

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

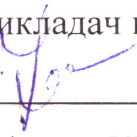
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної IT-інфраструктури компа-
нії на базі рішень Microsoft Active Directory»

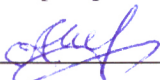
Виконав: студент 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Владислав ГАВРИЛЮК

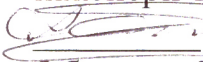
Керівник: старший викладач кафедри КІ та КБ,

 Ігор ФАЛЬКОВСЬКИЙ

Рецензент: доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Гаврилюк Владислав Богданович

Тема роботи: «Проект захищеної IT-інфраструктури компанії на базі рішень Microsoft Active Directory»

затверджена Наказом університету від 5 березня 2024 р. №97

Термін здачі студентом закінченої роботи 9 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Предметом дослідження є методи та засоби захисту IT-інфраструктури на базі рішень Microsoft Active Directory, які дозволяють створити ефективну та на-дійну систему управління доступом та захисту даних.

Об'єктом дослідження є IT-інфраструктура компанії, яка потребує захисту від потенційних кіберзагроз та забезпечення безпеки конфіденційної інформації.

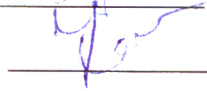
Обладнання та програмне забезпечення:

1. Гіпервізор Oracle VM VirtualBox
2. Програмне забезпечення GNS3
3. Операційні системи Windows 10, Kali Linux
4. Операційна система Windows Server 2019
5. Microsoft Active Directory

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

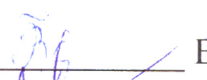
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О.С.	 05.03.2024	 05.03.2024
2	Головня О.С.	 05.03.2024	 05.03.2024
3	Головня О.С.	 05.03.2024	 05.03.2024

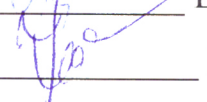
Студент  Владислав ГАВРИЛЮК

Керівник  Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05.03.2024	Виконано
2	Створення плану роботи	25.03.2024	Виконано
3	Опрацювання літературних джерел	03.04.2024 – 12.04.2024	Виконано
4	Написання вступної частини кваліфікаційної роботи	15.04.2024	Виконано
5	Аналіз теоретичних аспектів захисту IT-інфраструктури	16.04.2024 – 21.04.2024	Виконано
6	Огляд служби каталогів Active Directory	22.04.2024 – 25.04.2024	Виконано
7	Аналіз можливостей Active Directory для захисту мережі	27.04.2024 – 07.05.2024	Виконано
8	Проектування загальної топології	08.05.2024 – 17.05.2024	Виконано
9	Розробка IP-адресації та вибір обладнання	20.05.2024 – 25.05.2024	Виконано
10	Налаштування пристроїв мережі	27.05.2024 – 05.06.2024	Виконано
11	Встановлення і налаштування Active Directory	15.06.2024 – 19.06.2024	Виконано
12	Перевірка зроблених налаштувань	20.06.2024	Виконано
13	Написання пояснювальної записки	23.06.2024 – 26.06.2024	Виконано
14	Підготовка додаткових матеріалів	27.06.2024	Виконано
15	Отримання відгуку та рецензії	28.06.2024	Виконано
16	Захист	29.06.2024	Виконано

Студент  Владислав ГАВРИЛЮК

Керівник  Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Кваліфікаційна робота бакалавра на тему «Проект захищеної IT-інфраструктури компанії на базі рішень Microsoft Active Directory» присвячена розробці та впровадженню безпечної IT-інфраструктури для підприємства, використовуючи рішення Microsoft Active Directory. Пояснювальна записка складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текстова частина викладена на 87 сторінках друкованого тексту. Пояснювальна записка має 3 сторінки додатків. Список використаних джерел містить 21 найменування і займає 2 сторінки. В роботі наведено 77 рисунків. Загальний обсяг роботи – 94 сторінки.

Основною метою випускної кваліфікаційної роботи є розробка проекту захищеної IT-інфраструктури компанії на базі рішень Microsoft Active Directory, яка забезпечить надійний захист інформаційних ресурсів та ефективне управління доступом до них.

Досягнення поставленої мети передбачає роз'язання наступних завдань:

- Визначення основних завдань для розробки захищеної IT-інфраструктури;
- Аналіз базових принципів та механізмів безпеки Microsoft Active Directory;
- Ознайомлення із загальними рекомендаціями щодо захисту мережі;
- Проектування захищеної IT-інфраструктури та подальші налаштування мережі;
- Тестування впровадженої інфраструктури на предмет відповідності вимогам безпеки та ефективності.

Ключові слова: IT-ІНФРАСТРУКТУРА, ЗАХИСТ, MICROSOFT ACTIVE DIRECTORY, ПОЛІТИКИ БЕЗПЕКИ, ДОМЕННА СТРУКТУРА, ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ РЕСУРСАМИ.

					ККІКБ.КР.Б – 123 – 2 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної ІТ-інфраструктури компанії на базі рішень Microsoft Active Directory	Літ.	Арк.	Аркушів
Розроб.		Гаврилюк В.Б.		28.06				
Керівник		Фальковський І.Г.		28.06			4	93
Реценз.		Шелуха О.О.		28.06		ФІКТ, Гр. КІ-20-1		
Н. контр.		Фальковський І.Г.		28.06				
Затверд.		Єфіменко А.А.		28.06				

ANNOTATION

Bachelor's thesis on the Topic «Design of a Secure IT Infrastructure for a company Based on Microsoft Active Directory Solutions» is dedicated to the development and implementation of a secure IT infrastructure for an enterprise using Microsoft Active Directory solutions. The explanatory note consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The text part is presented on 88 pages of printed text. The explanatory note has 3 pages of appendices. The list of references includes 22 titles and occupies 2 pages. The work contains 77 figures. The total volume of the work is 93 pages.

The main goal of the final qualification work is to develop a project of a secure IT infrastructure for a company based on Microsoft Active Directory solutions, which will ensure reliable protection of information resources and effective access management.

Achieving this goal involves solving the following tasks:

- Identifying the main tasks for developing a secure IT infrastructure;
- Analyzing the basic principles and security mechanisms of Microsoft Active Directory;
- Familiarizing with general recommendations for network protection;
- Designing a secure IT infrastructure and further network configuration;
- Testing the implemented infrastructure for compliance with security requirements and efficiency.

