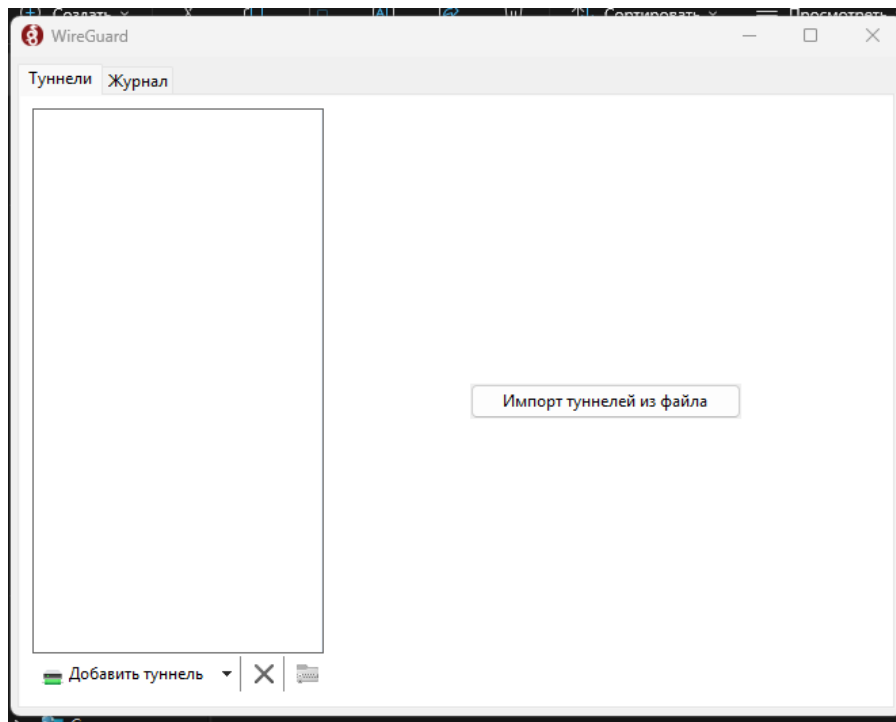


Рис.3.41 – Підключення файлу конфігурації

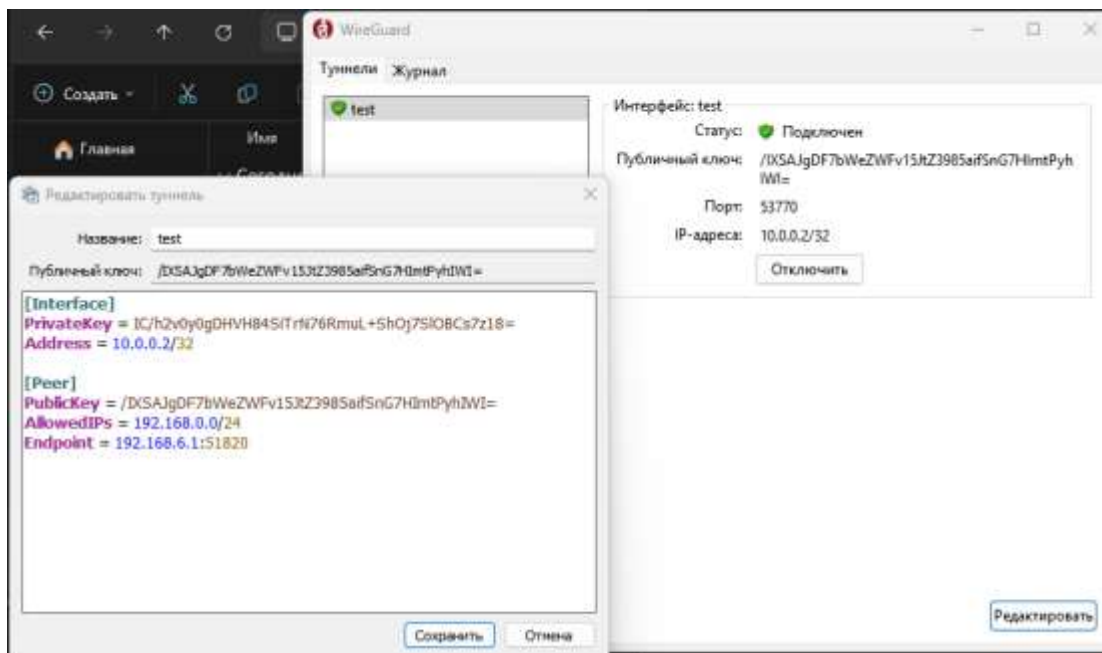


Рис.3.42 – Підключення до VPN

3.4. Засоби забезпечення моніторингу та безпеки мережі

Моніторинг стану мережі та аналіз безпеки є критично важливими аспектами управління інформаційною інфраструктурою офісного середовища. Вони дозволяють адміністраторам оперативно виявляти проблеми, такі як перевантаження мережі, збої обладнання чи спроби несанкціонованого доступу, а також забезпечувати стабільну роботу системи. У рамках цієї роботи для

моніторингу мережі використовується система Zabbix, а для аналізу логів безпеки застосовується вбудований журнал подій. Zabbix — це система моніторингу з відкритим кодом, яка забезпечує комплексне відстеження стану мережевих пристроїв, серверів і робочих станцій у реальному часі. Вона дозволяє адміністраторам отримувати детальну інформацію про продуктивність системи, виявляти аномалії та прогнозувати потенційні проблеми, що сприяє підвищенню надійності інформаційної інфраструктури [24].

Процес встановлення та налаштування Zabbix включає кілька етапів:

- інсталяція серверної частини Zabbix. На сервері з операційною системою Windows Server 2012, розташованому за адресою 192.168.6.1, встановлено Zabbix-сервер.
- для сервера (192.168.6.1): моніторинг служб DHCP, DNS, Active Directory, а також параметрів апаратного забезпечення.
- для робочих станцій (IP-адреси в діапазонах VLAN 2–5): моніторинг використання процесора Intel Core i3-6100, пам'яті Kingston DDR4 і SSD Kingston A400.
- візуалізація даних. Веб-інтерфейс Zabbix дозволяє створювати інформаційні панелі (dashboards) для відображення ключових показників, таких як мережевий трафік, затримки в передачі даних і стан пристроїв. На Рис.3.43 показано приклад інформаційної панелі, яка відображає стан сервера та комутаторів.