Keywords: IT INFRASTRUCTURE, SECURITY, MICROSOFT ACTIVE DIRECTORY, SECURITY POLICIES, DOMAIN STRUCTURE, CENTRALIZED RESOURCE MANAGEMENT.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ	9
1.1 Теоретичні аспекти захисту ІТ-інфраструктури	9
1.2 Принципи побудови ІТ-інфраструктури на базі служби каталогів Active Directory	18
1.3 Можливості Active Directory для захисту мережних інфраструктур	20
1.4 Аналіз загроз для ІТ-систем з використанням Active Directory	28
Висновки до першого розділу.....	50
РОЗДІЛ 2 ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ НА БАЗІ MICROSOFT ACTIVE DIRECTORY	52
2.1 Вибір обладнання для організації роботи мережі.....	52
2.2 Розробка проєкту мережі	54
2.3 Розробка адресації мережі.....	55
2.4 Проектування служб та сервісів прикладного рівня.....	57
Висновки до другого розділу	61
РОЗДІЛ 3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОЕКТУ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ	63
3.1 Налаштування мережі	63
3.2 Встановлення і налаштування Active Directory	64
3.3 Проектування доменної структури Active Directory.....	72
3.4 Подальший розвиток	83
Висновки до третього розділу	84
ВИСНОВКИ	86
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	87
ДОДАТКИ	89

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК – Портативний комп'ютер

Wi-Fi – Wireless Fidelity

ОС – Операційна система

ПЗ – Програмне забезпечення

ERP – Enterprise Resource Planning

CRM – Customer Relationship Management

VPS –Virtual Private Server

SSL – Secure Sockets Layer

SFTP – SSH File Transfer Protocol

HTTPS – Secure Hypertext Transfer Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

DNS – Domain Name System

HTTP – Hypertext Transfer Protocol

SMTP – Simple Mail Transfer Protocol

SSH – Secure Shell

IRC – Internet Relay Chat

SNMP – Simple Network Management Protocol

ICMP – Internet Control Message Protocol

OSPF – Open Shortest Path First

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

У сучасних умовах швидкого розвитку інформаційних технологій питання забезпечення надійного захисту ІТ-інфраструктури підприємств стає дедалі актуальнішим. Зростаюча кількість кіберзагроз та вимоги до збереження конфіденційної інформації зумовлюють необхідність впровадження ефективних заходів захисту. Одним із ключових рішень у цій сфері є використання Microsoft Active Directory, яке дозволяє створювати надійні та масштабовані інфраструктури для управління доступом та забезпечення безпеки даних.

Актуальність теми. В умовах постійно зростаючих загроз для інформаційних систем підприємств, розробка та впровадження захищеної ІТ-інфраструктури є надзвичайно важливим завданням. Microsoft Active Directory є одним з провідних інструментів, який дозволяє забезпечити централізоване управління користувачами та ресурсами, а також інтеграцію з іншими захисними механізмами. Вивчення та впровадження таких рішень дозволить підвищити рівень інформаційної безпеки підприємства, зменшити ризики втрати даних та несанкціонованого доступу до них.

Основною **метою** випускної кваліфікаційної роботи є розробка проекту захищеної ІТ-інфраструктури компанії на базі рішень Microsoft Active Directory, яка забезпечить надійний захист інформаційних ресурсів та ефективне управління доступом до них.

Об'єктом дослідження є ІТ-інфраструктура компанії, яка потребує захисту від потенційних кіберзагроз та забезпечення безпеки конфіденційної інформації.

Предметом дослідження є методи та засоби захисту ІТ-інфраструктури на базі рішень Microsoft Active Directory, які дозволяють створити ефективну та надійну систему управління доступом та захисту даних.

У процесі виконання кваліфікаційної роботи було розроблено проект, який включає створення детальної архітектури захищеної ІТ-інфраструктури, визначення та реалізацію політик безпеки на базі Microsoft Active Directory. Проект дозволяє підвищити рівень захисту інформаційних ресурсів, забезпечити централізоване управління доступом та ефективно реагувати на потенційні кіберзагрози.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ

1.1 Теоретичні аспекти захисту ІТ-інфраструктури

1.1.1 Поняття ІТ-інфраструктури та її складові

ІТ-інфраструктура – це складний комплекс взаємопов’язаної обчислювальної техніки, програмних засобів, сервісів та інформаційних систем, що забезпечує стабільне функціонування, взаємодію та розвиток ІТ-інструментів компанії. Серед таких інструментів можна виділити корпоративний веб-сайт, ERP- та CRM-системи, бази даних, віддалені робочі столи співробітників, а також сервіси для забезпечення взаємодії з клієнтами та інші рішення. [3]

Сучасний бізнес не може ефективно функціонувати без цих інструментів, і, отже, побудова та підтримка ІТ-інфраструктури визначаються як одне з ключових стратегічних завдань будь-якої компанії. ІТ-інфраструктура не просто є основою для життєздатності підприємства, але також виступає стратегічним активом, який стимулює розвиток та інновації в сфері бізнесу. [4]

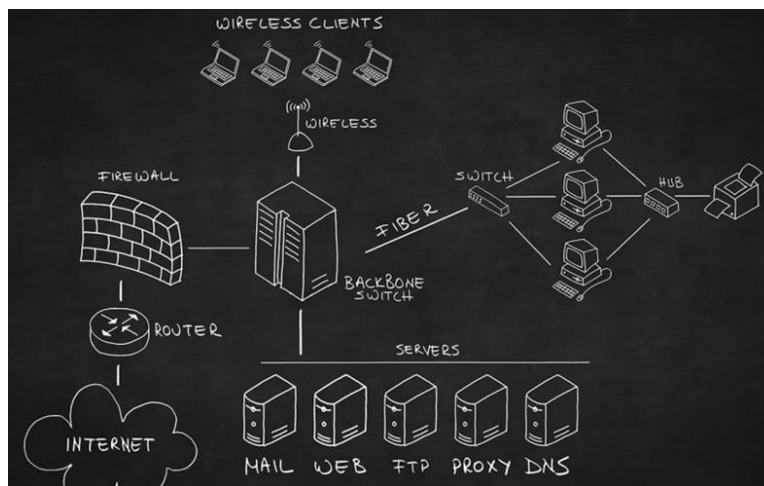


Рисунок 1.1 – Типова будова ІТ-інфраструктури

ІТ-інфраструктуру можна розділити на 3 основні частини:

1) *Апаратна частина* - визначається фізичним обладнанням, яке використовується для забезпечення роботи інформаційних систем та сервісів у підприємстві. Це включає в себе різноманітні пристрої та обладнання, які сприймають та обробляють дані, забезпечуючи фізичну базу для функціонування ІТ-систем. Основні компоненти апаратної частини включають:

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Індивідуальні комп'ютери для користувачів.
2. Сервери
3. Мережеве обладнання (маршрутизатори, комутатори, пристрої-фаєрволи)
4. Джерела безперебійного живлення
5. Системи відеоспостереження
6. Зберігання Даних:
 - Фізичні сервери або системи зберігання для даних.
 - Апаратні засоби для створення резервних копій.
7. Системи Віртуалізації: апаратне забезпечення, яке дозволяє віртуальні машини та контейнери
8. Інфраструктура Хмарних Технологій (фізичні сервери та обчислювальні потужності, які доступні через Інтернет).

2) *Програмна частина* - визначається програмним забезпеченням, що забезпечує функціонування та управління інформаційними системами та сервісами на підприємстві. Це включає в себе різноманітні програми та платформи, які реалізують різні функції та завдання. Основні компоненти програмної частини включають:

1. Операційні системи.
2. Системи Віртуалізації:
 - Гіпервізори;
 - Менеджери контейнерів.
3. Системи управління базами даних.
4. Системи безпеки:
 - Антивірусне та антишпигунське програмне забезпечення;
 - Програмні фаєрволи.
5. Корпоративне програмне забезпечення:
 - ERP-системи: для планування ресурсів підприємства;
 - CRM-системи: для управління відносинами з клієнтами; [5]
 - ПЗ для віддаленої роботи.
6. Системи моніторингу та управління ресурсами.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

7. Корпоративні додатки:

- Офісні пакети;
- Спеціалізовані додатки. (відповідно до потреб підприємства).