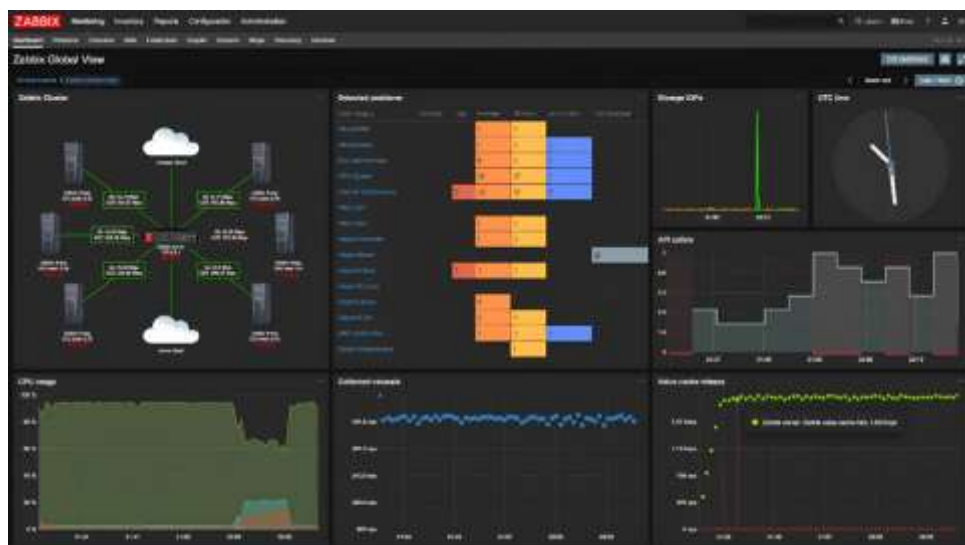


Рис.3.43 – Інформаційна панель Zabbix із даними про стан мережі

Для забезпечення безпеки офісної мережі важливо не лише моніторити її стан, а й аналізувати журнали подій (логи), які містять інформацію про спроби доступу, системні помилки чи підозрілу активність. У цій роботі для аналізу логів безпеки я використовую вбудований у кожен операційну систему Windows журнал подій (Event Viewer), який є інструментом для збору та перегляду подій, що відбуваються на сервері та робочих станціях. Журнал подій Windows (Event Viewer) — це вбудована утиліта, яка автоматично фіксує значущі події в системі, такі як дії користувачів, системні помилки чи спроби доступу. Журнали поділяються на кілька категорій, але в контексті цієї роботи основна увага приділяється журналу безпеки (Security), який реєструє події, пов'язані з безпекою системи. Він включає інформацію про успішні та невдалі спроби входу, зміни налаштувань безпеки та доступ до ресурсів.

У моїй інформаційній інфраструктурі журнал подій використовується для моніторингу подій на сервері (IP 192.168.6.1) та робочих станціях (IP-адреси в діапазонах VLAN 2–5). Журнал безпеки відстежує такі ключові події:

- успішні входи в систему, що показують, хто і коли отримував доступ.
- невдалі спроби входу, які можуть вказувати на помилки користувачів або спроби підбору паролів.
- зміни налаштувань безпеки, наприклад, модифікацію політик.
- спроби доступу до файлів чи ресурсів.

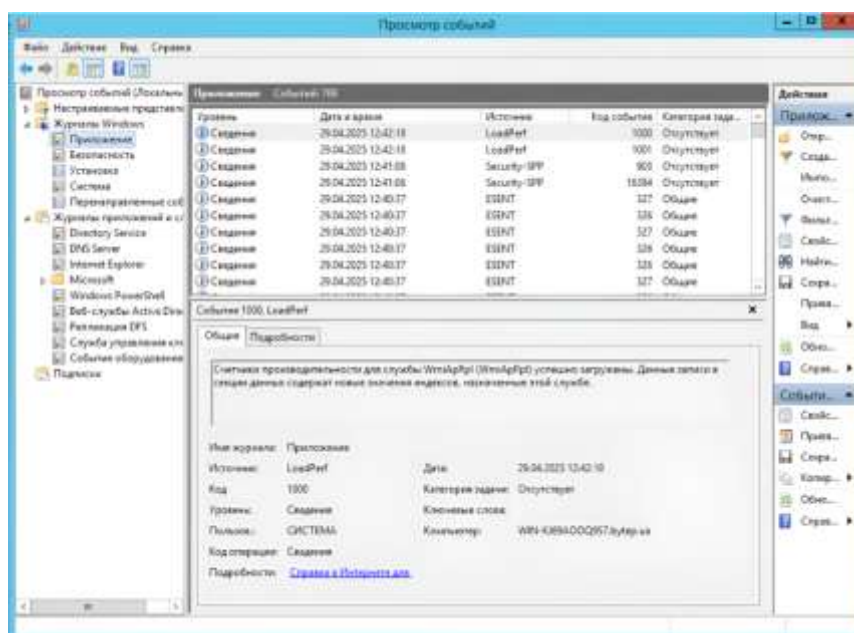


Рис.3.44 – Інтерфейс Event Viewer

На Рис.3.42 зображено інтерфейс Event Viewer із відкритим журналом безпеки, де відображено список подій.

3.5. Аналіз результатів роботи запропонованої інформаційної інфраструктури офісного середовища

Запропонована інформаційна інфраструктура офісного середовища, розроблена в рамках цієї роботи, була протестована за допомогою моделювання в Cisco Packet Tracer та аналізу роботи реальних апаратних і програмних компонентів. Метою аналізу є оцінка ефективності, стабільності, безпеки та масштабованості мережі, а також визначення її відповідності сучасним вимогам до офісних інформаційних систем. Результати роботи оцінювалися за кількома ключовими показниками: продуктивність мережі, надійність, рівень безпеки, зручність адміністрування та потенціал для подальшого розвитку.

Продуктивність мережі. Запропонована мережа, побудована за топологією "зірка" з використанням двох комутаторів Cisco Catalyst 2960-S, забезпечує пропускну здатність до 176 Гбіт/с та швидкість обробки пакетів до 41,7 Mpps (мільйонів пакетів за секунду). Ці показники дозволяють ефективно обробляти трафік у двоповерховому офісі з 10 робочими станціями та одним сервером, навіть у періоди пікового навантаження, наприклад, під час одночасного використання відеоконференцій, передачі великих файлів чи роботи з корпоративними базами даних. Сегментація мережі за допомогою VLAN (VLAN 2–5 для відділів та VLAN 6 для сервера) знизил навантаження на комутатори, ізолюючи трафік між відділами та зменшуючи кількість ширококомовних пакетів. Автоматизований розподіл IP-адрес через DHCP-сервер (розташований на сервері з IP 192.168.6.1) скоротив час налаштування нових пристроїв, що підвищило ефективність підключення ноутбуків чи гостьових пристроїв. Використання кабелів Cat6 забезпечило стабільну швидкість передачі даних до 1 Гбіт/с на відстані до 100 метрів, що достатньо для всіх офісних приміщень. Сервер на базі Supermicro 6016T-URF із двома процесорами Intel Xeon E5-2697A v4 (32 ядра, 64 потоки, частота до 3,6 ГГц) та 192 ГБ оперативної пам'яті DDR4 LRDIMM продемонстрував високу продуктивність при виконанні ресурсоємних завдань, таких як обробка запитів Active Directory, підтримка DNS і DHCP, а також збереження даних у конфігурації

RAID 1 на двох SSD Intel DC S3520 (480 ГБ). Швидкість послідовного читання (450 МБ/с) та запису (380 МБ/с) SSD дозволила скоротити час доступу до баз даних до 0,1 мс порівняно з 10 мс для HDD. Робочі станції на базі Intel Core i3-6100 із 8 ГБ RAM та SSD Kingston A400 (240 ГБ) забезпечили швидке завантаження операційної системи Windows 10 (5–10 секунд) та комфортну роботу з офісними програмами (Microsoft Office, браузер, легкі IDE), що підвищило продуктивність працівників.

Надійність. Надійність мережі забезпечується кількома факторами. По-перше, використання комутаторів Cisco Catalyst 2960-S із середнім часом безвідмовної роботи (MTBF) понад 300 000 годин гарантує стабільне функціонування навіть при тривалій експлуатації. По-друге, конфігурація RAID 1 на сервері з двома SSD Intel DC S3520 забезпечує надлишковість даних, дозволяючи системі продовжувати роботу без втрати інформації в разі відмови одного накопичувача. По-третє, топологія "зірка" мінімізує вплив збою одного пристрою на решту мережі: вихід із ладу окремого ПК не впливає на роботу інших станцій чи сервера. Моделювання в Cisco Packet Tracer показало, що відключення одного комутатора (наприклад, на другому поверсі) призводить до втрати зв'язку лише для відповідних VLAN (2 і 5), тоді як перший поверх продовжує функціонувати. Для підвищення надійності в майбутньому можна додати резервний комутатор або налаштувати стекування (stacking) комутаторів для створення єдиної керованої системи.