8. Системи ідентифікації та аутентифікації.

9. Інфраструктура хмарних технологій:

- Сервери;
- Обчислювальні ресурси; [6]
- Хмарний бекап-сервер.

10. Системи моніторингу та управління ресурсами для відстеження та оптимізації роботи обладнання.

3) *Дата-центр* - це спеціалізоване приміщення або комплекс будівель, який призначений для зберігання, обробки та управління інформацією та обчислювальним обладнанням підприємства або організації. Основна мета дата-центру полягає в наданні надійного та безпечного середовища для обслуговування ІТ-інфраструктури та забезпечення безперебійності роботи інформаційних систем.

Центр обробки даних (ЦОД) представляє собою середовище, в якому розташовується обладнання ІТ-інфраструктури. ЦОД не тільки виконує роль фізичного простору для апаратури, але й забезпечує її безперебійну роботу. Для цього необхідні спеціалізовані умови та обладнання. Компанія може організувати локальний дата-центр самостійно або орендувати місце у професійному ЦОД.

1. Системи безперебійного і гарантованого електропостачання. (резервні джерела живлення та альтернативні канали зв'язку)

2. Системи диспетчеризації та моніторинг.

3. Фізична безпека:

- Системи вогнегасіння;
- Відеоспостереження;
- Системи контролю доступу.

4. Системи охолодження та клімат-контроль.

5. Мережева інфраструктура.

6. Структурована кабельна мережа.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

7. Системи захисту даних.

1.1.2 Основні типи ІТ-інфраструктур

ІТ-інфраструктури можна класифікувати за трьома основними типами – серверні, хмарні та гібридні. Ці категорії відрізняються у принципах побудови та методах організації ресурсів. Розглянемо основні технологічні відмінності між цими видами інфраструктур:

1) Серверна ІТ-інфраструктура орієнтована на використання фізичних або віртуальних серверів, розташованих локально на підприємстві. Забезпечує внутрішню мережу, де обчислювальні ресурси централізовано обробляються.

Часто припускають, що серверна інфраструктура тотожна локальній інфраструктурі в офісі компанії, тоді як хмарна інфраструктура вважається віддаленою системою в дата-центрі провайдера. Проте важливо відзначити, що серверну інфраструктуру також можна замовити у постачальника послуг та розмістити у професійному дата-центрі, і архітектура не обов'язково визначає можливість віддаленого доступу. [7]

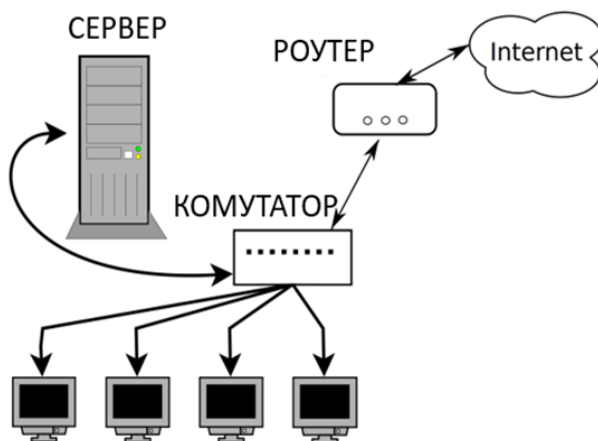


Рисунок 1.2 – Схема серверної ІТ-інфраструктури

У традиційній серверній інфраструктурі користувач працює з потужностями окремих машин, будь то фізичні чи віртуальні. Зазвичай використовують віртуальні приватні сервери) (VPS) як робочі одиниці, які є віртуальними сегментами конкретних серверів. Кожен VPS має фіксований набір параметрів, таких як процесорні ядра, обсяг оперативної пам'яті та сховище. Такі сегменти використовують для ефективного розподілу ресурсів між різними процесами.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

2) Хмарна ІТ-інфраструктура основана на використанні хмарних ресурсів, які надаються через Інтернет. Ключовим принципом хмарної інфраструктури є об'єднання серверних ресурсів в абстрактний пул, тобто в набір потужностей усіх серверів. Ресурси можуть включати віртуальні сервери, сховища даних та інші послуги, які можна масштабувати за потребою.

На базі цього набору також створюють віртуальні машини – різниця в тому, що у хмарі можна створити ВМ із ресурсів усієї системи, а не на основі конкретного сервера. Це надає можливість гнучкості та масштабованості, оскільки конфігурацію віртуальної машини можна змінювати будь-якої миті без прив'язки до конкретного обладнання.

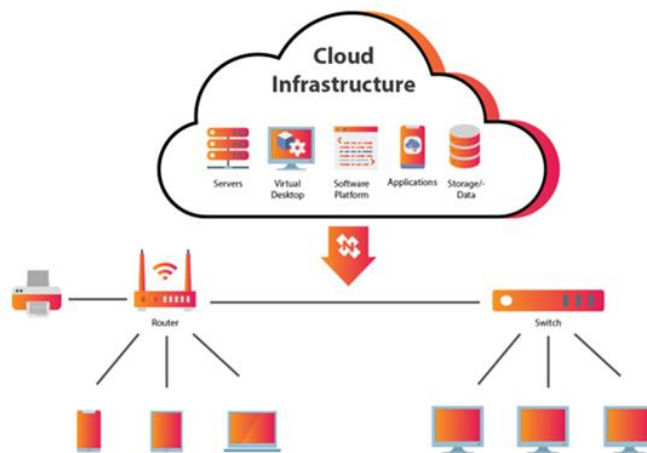


Рисунок 1.3 – Схема хмарної ІТ-інфраструктури

Важливим аспектом хмарної інфраструктури є також можливість автоматизованого управління та моніторингу ресурсів через централізовану систему. Це дозволяє ефективно розподіляти ресурси, оптимізувати роботу віртуальних машин та реагувати на зміни в навантаженні без необхідності втручання людини. Такий підхід сприяє економії часу та ресурсів, а також забезпечує надійність та швидкість обслуговування запитань користувачів чи додатків.

3) Гібридна ІТ-інфраструктура логічно поєднує елементи серверної та хмарної інфраструктур, щоб найкращим чином задовольняти потреби підприємства.

Гібридна ІТ-інфраструктура дозволяє зберігати певні дані та процеси на локальних серверах, тоді як інші елементи можуть бути розміщені у хмарних

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

сервісах. Ця система може включати в себе два типи хмар (публічний та приватний) або комбінацію хмарної та серверної інфраструктур.



Рисунок 1.4 – Схема гібридної ІТ-інфраструктури

Гібридна архітектура необхідна для того, щоб користуватись перевагами обох підходів в залежності від конкретних завдань та потреб бізнесу. Наприклад, можна розмістити процеси зі стабільним навантаженням у серверній інфраструктурі, забезпечуючи надійність та швидкість доступу. Тим часом, завдання, які вимагають гнучкості та масштабованості, можна перенести у хмарні сервіси, забезпечуючи ефективне використання ресурсів та можливість швидко реагувати на зміни в обсязі роботи. Такий гібридний підхід дає компаніям можливість оптимізувати використання ресурсів, забезпечуючи гнучкість та ефективність в різних аспектах їхньої інфраструктури.

Таким чином, серверна інфраструктура акцентується на внутрішньому обслуговуванні, хмарна інфраструктура забезпечує гнучкість та доступність через мережу Інтернет, а гібридна інфраструктура дає можливість комбінувати обидва підходи для оптимального використання ресурсів в залежності від конкретних вимог і умов.

1.1.3 Основні вразливості для безпеки ІТ-інфраструктури та способи їх усунення

В сучасному цифровому середовищі безпека ІТ-інфраструктури є пріоритетною задачею для будь-якої сучасної компанії, незалежно від її розміру, так як зловмисникам цікаві всі, включаючи середні та малі бізнеси. У порівнянні з корпораціями, менші підприємства частіше залишаються без належної уваги до стану своїх мереж і стають частішими жертвами витоків та кібератак. Важливість цього

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

питання стає очевидною, розглядаючи щоденну роботу з підтримки та моніторингу корпоративної мережі, а також наслідки подібних інцидентів. [8]

Отримання доступу до цифрових ресурсів стає необхідною передумовою для ефективної діяльності будь-якої організації, проте це водночас відкриває широкий спектр потенційних вразливостей і загроз. Серед основних загроз для ІТ-інфраструктури можна виділити наступні:

- Застаріле обладнання;
- Застаріле ПЗ та ОС;
- Незахищена корпоративна мережа;
- Соціальна інженерія;
- Відсутність систем моніторингу подій ІТ-безпеки.

1) Застаріле обладнання

Застаріле обладнання в ІТ-інфраструктурі може призводити до серйозних наслідків, зокрема, повільної роботи додатків та вразливості перед новими кіберзагрозами через відсутність оновлень. Для усунення цих проблем необхідно провести ретельний ІТ-аудит, виявити уразливості та здійснити оновлення або заміну застарілого програмного забезпечення та операційних систем. В разі потреби можливе розроблення власного програмного забезпечення, враховуючи вимоги кібербезпеки та унікальні потреби компанії. Такий комплексний підхід дозволяє підтримувати ІТ-інфраструктуру в актуальному та безпечному стані.

2) Застаріле ПЗ та ОС

Застаріле програмне забезпечення та операційні системи можуть стати причиною негативних наслідків, таких як нестабільний зв'язок, можливі перевантаження мережі, низька пропускна здатність і недостатні потужності для оновленого ПЗ і операційних систем.

Ефективним рішенням є розгляд можливостей придбання нового обладнання або використання хмарних технологій. За допомогою хмарних рішень можна ефективно розподілити навантаження, зменшити фізичний обсяг обладнання в офісі, покращити рівень захисту всієї периферії ІТ-інфраструктури та забезпечити зручний доступ до мережі незалежно від локації та пристрою. У сучасних умовах хмарні

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

технології визнані не лише трендом, але й вирішальним інструментом для успішного розвитку компаній.

3) Незахищена корпоративна мережа

Недостатня захищеність корпоративної мережі може призвести до серйозних наслідків, включаючи втрату трафіку, нелегальні вторгнення в ІТ-інфраструктуру та потенційний витік критичної інформації компанії. З метою вирішення таких ситуацій необхідно впроваджувати комплекс заходів безпеки. Важливо враховувати, що приховання лише одного слабкого місця може залишити інші аспекти без належного захисту. Таким чином, реалізація повного ланцюжка заходів включає в себе:

- Впровадження ефективних мережевих брандмауерів та інтегрованих систем виявлення вторгнень для активного моніторингу трафіку та вчасного реагування на потенційні загрози;
- Забезпечення регулярного оновлення антивірусного та антишпигунського ПЗ для ефективного виявлення та блокування шкідливих програм;
- Регулярне проведення навчань та тренінгів для персоналу з питань кібербезпеки, щоб зменшити ризик соціально-інженерних атак. Забезпечте співробітників навиченнями елементарних методів безпечної роботи, щоб підвищити рівень кібергігієни та виявлення можливих загроз;
- Застосування суворих політик доступу та багатфакторної автентифікації для управління правами користувачів і зменшення можливостей несанкціонованого доступу;
- Використання шифрування для захисту конфіденційної інформації під час передачі через мережу;
- Забезпечення безпечного периметру;
- Впровадження термінальних сервісів;

4) Соціальна інженерія

Недбалість працівників компанії, особливо в контексті соціальної інженерії, може стати серйозною загрозою для інформаційної безпеки. Наслідки недбалості

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

працівників можуть включати небезпечні ситуації, такі як витік конфіденційної інформації, невірна обробка даних, або навіть несанкціонований фізичний доступ до приміщень компанії. Профілактика таких випадків вимагає систематичного навчання персоналу щодо питань кібербезпеки, виявлення та усунення можливих слабких місць у системі безпеки, а також встановлення ефективної політики доступу та обміну інформацією.

Належна увага до навчання персоналу та ретельна робота над збереженням культури кібербезпеки в колективі допомагають запобігти виникненню ситуацій, коли недбалість працівників може стати витоком для зловмисників.

5) Відсутність систем моніторингу подій IT-безпеки

Відсутність систем моніторингу подій в області IT-безпеки може призвести до серйозних наслідків, таких як проблеми в підтримці мережі через відсутність даних про її роботу, повільна реакція або навіть відсутність реакції на нелегальні проникнення в IT-інфраструктуру та повільне відновлення після збоїв.

Для вирішення цих проблем рекомендується впровадження професійної системи моніторингу, що базується на продуктах, таких як Zabbix, Microsoft System Center Operations Manager і Dell Foglight. Використання подібних систем дозволить підтримувати IT-інфраструктуру під постійним наглядом, значно зменшуючи час реакції на потенційні атаки та інші незаконні дії в мережі.

Також, завдяки цим системам, компанія матиме можливість аналізувати навантаження та визначати тенденції в розвитку. З урахуванням зростаючої кількості кібератак, моніторинг стає необхідною складовою стабільної та безпечної IT-інфраструктури вашої компанії, сприяючи швидкому виявленню зловмисника та вживанню відповідних заходів.

Усі розглянуті пункти, а саме застарілі, не захищені або відсутні елементи в IT-інфраструктурі, неналежне навчання персоналу та недостатній моніторинг усіх елементів системи представляють серйозну загрозу для функціонування підприємства. Можливі неполадки та незаконне вторгнення стають результатом недбалості у підтримці та забезпеченні безпеки інформаційних систем. Ці негаразди можуть призвести до серйозних наслідків, таких як втрати конфіденційної

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

інформації, переривання бізнес-процесів, а також витрат на відновлення та усунення наслідків кібератак.