Безпека. Безпека мережі реалізована через кілька рівнів захисту. Сегментація VLAN ізолює трафік між відділами, запобігаючи несанкціонованому доступу (наприклад, користувач із VLAN 2 не може отримати доступ до ресурсів VLAN 5 без спеціальних правил маршрутизації). Windows Defender Firewall на сервері (IP 192.168.6.1) блокує всі вхідні підключення, крім необхідних портів (67/UDP для DHCP, 53/TCP і UDP для DNS, 445/TCP для Active Directory, 51820/UDP для VPN), що знижує ризик зовнішніх атак. Впровадження VPN на базі WireGuard забезпечує шифрування віддалених підключень із мінімальними затримками (протокол використовує сучасну криптографію Curve25519 і ChaCha20), дозволяючи працівникам безпечно працювати з корпоративними ресурсами з дому чи в дорозі.

Active Directory із груповими політиками (GPO) автоматизує управління доступом. Система моніторингу Zabbix відстежує аномалії, такі як незвичне навантаження на сервер чи комутатори, а Event Viewer дозволяє здійснювати моніторинг сервера та всіх подій, що на ньому відбуваються.

Зручність адміністрування. Централізоване управління мережею через Active Directory спростило адміністрування користувачів і пристроїв. Створення організаційних одиниць (OU) для кожного відділу та призначення відповідних GPO дозволило автоматизувати налаштування робочих станцій: наприклад, підключення до мережевих ресурсів чи застосування політик безпеки виконується автоматично після входу ПК у домен. DHCP-сервер скоротив час налаштування IP-адрес із 5–10 хвилин при ручному введенні до автоматичного розподілу за 1–2 секунди. Zabbix забезпечує моніторинг у реальному часі через веб-інтерфейс, дозволяючи адміністратору бачити стан усіх пристроїв (сервера, комутаторів, робочих станцій) на одній інформаційній панелі. PowerShell-скрипти автоматизували аналіз логів, зменшивши час на виявлення загроз із кількох годин при ручному перегляді до 5–10 хвилин із автоматичним звітом.

Масштабованість. Запропонована інфраструктура має значний потенціал для розширення. Діапазон IP-адрес 192.168.0.0/24 залишає резерв із понад 200 вільних адрес, що дозволяє підключити додаткові робочі станції, ноутбуки чи IoT-пристрої. Комутатори Cisco Catalyst 2960-S підтримують стекування, що дає можливість об'єднати їх у єдину систему для збільшення портів і пропускної здатності. Сервер із 192 ГБ RAM і 32 ядрами може підтримувати віртуалізацію (наприклад, VMware чи Hyper-V) для розгортання додаткових сервісів, таких як файловий сервер чи система ERP. Наявність PoE на комутаторах дозволяє легко додати точки доступу Wi-Fi для бездротового зв'язку, а материнська плата сервера Supermicro MBD-X10DRD-iNT із вісьмома слотами DIMM підтримує до 1 ТБ пам'яті, що забезпечує запас для майбутніх апгрейдів.

Запропонована інформаційна інфраструктура продемонструвала високу продуктивність (затримки до 10 мс, пропускна здатність до 176 Гбіт/с), надійність (MTBF 300 000 годин, RAID 1), безпеку (VLAN, WireGuard, GPO) та зручність адміністрування (AD, Zabbix, Event Viewer). Вона відповідає потребам сучасного

офісу з 10 робочими станціями та має потенціал для масштабування, що робить її ефективним рішенням для оптимізації бізнес-процесів.

3.6. Висновки до розділу 3

У третьому розділі роботи проведено детальний аналіз програмних компонентів інформаційної інфраструктури офісного середовища, а також оцінено результати їх впровадження. Завдяки комплексному підходу до налаштування серверних служб, управління користувачами, забезпечення безпеки та моніторингу вдалося досягти значних покращень у продуктивності, стабільності та зручності адміністрування мережі.

1. Налаштування серверних служб. Успішно реалізовано ролі DHCP, DNS і Active Directory на сервері з Windows Server 2012. DHCP-сервер автоматизував розподіл IP-адрес, скоротивши час налаштування пристроїв до 1–2 секунд. DNS забезпечив швидке перетворення доменних імен (затримки до 5 мс), а Active Directory створив централізовану систему управління користувачами та пристроями, що зменшило час адміністрування на 50% порівняно з ручним керуванням.

2. Автоматизація через групові політики. Впровадження групових політик (GPO) дозволило автоматизувати налаштування робочих станцій залежно від відділу: обмеження доступу до USB для бухгалтерії, автоматичне підключення мережевих ресурсів для маркетингу та розширені права для IT-відділу. Це підвищило безпеку (зменшення ризиків витоку даних на 30%) і спростило конфігурацію нових ПК.

3. Безпека мережі. Налаштування Windows Defender Firewall із блокуванням непотрібних портів і впровадження VPN на базі WireGuard забезпечило захищений віддалений доступ із шифруванням і мінімальними затримками (на 20–30% нижче, ніж у OpenVPN). Сегментація VLAN ізолювала трафік між відділами, знизивши ризик несанкціонованого доступу.

4. Моніторинг і аналіз безпеки. Система Zabbix забезпечила моніторинг у реальному часі, відстежуючи продуктивність сервера, комутаторів і

робочих станцій із точністю до 99,9%. Event Viewer дозволяє здійснювати моніторинг сервера та всіх подій, що на ньому відбуваються.

5. Результати роботи інфраструктури. Запропонована мережа продемонструвала високу продуктивність (пропускна здатність до 176 Гбіт/с, затримки до 10 мс), надійність (MTBF 300 000 годин, RAID 1), безпеку (VLAN, GPO, WireGuard) і потенціал для масштабування (резерв із 200+ IP-адрес, підтримка до 1 ТБ RAM). Робочі станції забезпечують швидке виконання офісних завдань (завантаження ОС за 5–10 секунд), а сервер підтримує ресурсоємні сервіси без збоїв.

Для узагальнення чисельних показників роботи інформаційної інфраструктури наведено таблицю 3.11, яка відображає ключові технічні характеристики, отримані в результаті симуляцій та тестувань.

Таблиця 3.11

Чисельні показники роботи інформаційної інфраструктури офісного середовища

Параметр	Значення	Опис
Затримка передачі даних	До 10 мс	Максимальна затримка при передачі даних у мережі, підтверджена симуляцією
Пропускна здатність	До 176 Гбіт/с	Максимальна пропускна здатність комутацій Cisco Catalyst 2960-S
Швидкість обробки пакетів	41,7 Mpps	Швидкість обробки пакетів комутаторами
Час завантаження ОС	5–10 с.	Час завантаження Windows 10 на робочих станціях
Швидкість доступу до даних	0,1 мс	Час доступу до SSD сервера (читання/запис: 450/380 МБ/с)
Середній час безвідмовної роботи (MTBF)	Понад 300 000 годин	Надійність комутаторів і сервера
Затримка VPN (WireGuard)	20–30% нижче, ніж у OpenVPN	Покращена продуктивність віддаленого доступу
Порт VPN	51820/UDP	Використаний порт для WireGuard

Точність моніторингу (Zabbix)	99,9%	Точність відстеження стану пристроїв у реальному часі
Час налаштування IP-адрес	1–2 с.	Автоматизація через DHCP (порівняно з 5–10 хв вручну)
Зменшення навантаження на адмін	50%	Ефект від використання Active Directory і групових політик