В умовах постійно зростаючих загроз, підтримка та модернізація ІТ-інфраструктури є необхідними етапами для забезпечення стійкості та надійності бізнес-процесів. Ретельний моніторинг, регулярні аудити безпеки та

впровадження сучасних технологій є важливими компонентами стратегії захисту, а заходи, спрямовані на усунення слабких місць та вдосконалення ІТ-інфраструктури, є ключовим елементом забезпечення стабільності та відповідальності перед сучасними викликами кіберпростору.

1.2 Принципи побудови ІТ-інфраструктури на базі служби каталогів Active Directory

Active Directory (AD) – це служба каталогів, розроблена компанією Microsoft, яка використовується для управління мережними ресурсами. Вона дозволяє адміністраторам використовувати групові політики (GPO) для налаштування робочого середовища користувачів, розгортання програмного забезпечення, встановлення оновлень на всіх комп'ютерах у мережі та зберігання даних і налаштувань середовища в централізованій базі даних. Мережі AD можуть мати різний розмір - від кількох сотень до мільйонів об'єктів.

Служба каталогів Active Directory є центральним компонентом ІТ-інфраструктури будь-якої організації, забезпечуючи централізоване управління користувачами, комп'ютерами та іншими ресурсами, а також базову безпеку для мережі.
[9]

Active Directory використовує ієрархічну структуру для організації об'єктів у мережі на трьох основних рівнях: об'єкти, групи та контейнери. Об'єкти організовані в контейнери, так звані організаційними одиницями (OU), які об'єднуються в домени, дерева та ліси.

Організаційні одиниці (OU) – це контейнери, що дозволяють групувати об'єкти всередині домену для полегшення адміністративних завдань. Вони можуть бути вкладеними, що дозволяє створювати ієрархії управління.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Групи – об'єкти, які об'єднують користувачів і комп'ютери для полегшення управління дозволами та ресурсами. Групи можуть бути двох типів: групи безпеки (security groups) та групи розсилки (distribution groups).

Домен – це логічна частина мережі, яка містить певні об'єкти і має унікальне ім'я та безпековий контекст. Наприклад, contoso.com.

Дерево – група доменів, об'єднаних в ієрархічну структуру з одним батьківським і кількома дочірніми доменами. Якщо у вас є домени sales.contoso.com і marketing.contoso.com, то вони можуть утворювати дерево. [10]

Ліс – колекція дерев, які взаємодіють та спільно використовують глобальний каталог та ідентифікаційні дані. Якщо у вас є дерево з доменами contoso.com і adatum.com, то вони можуть утворювати ліс.

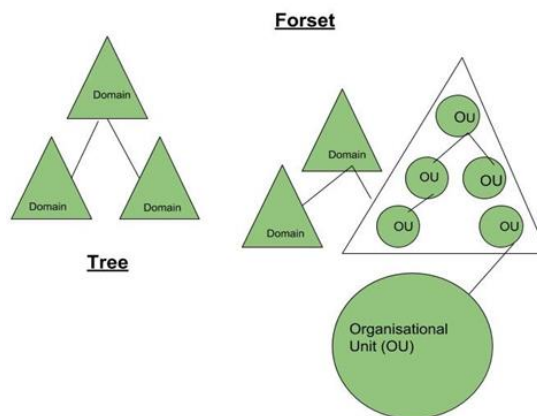


Рисунок 1.5 Організація об'єктів в Active Directory

Кожен Active Directory має принаймні один ліс. Організації можуть мати два або більше лісів Active Directory, або вони можуть отримати кілька лісів через угоди злиття та поглинання.

Один ліс є найбільш економічно ефективним варіантом, перш за все тому, що він вимагає найменших адміністративних витрат. Також забезпечує максимальну співпрацю між користувачами, оскільки всі об'єкти в лісі перераховані в єдиному глобальному каталозі.

Кілька лісів можуть бути потрібними або навіть необхідними, залежно від вимог ізоляції та автономності даних для груп у вашій організації. Однак наявність кількох лісів сама по собі не підвищує безпеку; потрібно правильно керувати та охороняти кожен ліс. Тому варто збалансувати витрати на наявність кількох лісів.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Зокрема, найкращі практики вимагають окремих груп управління ІТ для кожного лісу, щоб забезпечити належний розподіл обов'язків.

Як правило, лише найбільші та найскладніші організації мають кілька лісів Active Directory. Більшість організацій створюють єдиний ліс із кількома дочірніми доменами, кожен із яких має власну базу даних Active Directory із власними ресурсами, дозволами, об'єктами групової політики (GPO) тощо.

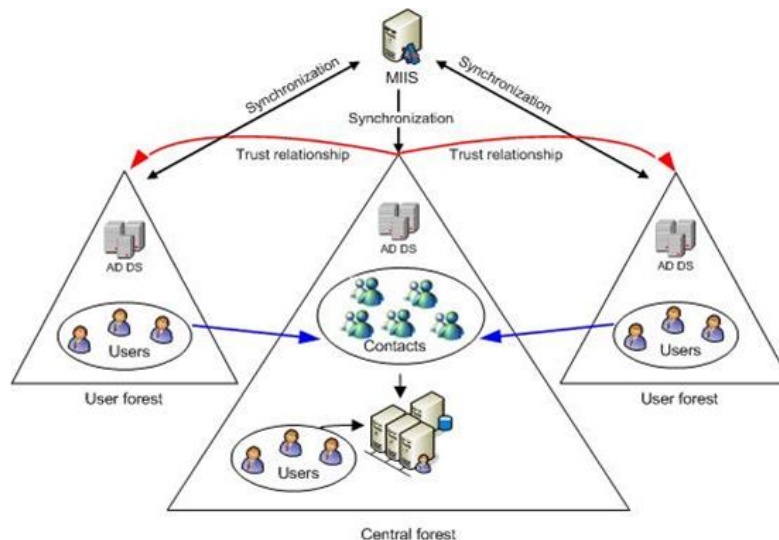


Рисунок 1.6. Приклад організації з кількома лісами

Переваги використання Active Directory:

- Централізоване управління – дозволяє адміністратору централізовано керувати всіма користувачами, комп'ютерами та іншими об'єктами.
- Безпека – забезпечує розширені можливості автентифікації та авторизації, захищаючи ресурси мережі від несанкціонованого доступу.
- Масштабованість – може використовуватися в мережах будь-якого розміру, від невеликих компаній до великих корпорацій з тисячами користувачів.
- Гнучкість – підтримує різні топології мережі та дозволяє організаціям адаптувати структуру AD до своїх потреб.

1.3 Можливості Active Directory для захисту мережних інфраструктур

Безпека Active Directory (AD) стосується заходів і методів кібербезпеки, які впроваджуються для захисту інфраструктури Microsoft Active Directory мережі. Ця

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

служба, розроблена корпорацією Майкрософт, спрощує керування та організацію інформації про користувачів, комп'ютери та інші ресурси в мережі.

Захищеність AD є ключовою для автентифікації, авторизації та загального захисту середовища Windows. Вона має життєво важливе значення для запобігання витоку даних, несанкціонованого доступу, підтримки безвідмовної роботи системи тощо. [11]

Критичні аспекти безпеки Active Directory включають:

- Захист облікових записів адміністратора;
- Резервне копіювання та відновлення;
- Аудит та моніторинг;
- Управління доступом та дозволами;
- Безпечний зв'язок;
- Захист від атак на аутентифікацію;
- Оновлення та патчі;
- Політики безпеки;
- Розділення обов'язків;
- Захист від внутрішніх загроз;
- Брандмауер і сегментація мережі.