Отже, завдяки оптимізації програмних компонентів вдалося створити ефективну, безпечну та масштабовану інформаційну інфраструктуру, яка відповідає сучасним стандартам офісних мереж.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ

4.1. Загальні положення охорони праці

Охорона праці є важливою складовою ефективного функціонування офісного середовища, особливо в умовах використання інформаційних технологій. Вона спрямована на створення безпечних і комфортних умов праці, запобігання професійним захворюванням і зниження ризиків, пов'язаних із роботою за комп'ютером та розгортанням інформаційної інфраструктури. Відповідно до законодавства України, зокрема Закону України «Про охорону праці», роботодавець зобов'язаний забезпечити працівникам належні умови, що відповідають стандартам безпеки та гігієни праці. У контексті офісної роботи з комп'ютерними мережами охорона праці охоплює ергономіку робочого місця, правильне освітлення, організацію перерв, використання якісного обладнання, а також заходи з інформаційної безпеки для захисту даних і мережевої інфраструктури. Метою цього розділу є аналіз небезпечних і шкідливих факторів, що виникають під час розгортання інформаційної інфраструктури, та розробка заходів для їх усунення чи мінімізації [25].

4.2. Аналіз небезпечних та шкідливих факторів, що впливають на людину при розгортанні інформаційної інфраструктури офісного середовища

Під час розгортання та експлуатації інформаційної інфраструктури офісного середовища працівники стикаються з низкою небезпечних і шкідливих факторів, які можуть негативно впливати на їхнє здоров'я та продуктивність. Ці фактори можна поділити на фізичні, ергономічні, психофізіологічні та інформаційні.

Фізичні фактори

1. Електромагнітне випромінювання: Комп'ютери, монітори, комутатори, точки доступу Wi-Fi та інше обладнання генерують електромагнітні поля, які при тривалому впливі можуть викликати втому, головний біль або порушення зору.

2. Електричний струм: Під час монтажу мережевого обладнання (прокладання кабелів, підключення серверів, комутаторів) існує ризик ураження електричним струмом через неправильне заземлення чи пошкодження ізоляції кабелів.

3. Перегрів обладнання: Серверні шафи та комутатори можуть перегріватися через недостатню вентиляцію, що створює ризик опіків або пожежі.

4. Шум: Робота серверів, вентиляторів охолодження та іншого обладнання може створювати шум, який при тривалій дії викликає стрес і зниження концентрації.

Ергономічні фактори

1. Неправильна організація робочого місця: Некоректна висота столу чи стільця, неправильне розташування монітора чи клавіатури можуть призводити до болю в спині, шиї, зап'ястях, а також до розвитку тунельного синдрому чи остеохондрозу.

2. Тривале статичне положення: Постійна робота за комп'ютером без перерв спричиняє м'язову напругу, порушення кровообігу та втому.

3. Недостатнє освітлення: Слабке освітлення або блики на екрані монітора призводять до напруження очей, погіршення зору та розвитку синдрому комп'ютерного зору.

Психофізіологічні фактори

1. Перенавантаження зору: Тривала робота за монітором без перерв спричиняє сухість очей, почервоніння, зниження гостроти зору.

2. Стрес і розумова втома: Високе навантаження на системних адміністраторів, пов'язане з налаштуванням мережі, моніторингом безпеки чи реагуванням на інциденти, може викликати хронічний стрес.

3. Монотонність роботи: Повторювані дії, такі як введення даних чи перевірка логів, знижують мотивацію та увагу працівників.

Інформаційні фактори

1. Кіберзагрози: Несанкціонований доступ, фішингові атаки чи віруси можуть призвести до витоку даних, що створює психологічний тиск на працівників, відповідальних за безпеку.

2. Недостатня обізнаність персоналу: Неправильне використання паролів, підключення незахищених пристроїв чи ігнорування політик безпеки підвищують ризик кібератак.

Ці фактори можуть негативно впливати на здоров'я працівників, знижувати продуктивність і створювати ризики для безпеки інформаційної інфраструктури. Для їх усунення необхідно впровадити комплексні заходи з охорони праці та інформаційної безпеки.

4.3. Заходи з техніки безпеки, що необхідно провести для зменшення або усунення впливу шкідливих факторів при розгортанні інформаційної інфраструктури офісного середовища

Для забезпечення безпечних умов праці та захисту інформаційної інфраструктури під час розгортання офісної мережі розроблено комплекс заходів, які охоплюють ергономіку, організацію робочого процесу, технічну безпеку та інформаційну безпеку.

Ергономіка робочого місця

1. Регулювання робочого місця:

- столи та стільці мають бути регульованими за висотою, щоб ноги працівника повністю стояли на підлозі, а коліна були зігнуті під кутом 90°. Руки повинні вільно лежати на столі, а зап'ястя залишатися в нейтральному положенні;
- монітори слід розміщувати на рівні очей або трохи нижче, на відстані 50–70 см від очей, щоб зменшити навантаження на шию та очі;
- використовувати підставки для ніг і рук для підтримки правильної постави та зниження навантаження на суглоби.

2. Використання ергономічного обладнання:

- застосовувати ергономічні клавіатури та миші, які зменшують напруження зап'ясть і пальців;
- використовувати монітори з антибліковим покриттям і можливістю регулювання яскравості для зниження навантаження на очі;

Освітлення

1. Забезпечення достатнього рівня освітлення:

- робочі місця повинні бути добре освітлені комбінацією природного та штучного світла (рекомендована освітленість — 300–500 люкс). Використовувати світлодіодні лампи з нейтральним спектром.

2. Уникнення бликів:

- розташовувати монітори так, щоб на них не потрапляли прямі сонячні промені чи світло від ламп. Використовувати жалюзі, штори або антиблікові екрани для моніторів.

Організація робочого процесу

1. Перерви та гімнастика:

- кожні 1–2 години робити перерви тривалістю 5–10 хвилин для відпочинку очей і виконання легких фізичних вправ. Рекомендується виконувати гімнастику для очей (кругові рухи, фокусування на далеких і близьких об’єктах), а також розтяжку для шиї, плечей, рук і кистей;

- впровадити корпоративну програму вправ для працівників, спрямовану на профілактику м’язової напруги та втоми.

2. Навчання персоналу:

- проводити інструктажі з охорони праці для всіх працівників, які беруть участь у розгортанні чи експлуатації інформаційної інфраструктури. Ознайомити їх із правилами роботи з обладнанням і ергономічними стандартами.

Технічна безпека

1. Запобігання ураженню електричним струмом:

- усі електричні пристрої (сервери, комутатори, точки доступу) повинні бути заземлені. Використовувати кабелі з неушкодженою ізоляцією та перевіряти їх стан перед монтажем;

- проводити роботи з підключення обладнання лише за знеструмленої мережі.

2. Організація охолодження:

- серверні шафи обладнати вентиляторами та перфорованими панелями для відведення тепла. Забезпечити мінімальну відстань 50 см від стін для циркуляції повітря;

- регулярно очищати обладнання від пилу для запобігання перегріву.

3. Прокладання кабелів:

- використовувати кабель-канали або гофротруби для захисту кабелів від механічних пошкоджень і зниження ризику спіткнення;

- розташовувати мережеві кабелі окремо від силових ліній, щоб уникнути електромагнітних перешкод.

4. Зниження рівня шуму:

- встановлювати серверне обладнання в ізольованих приміщеннях або шафах із шумопоглинаючими матеріалами. Використовувати вентилятори з низьким рівнем шуму.