Захист облікових записів адміністратора

Облікові записи адміністратора є критичними для безпеки Active Directory, оскільки вони мають широкий спектр повноважень. Необхідно використовувати унікальні і складні паролі для цих облікових записів, щоб ускладнити їх компрометацію. Крім того, слід обмежити кількість облікових записів з адміністративними правами, надаючи їх лише тим користувачам, які дійсно потребують цього для виконання своїх обов'язків. Використання багатофакторної аутентифікації (MFA) забезпечує додатковий рівень захисту, унеможливлюючи доступ до облікових записів лише за допомогою пароля. [12]

Резервне копіювання та відновлення

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Регулярне резервне копіювання бази даних Active Directory є надзвичайно важливим для забезпечення безперервності роботи підприємства. У разі збою системи або атаки, резервні копії дозволять швидко відновити роботу. Тестування процесу відновлення повинно проводитися регулярно, щоб гарантувати, що відновлення може бути виконане ефективно і без втрат даних. Реалізація надійних механізмів резервного копіювання та відновлення забезпечує доступність і цілісність даних у разі втрати, пошкодження або інциденту безпеки. [12]

Аудит та моніторинг

Для забезпечення безпеки Active Directory важливо налаштувати журнали подій, які будуть відстежувати зміни і доступ до системи. Використання інструментів для моніторингу в режимі реального часу та аналізу журналів дозволяє виявляти підозрілі дії та реагувати на потенційні загрози негайно. Це допомагає запобігати несанкціонованому доступу та швидко виявляти спроби компрометації системи. [12]

Управління доступом та дозволами

Використання принципу найменших привілеїв є ключовим аспектом управління доступом у Active Directory. Це означає, що користувачі повинні мати лише ті права, які необхідні для виконання їхніх завдань. Регулярний огляд і оновлення дозволів допомагає підтримувати безпеку системи, знижуючи ризик несанкціонованого доступу або зловживання правами. [12]

Захист контролерів домену

Контролери домену є основними компонентами Active Directory, тому їх захист є надзвичайно важливим. Фізичний захист серверів, на яких працюють контролери домену, є першочерговим завданням. Використання сучасного антивірусного програмного забезпечення та регулярне оновлення системи допомагає запобігти шкідливим атакам та забезпечити стабільну роботу контролерів. [12]

Безпечний зв'язок

Налаштування безпечних каналів зв'язку між компонентами Active Directory є важливим для захисту від підслуховування та атак типу «людина посередині». Це

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

часто передбачає використання таких протоколів, як Kerberos, і впровадження механізмів шифрування. Забезпечення безпечного зв'язку гарантує, що дані передаються захищено і не можуть бути перехоплені зловмисниками. [12]

Захист від атак на аутентифікацію

Сучасні протоколи аутентифікації, такі як Kerberos, забезпечують більш високий рівень безпеки порівняно з застарілими методами. Важливо захищати систему від атак типу "Pass-the-Hash" і "Pass-the-Ticket", які можуть дозволити зловмисникам отримати доступ до облікових записів без знання паролів. Використання додаткових механізмів захисту, таких як білі списки IP-адрес та моніторинг аномальної активності, допомагає запобігти цим загрозам. [12]

Оновлення та патчі

Регулярне оновлення операційної системи та програмного забезпечення є важливим для усунення відомих вразливостей і забезпечення безпеки Active Directory. Впровадження критичних патчів своєчасно знижує ризик експлуатації вразливостей зловмисниками, що може призвести до компрометації системи. [12]

Політики безпеки

Налаштування політик груп (Group Policy) дозволяє централізовано керувати налаштуваннями безпеки кінцевих точок і забезпечити відповідність стандартам безпеки. Використання політик для керування паролями, блокуванням облікових записів та іншими аспектами безпеки допомагає знизити ризики, пов'язані з людським фактором і зловмисними діями. [12]

Розділення обов'язків

Поділ адміністративних обов'язків між різними адміністраторами є важливим для зменшення ризику зловживання правами. Це забезпечує додатковий рівень контролю та запобігає концентрації повноважень в одних руках, що може бути небезпечним у випадку компрометації одного з облікових записів. [12]

Захист від внутрішніх загроз

Впровадження механізмів контролю доступу до конфіденційних даних і проведення регулярних перевірок безпеки та аудитів допомагають виявляти потен-

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

ційні внутрішні загрози. Це дозволяє своєчасно реагувати на підозрілі дії та запобігати витоку конфіденційної інформації, що може мати критичні наслідки для організації. [12]

Брандмауер і сегментація мережі

Використання брандмауерів та сегментація мережі допомагає контролювати трафік між різними частинами мережі та обмежити поверхню атаки. Це дозволяє ізолювати критичні компоненти системи від потенційно небезпечних зон і знижує ризик розповсюдження атак по всій мережі. Сегментація мережі та налаштування правил брандмауера забезпечують додатковий рівень захисту для Active Directory. [12]

1.3.1 Множинний фактор аутентифікації (MFA)

Автентифікація - це процес перевірки особистості користувача або пристрою, щоб надати їм доступ до мережі, ресурсів або даних. Це перший крок до забезпечення безпеки, який гарантує, що лише авторизовані особи мають доступ до потрібної їм інформації.

Множинний фактор аутентифікації (MFA) є важливим елементом стратегії безпеки в сучасному інформаційному середовищі. Особливо актуальним стає використання MFA при взаємодії з Active Directory та іншими службами, де зберігається значна кількість конфіденційної інформації.

MFA базується на ідеї використання не одного, а кількох факторів для підтвердження ідентичності користувача. Зазвичай це щось, що користувач знає (наприклад, пароль) і щось, що він має (такий як токен або мобільний пристрій). Це значно ускладнює завдання неправомірних осіб, які намагаються незаконно отримати доступ до системи.

Використання MFA в Active Directory дозволяє додатково захистити облікові записи користувачів від несанкціонованого доступу. Комбінація пароля та, наприклад, одноразового коду з мобільного додатку стає бар'єром для хакерів. Навіть якщо пароль виявиться скомпрометованим, вторгнення буде унеможливлене без додаткового фактора аутентифікації.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Підвищення рівня безпеки не тільки запобігає неправомірному доступу, але й допомагає відвернути наслідки можливих атак, що можуть призвести до втрати чутливої інформації або порушення конфіденційності. У світі, де кіберзагрози стають все більш вишуканими, використання MFA стає необхідністю для забезпечення надійного захисту інформаційних ресурсів.

Основними перевагами MFA є:

- Підвищений рівень безпеки: Введення додаткових факторів робить важчими атаки на автентифікацію, такі як перехоплення паролів.
- Захист від втрати або компрометації паролів: Якщо пароль стає відомим третій стороні, MFA надає додатковий шар захисту, оскільки зломисник все одно не може отримати доступ без інших факторів.
- Зменшення ризику викрадення облікових даних: Якщо зломисник отримав доступ до пароля, йому все одно потрібно пройти інші етапи автентифікації.
- Використання різних видів факторів: Комбінація різних видів факторів (наприклад, щось, що знаєте, і щось, що маєте) робить MFA більш надійним.
- Відповідність нормативам безпеки: У багатьох випадках MFA вимагається або рекомендується нормативами безпеки для забезпечення високого рівня захисту інформації.

1.3.2 Групові політики в Active Directory

Групові політики (Group Policies, GPO) в Active Directory – це потужний інструмент для централізованого управління конфігурацією корпоративних комп'ютерів у мережі Windows. Вони дозволяють адміністраторам визначати та контролювати різні параметри та поведінку систем усіх комп'ютерів та користувачів в домені Active Directory. Групові політики, у свою чергу, складається з набору політик, які називаються об'єктами групової політики (GPO). [13]

При створенні домену AD автоматично створюються два об'єкти групової політики:

- Політика домену за замовчуванням встановлює базові параметри для всіх користувачів та комп'ютерів у домені в трьох площинах:

1) політика паролів,

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

2) політика блокування облікових записів

3) політика Kerberos.

– Політика контролерів домену за промовчанням встановлює базові параметри безпеки та аудиту для всіх контролерів домену в межах домену.

Для набрання чинності об'єкт групової політики необхідно застосувати (пов'язати) з одним або декількома контейнерами Active Directory: сайт, домен або підрозділ (OU). Наприклад, можна використовувати групову політику, щоб вимагати від усіх користувачів певного домену використовувати складніші паролі або заборонити використання знімних носіїв на всіх комп'ютерах тільки у фінансовому підрозділі даного домену.

Об'єкт групової політики не діє, доки не буде пов'язаний з контейнером Active Directory, наприклад сайтом, доменом або підрозділом. Будь-який об'єкт групової політики може бути пов'язаний з кількома контейнерами, і, навпаки, з конкретним контейнером може бути пов'язано кілька об'єктів групової політики. Крім того, контейнери успадковують об'єкти групової політики, наприклад, об'єкт групової політики, пов'язаний з підрозділом, застосовується до всіх користувачів та комп'ютерів у його дочірніх підрозділах. Аналогічно, об'єкт групової політики, який застосовується до OU, застосовується не тільки до всіх користувачів та комп'ютерів у цьому OU, але й успадковується всім користувачам та комп'ютерам у дочірніх OU.

Налаштування різних об'єктів групової політики можуть перекриватись або конфліктувати. За замовчуванням об'єкти групової політики обробляються у такому порядку (причому створені пізніше мають пріоритет над створеними раніше):

- Локальний (персональний комп'ютер);
- Сайт;
- Домен;
- Організаційна одиниця.

У цю послідовність можна втручатися, виконавши будь-яку з наступних дій:

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

– Зміна послідовності GPO. Об'єкт групової політики, створений пізніше, обробляється останнім і має найвищий пріоритет, перезаписуючи налаштування в створених раніше об'єктах. Це працює у разі виникнення конфліктів.

– Блокування успадкування. Дочірні об'єкти успадковують усі об'єкти групової політики від батьківського, але ви можете заблокувати це спадкування.

– Примусове ігнорування зв'язку GPO. Параметри батьківських політик перезаписуються будь-якими конфліктуючими політиками дочірніх об'єктів. Ви можете перевизначити цю поведінку.

– Вимкнення зв'язків GPO. Обробка включена для всіх зв'язків GPO. Ви можете запобігти застосуванню групи групової політики для конкретного контейнера, відключивши зв'язок з об'єктом групової політики цього контейнера.

1.3.3 Резервне копіювання та відновлення в Active Directory

Резервне копіювання та відновлення, грають важливу роль у забезпеченні надійності та доступності даних в Active Directory. Для забезпечення цих функцій в AD використовуються інструменти резервного копіювання, такі як Windows Server Backup або інші сторонні рішення. Ці інструменти дозволяють адміністраторам регулярно створювати резервні копії бази даних AD і відновлювати їх у випадку втрати даних або несправності системи.

Доменні служби Active Directory включають механізми резервного копіювання, які забезпечують консистентність та відновлення даних каталогу. Під час резервного копіювання весь каталог AD, включаючи об'єкти, атрибути та конфігураційні дані, може бути включений до резервної копії.

Ці резервні копії можуть бути використані для відновлення даних після випадкового видалення об'єктів, помилкових змін або в разі відмови обладнання. Адміністратори можуть планувати регулярні резервні копії, щоб забезпечити актуальність та надійність даних.

Після створення резервної копії, відновлення може бути виконано в разі потреби. Це може включати відновлення всього каталогу, окремих об'єктів або навіть окремих атрибутів. Забезпечення безпеки та можливості відновлення є ключовими

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

аспектами управління AD, оскільки ця служба є критично важливою для функціонування багатьох організаційних мереж. [14]

1.4 Аналіз загроз для ІТ-систем з використанням Active Directory

1.4.1 Типові протоколи побудови мережних інфраструктур

Побудова мережної інфраструктури включає в себе використання різних протоколів та технологій для забезпечення ефективного та безпечного обміну інформацією між різними пристроями в мережі. Загалом протоколи для мережі можна розбити на такі категорії:

- Протоколи мережевого зв'язку;
- Протоколи керування мережею;
- Протоколи безпеки мережі.

1) Протоколи мережевого зв'язку

Протоколи зв'язку є важливим елементом для функціонування мережі, адже без них комп'ютерні мережі не можуть існувати. Ці протоколи формалізують формати та правила, які визначають передачу даних в мережі. Це необхідна умова для обміну повідомленнями між обчислювальними системами та в телекомунікаціях, охоплюючи як апаратне, так і програмне забезпечення. Комунікаційні протоколи також відповідають за автентифікацію та виявлення помилок, а також за синтаксис, синхронізацію та семантику, обов'язкові для ефективної роботи як аналогових, так і цифрових комунікацій.

TCP/IP – цей протокольний набір є фундаментом Інтернету та багатьох корпоративних мереж. Він визначає правила для передачі даних між пристроями в мережі, забезпечуючи надійність інтеракцій, а саме TCP керує передачею,

розділяє дані на пакети, якими можна спільно користуватися в мережі. Потім ці пакети можуть бути надіслані такими пристроями, як комутатори та маршрутизатори, до визначених цілей, а IP розділяє та розбиває дані на менші пакети для полегшення маршрутизації. Замість того, щоб надсилатися на пристрої, цей протокол використовується Інтернетом для маршрутизації та адресації цих даних у мережах, щоб вони надходили до потрібного пункту призначення. Основною атакою,

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

яка робиться на основі цих протоколів це ARP Spoofing (ARP Poisoning), у якій зловмисник відправляє невірні ARP-відповіді, що призводить до того, що обманюється адреса мережевої карти іншого пристрою та можливість отримати несанкціонований доступ до передачі даних, перехоплення та зміна пакетів.