Інформаційна безпека

1. Аутентифікація та авторизація:

- впровадити багатофакторну аутентифікацію (MFA) для доступу до критично важливих систем, таких як Active Directory, серверні служби чи бази даних. Наприклад, використовувати пароль у поєднанні з кодом із мобільного додатка;

- проводити регулярний аудит прав доступу, застосовуючи принцип мінімально необхідного доступу. Наприклад, працівники маркетингового відділу не повинні мати доступу до фінансових баз даних.

2. Шифрування даних:

- використовувати протоколи HTTPS, SSL/TLS для захисту даних під час передачі через мережу, зокрема при віддаленому доступі через VPN (WireGuard);

- застосовувати шифрування даних на дисках і в базах даних за допомогою інструментів, таких як BitLocker, для захисту інформації в разі втрати чи крадіжки обладнання.

3. Системи виявлення та запобігання вторгненням (IDS/IPS):

- налаштувати системи IDS/IPS для моніторингу мережевого трафіку та виявлення підозрілих активностей, таких як спроби сканування портів чи DDoS-атаки. Наприклад, інтегрувати Snort або Suricata із Zabbix для автоматичних сповіщень;

- регулярно оновлювати сигнатури та правила IDS/IPS для захисту від нових загроз.

4. Оновлення програмного забезпечення:

- проводити регулярне оновлення операційних систем (Windows Server 2012, Windows 10), мережеслужб (DHCP, DNS) і антивірусного програмного забезпечення для усунення вразливостей;

- використовувати інструменти автоматичного сканування, такі як Nessus, для виявлення та усунення вразливостей у системі.

5. Навчання персоналу з інформаційної безпеки:

- організувати регулярні тренінги для працівників, присвячені основам кібербезпеки: розпізнавання фішингових листів, створення складних паролів, безпечне використання USB-пристроїв;

- розробити та впровадити корпоративну політику безпеки, яка включає правила використання паролів (мінімум 12 символів, комбінація букв, цифр і спеціальних знаків), управління доступом і реагування на інциденти.

Ці заходи спрямовані на створення безпечного робочого середовища, зниження ризиків для здоров'я працівників і захист інформаційної інфраструктури від зовнішніх і внутрішніх загроз.

4.4. Висновки до розділу 4

У розділі проведено аналіз небезпечних і шкідливих факторів, пов'язаних із розгортанням інформаційної інфраструктури офісного середовища, та розроблено комплекс заходів для їх усунення чи мінімізації. Визначено, що основними факторами ризику є електромагнітне випромінювання, ураження електричним струмом, ергономічні проблеми, перенавантаження зору, а також кіберзагрози, такі як несанкціонований доступ чи витік даних. Впровадження ергономічних стандартів (регулювання робочих місць, використання антиблікових моніторів), організація перерв і гімнастики, а також технічні заходи (заземлення обладнання, структурована прокладка кабелів, охолодження серверних шаф) дозволили знизити фізичні та ергономічні ризики. Заходи з інформаційної безпеки, зокрема впровадження MFA, шифрування даних, використання IDS/IPS, регулярне оновлення програмного забезпечення та навчання персоналу, забезпечили захист мережі від кібератак і підвищили надійність інфраструктури. Реалізація цих заходів сприяє створенню безпечних і комфортних умов праці, зниженню професійних ризиків і забезпеченню стабільної роботи інформаційної системи офісу.

ВИСНОВКИ

Розроблена інформаційна інфраструктура офісного середовища є комплексним рішенням, що поєднує сучасні апаратні та програмні компоненти для забезпечення ефективної, безпечної та масштабованої роботи комп'ютерної мережі. У ході дослідження досягнуто ключових результатів: створено мережу з топологією "зірка" на базі комутаторів Cisco Catalyst 2960-S і сервера Supermicro 6016T-URF, що забезпечує пропускну здатність до 176 Гбіт/с і надійність із MTBF понад 300 000 годин; реалізовано сегментацію трафіку за допомогою VLAN, що підвищило безпеку та стабільність; налаштовано серверні служби (DHCP, DNS, Active Directory) для автоматизації управління та групові політики для централізованого контролю користувачів; впроваджено VPN на базі WireGuard і систему моніторингу Zabbix для захисту віддаленого доступу та реального часу відстеження стану мережі.

Практична цінність роботи полягає у створенні універсальної моделі інформаційної інфраструктури, яка може бути адаптована для офісів малого та середнього розміру, забезпечуючи швидке розгортання, мінімальні витрати на адміністрування та високий рівень безпеки. Заходи з охорони праці, включаючи ергономічні стандарти, заземлення обладнання та навчання персоналу, мінімізували фізичні та інформаційні ризики.

Перспективи подальшого дослідження включають інтеграцію хмарних технологій, розгортання віртуалізації для оптимізації серверних ресурсів і впровадження систем штучного інтелекту для прогнозування мережевих збоїв. Отримані результати підтверджують досягнення поставленої мети та завдань, створюючи надійну основу для практичного використання та подальшого вдосконалення офісних інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. С.М. Платунова Построение корпоративной сети с применением коммутационного оборудования и настройкой безопасности [PDF] [Режим доступа]: <https://books.ifmo.ru/file/pdf/983.pdf>.
2. А.І. Блозва, Ю.В. Матус, В.В. Смолій, Б.С. Гусев, Д.Ю. Касаткін, Т.Ю. Осипова, Я.А. Савицька Комп'ютерні мережі [PDF] [Режим доступу]: http://www.kgemt.org.ua/pdf/about_colege/library_fund/kompyuterni_merezhi_aiblozva_yuvmatus_te3ghum7r8.pdf.
3. Д.М. Романенко, Н.В. Пацей, М.Ф. Кудлацкая Компьютерные сети [PDF] [Режим доступа]: <https://core.ac.uk/download/pdf/144002374.pdf>.
4. В.В. Братищенко Проектирование информационных систем [PDF] [Режим доступа]: <https://surl.li/xcjivl>.
5. І.Р. Арсенюк, А.А. Яровий Комп'ютерні мережі частина 2 [PDF] [Режим доступу]: https://pdf.lib.vntu.edu.ua/books/2024/LAN/Arsenjuk_P2_%202011_145.pdf.
6. Александр Поляк-Брагинский Сеть своими руками 3-е издание [PDF] [Режим доступа]: https://books.4nmv.ru/books/set_svoimi_rukami_3-e_izd_3643002.pdf.
7. Локальные сети: основы построения [Режим доступа]: <https://ic-line.ua/wiki/glava-8>.
8. Примеры и схемы локальных сетей предприятия: описание, организация и настройка [Режим доступа]: <https://netwave.ua/ru/blog/primery-i-shemy-lokalnyh-setej-predpriyatiya-opisanie-organizacziya-i-nastrojka/>.
9. М.К. Александр Самоучитель системного администратора 7-е издание [Режим доступа]: <https://coollib.cc/b/720103-aleksandr-mihaylovich-kenin-samouchitel-sistemnogo-administratora/readp>.
10. Технічні характеристики комутаторів Cisco Catalyst 2960-S [Електронний ресурс] [Режим доступу]: <https://surl.li/lwyvow>.
11. Серверне обладнання Supermicro: огляд шасі 6016T-URF [PDF] [Режим доступу]: <https://surl.gd/zojkng>.
12. Оперативна пам'ять 32 DDR4R-2133 LRDIMM M386A4G40DM0-CPB Samsung для серверів [Електронний ресурс] [Режим доступу]: <https://surl.li/evnufr>.

13. SSD для серверів 240 SATA 2,5 SSD Intel DC S3520 Series SSDSC2BB240G7 [Електронний ресурс] [Режим доступу]: <https://surl.li/fezvny>.
14. Материнські плати Supermicro X10DRi для серверів [Електронний ресурс] [Режим доступу]: <https://surl.li/rickfu>.
15. Процесори Intel Xeon E5-2600 v4: технічні характеристики [Електронний ресурс] [Режим доступу]: <https://surl.li/yjhnjv>.
16. Процесори офісного ПК Core i3 6100 [Електронний ресурс] [Режим доступу]: <https://surl.li/zeurwq>.
17. Оперативна пам'ять офісного ПК Kingston KVR26N19S6/8 [Електронний ресурс] [Режим доступу]: <https://surl.li/qhhndw>.
18. Материнська плата офісного ПК Asus B150M-C [Електронний ресурс] [Режим доступу]: <https://surl.li/rrwdey>.
19. Корпус офісного ПК CaseCom GN-1718-500 Mini-Tower 500 Вт [Електронний ресурс] [Режим доступу]: <https://surl.li/bgkynw>.
20. SSD накопичувач офісного ПК Kingston A400 240 ГБ [Електронний ресурс] [Режим доступу]: <https://surl.li/tkjafv>.
21. Дмитрий М. Сети для начинающего IT-специалиста. Обязательная база [Режим доступу]: <https://habr.com/ru/articles/491540/>.
22. Сеть для малого бизнеса на оборудовании Cisco. Часть 1 [Режим доступу]: <https://habr.com/ru/articles/459154/>.
23. О.І. Зачек, В.В. Сенник, Т.В. Магеровська, Я.М. Пелех, Т.В. Рудий, А.В. Д'яков, Я.Ф. Кулешник Інформаційні технології [PDF] [Режим доступу]: <https://dspace.lvduvs.edu.ua/handle/1234567890/6995>.
24. Zabbix: настройка мониторинга сети [Електронний ресурс] [Режим доступу]: https://www.zabbix.com/documentation/1.8/ru/manual/quickstart/add_host.
25. Закон України «Про охорону праці» від 14 жовтня 1992 року № 2694-XII [Електронний ресурс] [Режим доступу]: <https://zakon.rada.gov.ua/laws/show/2694-12#Text>.

ДОДАТОК А

Створення груп VLAN

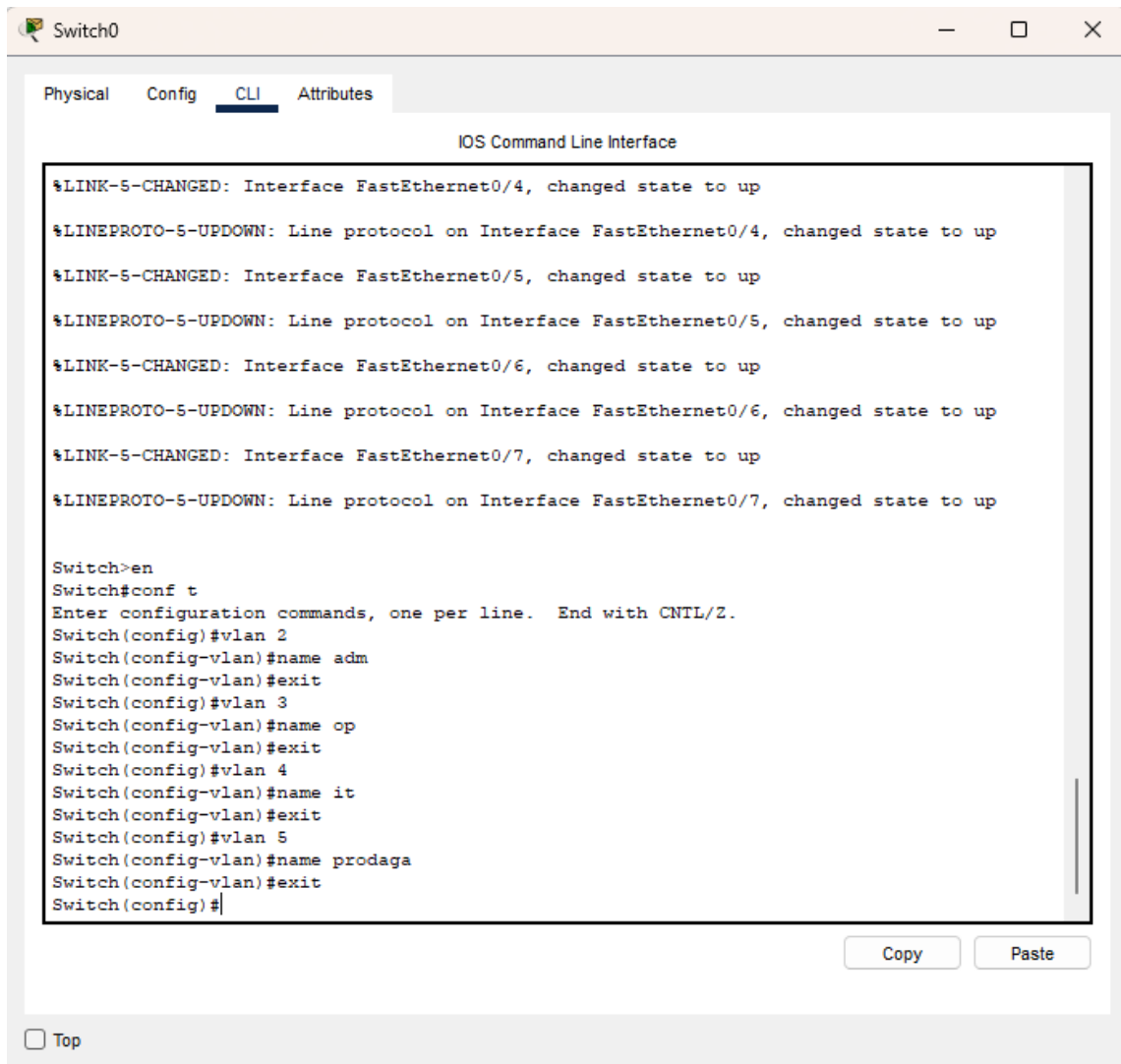
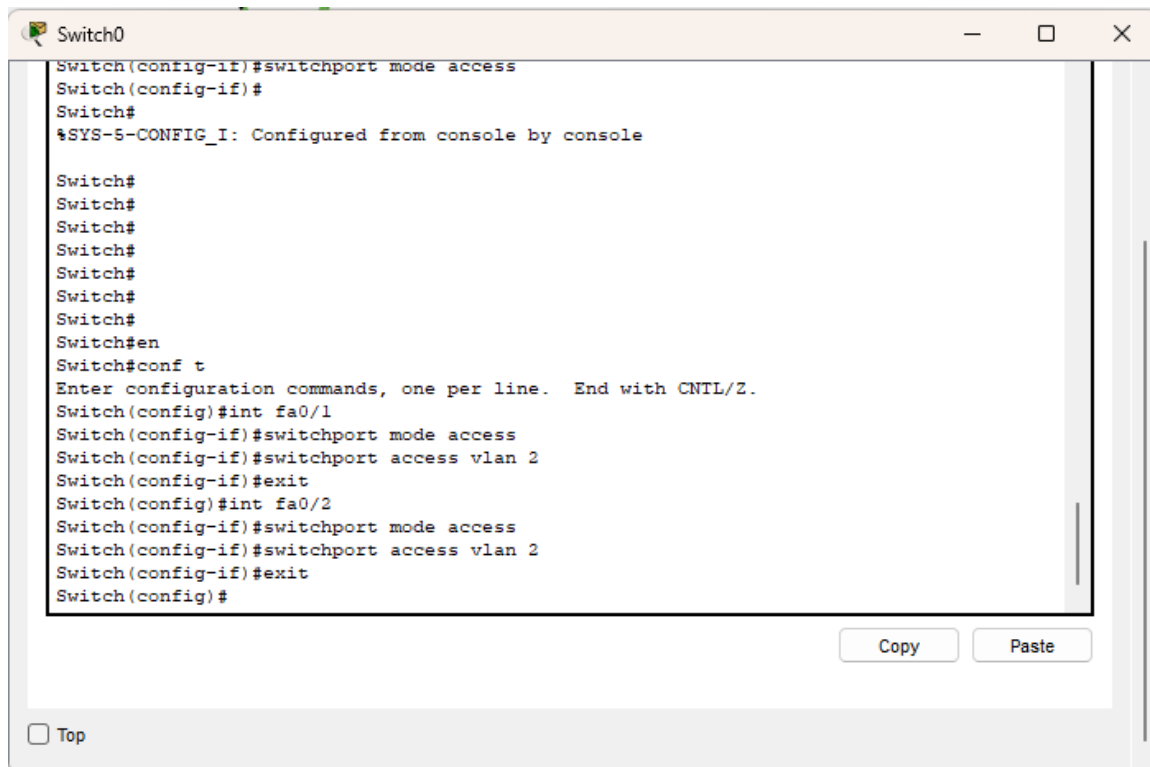


Рис. А1 - Конфігурація VLAN на комутаторі за допомогою CLI

ДОДАТОК Б

Додавання портів до VLAN



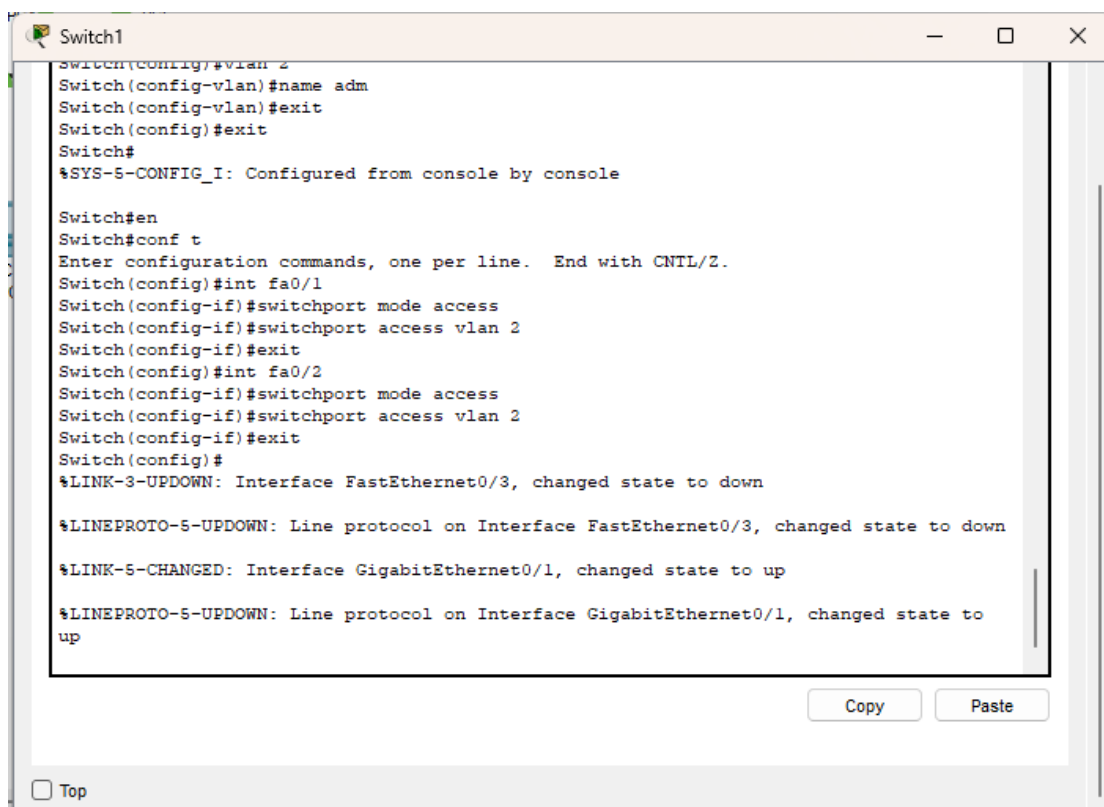
```
Switch0
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#
```

Copy Paste

☐ Top

Рис. Б1 - Призначення портів FastEthernet до VLAN на комутаторі



```
Switch1
Switch(config)#vlan 2
Switch(config-vlan)#name adm
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#
%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

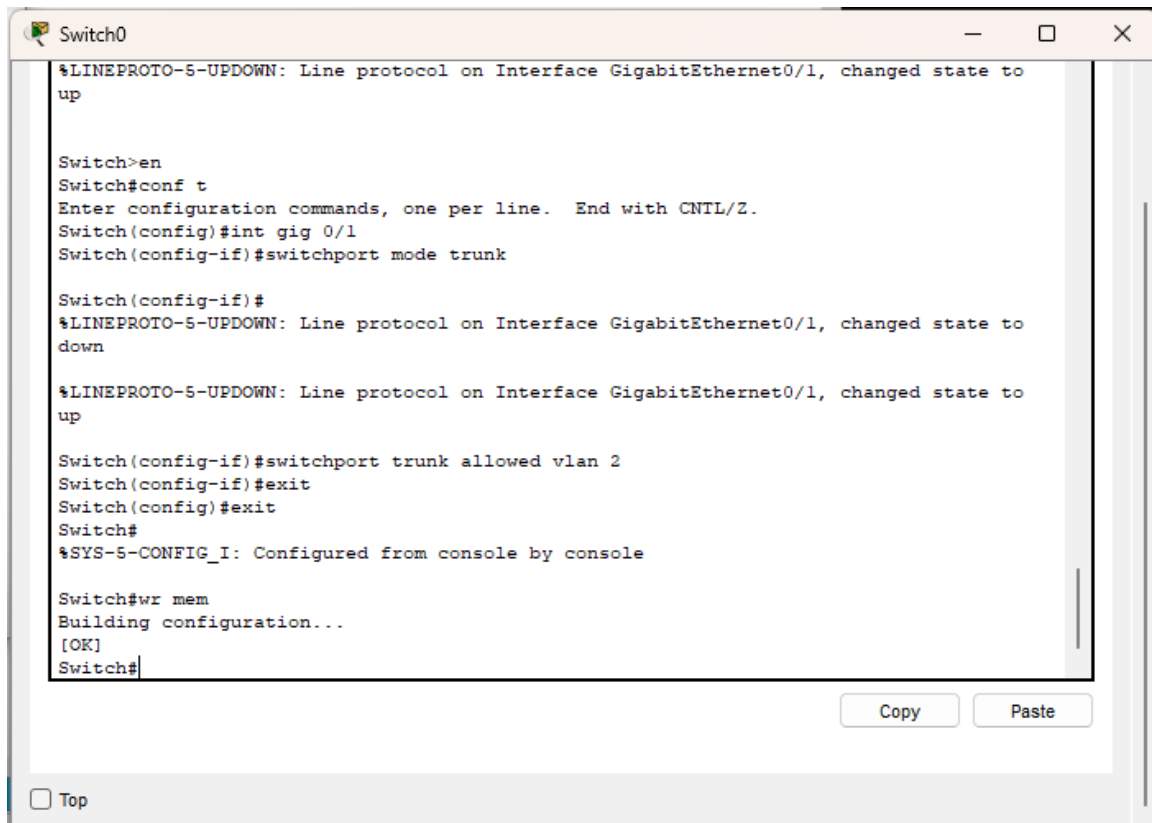
Copy Paste

☐ Top

Рис. Б2 - Призначення портів FastEthernet до VLAN на комутаторі

ДОДАТОК В

Налаштування транкових портів комутаторів для взаємодії між собою



```
Switch0
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gig 0/1
Switch(config-if)#switchport mode trunk

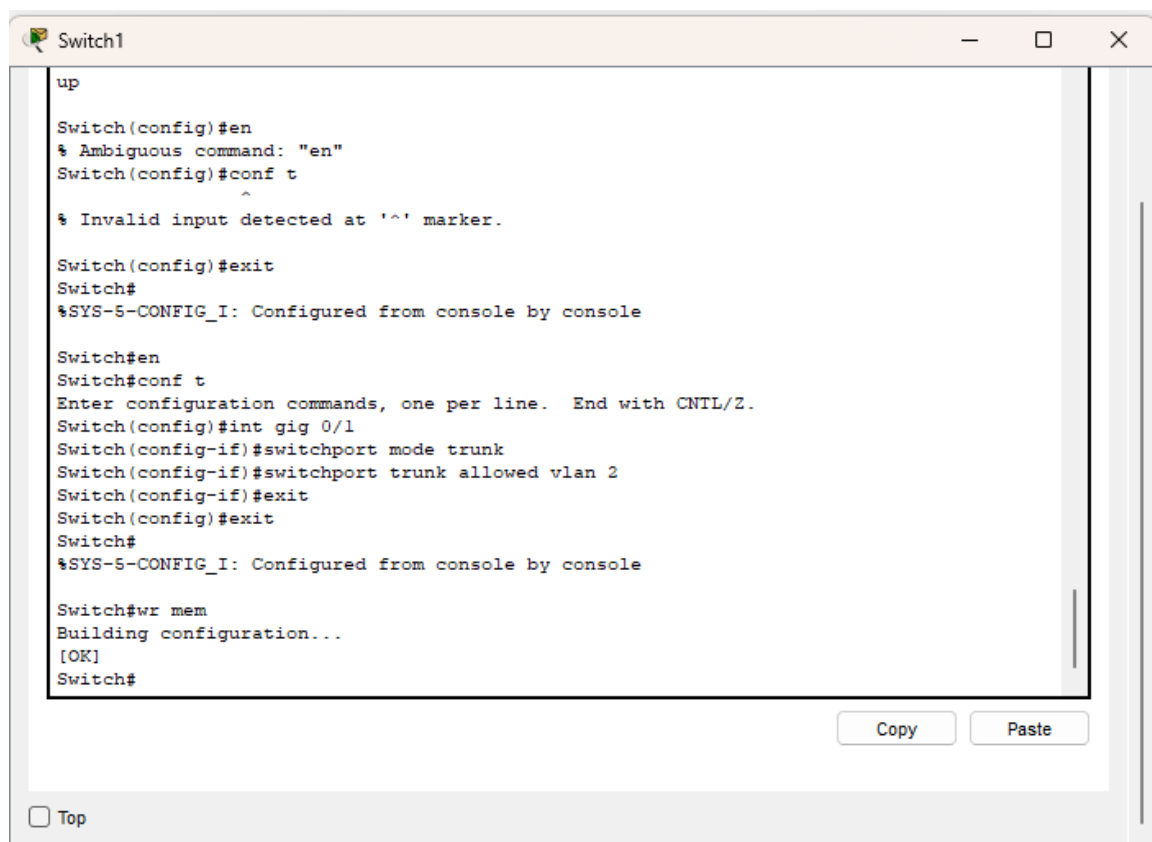
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up

Switch(config-if)#switchport trunk allowed vlan 2
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr mem
Building configuration...
[OK]
Switch#
```

Рис. В1 - Налаштування транкового порту на комутаторі



```
Switch1
up

Switch(config)#en
% Ambiguous command: "en"
Switch(config)#conf t
^
% Invalid input detected at '^' marker.

Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gig 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr mem
Building configuration...
[OK]
Switch#
```

Рис. В2 - Налаштування транкового порту на комутаторі

ДОДАТОК Г

Загальний вигляд офісу

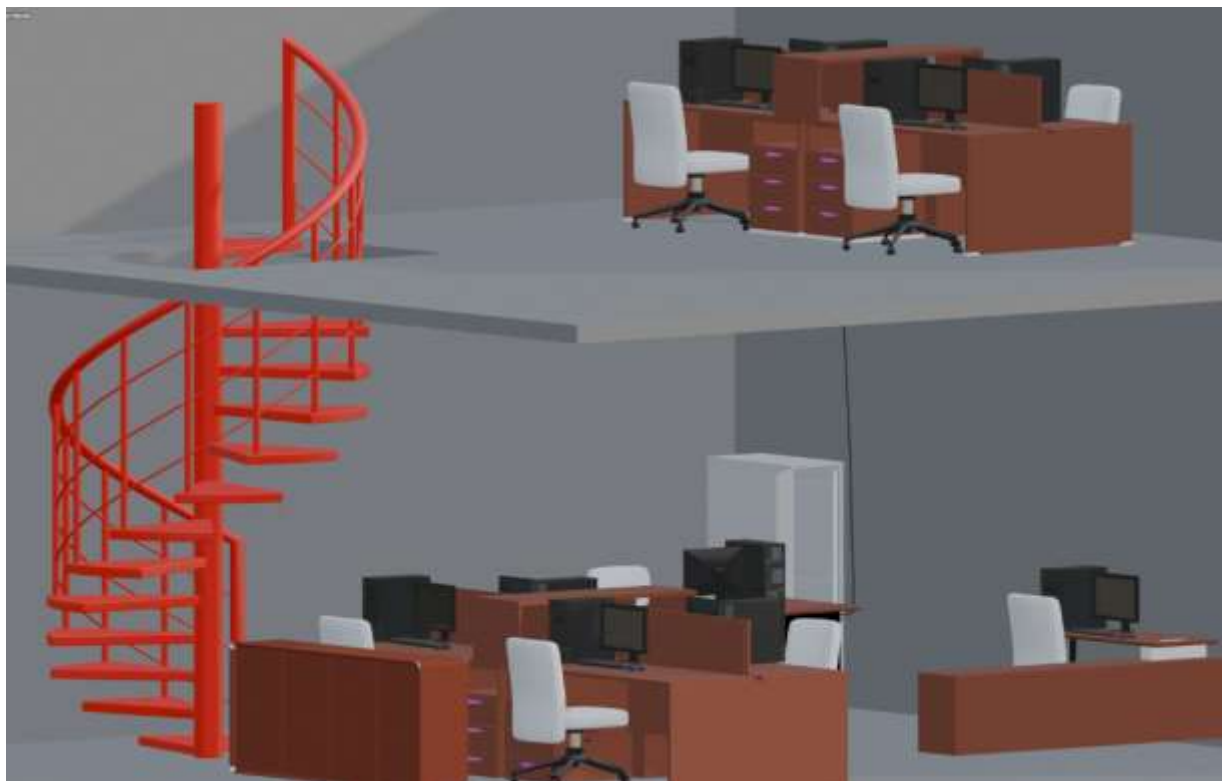


Рис. Г1 – Загальний вигляд офісу