DNS – використовується для перетворення доменних імен в IP-адреси та забезпечення ідентифікації ресурсів в мережі. Це необхідно для спрощення людського взаємодії з комп'ютерами, оскільки доменні імена легше запам'ятовуються, ніж числові IP-адреси. Для даного протоколу є небезпечною атака DNS Spoofing, під час виконання якої зловмисник впроваджує неправдиві DNS-відповіді, щоб перенаправити трафік на фальшивий сервер і здійснити атаки типу "Man-in-the-Middle" та викрадення інформації.

HTTP – протокол використовуються для передачі гіпертекстових даних, таких як веб-сторінки, між веб-серверами та клієнтами. Протокол є не дуже безпечним, так як усі дані зберігаються у відкритому вигляді, їх можна дуже легко скомпрометувати та використати у власних цілях.

SMTP – є протоколом для відправлення та прийому електронних листів. Він визначає правила для обміну повідомленнями між різними електронними поштовими серверами.

FTP – використовується для передачі файлів між пристроями в мережі. Цей протокол дозволяє користувачам завантажувати та завантажувати файли з серверів.

SSH – це протокол безпеки, що використовується для безпечного з'єднання та взаємодії з віддаленими пристроями. Він забезпечує захищену передачу даних через ненадійні мережі та дозволяє користувачам безпечно отримувати доступ до пристроїв навіть через незахищену мережу.

IRC – це текстовий протокол зв'язку. Програмні клієнти використовуються для зв'язку з серверами та надсилання повідомлень іншим клієнтам. Цей протокол добре працює в мережах з великою кількістю розподілених машин.

2) Протоколи керування мережею

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Протоколи управління мережею грають ключову роль у забезпеченні ефективності та надійності комп'ютерних мереж, так як вони дозволяють адміністраторам визначати параметри моніторингу, контролю та налагодження, що сприяє підтримці стабільного функціонування мережі. Одні з основних завдань протоколів управління включають в себе виявлення та виправлення неполадок, що можуть виникнути в процесі обміну даними між різними пристроями. Це може включати в себе виявлення втрати пакетів, аналіз стану доступності хостів та ідентифікацію ефективності з'єднань.

Політики, які реалізуються за допомогою цих протоколів, можуть бути широким спектром: від управління пропускнуою здатністю до встановлення правил безпеки та керування ресурсами. Такий підхід дозволяє створювати індивідуальні налаштування для різних типів пристроїв у мережі, забезпечуючи оптимальні умови для їхньої роботи.

Серед основних протоколів, що використовуються сучасними мережевими адміністраторами для забезпечення стабільності, ефективності та безпеки мережевого середовища управління можна виділити:

SNMP – є простим протоколом на основі TCP для моніторингу та управління різноманітними пристроями у мережі, що покладається на використання агентів для збору та надсилання даних загальному менеджеру SMNP, який, у свою чергу, запитує агентів і отримує їхні відповіді. Він дозволяє дозволяє адміністраторам переглядати та змінювати інформацію про кінцеву точку, щоб змінити поведінку пристроїв у мережі, дізнаватись про стан пристроїв, виявляти неполадки та вчасно реагувати на події в мережі, віддалено контролювати та налаштовувати роботу різних пристроїв, що спрощує

управління мережею. Основною загрозою є атака SNMP Community String Guessing, під час якої зловмисник намагається вгадати "community string" для доступу до управління мережею, що може призвести до несанкціонованого доступу до інформації або зміни конфігурації пристроїв.

ICMP – протокол керуючих повідомлень Інтернету (ICMP), використовується для діагностики стану мережі та виявлення проблем під час передачі даних.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

Керовані пристрої у мережі можуть використовувати цей протокол для відсилання повідомлень про помилки, що надає інформацію про проблеми підключення між пристроями.

3) Протоколи безпеки мережі

Протоколи безпеки мережі забезпечують надійність та конфіденційність передачі даних через мережеві підключення. Ці протоколи визначають методи захисту даних від незаконного перегляду чи видалення, забезпечуючи, що лише авторизовані користувачі, служби або пристрої матимуть доступ до мережевої інформації. Ця захист діє у всіх типах даних та в різних мережевих середовищах. На протоколи безпеки зазвичай виконуються атаки відмови в обслуговуванні DDoS чи Man-in-the-Middle (MITM).

Зазвичай протоколи безпеки мережі використовують шифрування для захисту даних, і лише за допомогою спеціальних алгоритмів, формул і логічних ключів можливий доступ до цих даних. Найпопулярніші безпекові протоколи включають в себе:

SSL – є протоколом безпеки мережі, який в основному використовується для створення захищених з'єднань у Інтернеті та забезпечення безпеки конфіденційних даних. Цей протокол забезпечує можливість здійснення захищеного зв'язку як між сервером і клієнтом, так і між серверами. Дані, які передаються за допомогою *SSL*, шифруються для унеможливлення їх читання неправомірними особами.

SFTP – протокол безпечної передачі файлів) - є механізмом для захищеної передачі файлів через мережу. За допомогою *SFTP* дані шифруються, і взаємна аутентифікація клієнта і сервера забезпечує безпечний обмін інформацією.

HTTPS – представляє собою безпечну і зашифровану версію *HTTP*. Цей протокол забезпечує безпеку передачі даних між браузером і сервером. Дані шифруються для гарантії конфіденційності та захисту інформації. [17]

1.4.2 Вразливості та потенційні ризики використання Active Directory

Active Directory (AD) є службою каталогів та службою управління доступом в операційних системах Windows.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Хоча Active Directory є потужним і корисним інструментом для управління мережею та ресурсами, він також може стати об'єктом атак та вразливостей.

Кібератаки на Active Directory (AD) можуть набувати різноманітних форм, таких як атаки на паролі, підвищення привілеїв і моніторинг мережевого трафіку. Зловмисники часто використовують методи соціальної інженерії, наприклад фішинг, для отримання доступу до облікових даних AD, які потім вони можуть використовувати для проникнення в мережу та отримання доступу до конфіденційних ресурсів. Після успішного вторгнення зловмисники можуть виконувати команди, встановлювати шкідливе програмне забезпечення та виконувати інші зловмисні дії, зазвичай з метою викрадання конфіденційних даних або порушення бізнес-операцій. Розглянемо основні категорії кібератак на Active Directory, які часто здійснюються зловмисниками.

«Розпилення» пароля (Password Spraying) представляє собою один з найбільш поширених видів атак на Active Directory. Атакуючий намагається здійснити вхід в AD, використовуючи перелік часто вживаних паролів, з надією отримати доступ до одного чи кількох облікових записів. Для цього він може використовувати автоматизовані засоби для перевірки великої кількості паролів зі списком імен користувачів. Якщо атака вдається і атакуючий отримує доступ до облікового запису, зловмисники можуть потенційно викрасти конфіденційну інформацію або встановити шкідливе програмне забезпечення на скомпрометованій машині. Для запобігання атакам з «розпилювання» паролів, організації повинні сприяти використанню надійних паролів та впроваджувати політику блокування облікових записів, що мінімізує ризик атак методом перебору. Крім того, використання багатофакторної аутентифікації може ускладнити спроби зловмисників отримати доступ до облікових записів, навіть якщо вони володіють правильним паролем.

Іншим видом атаки на Active Directory є "передача хешу" (Pass-the-Hash). У цьому виді атаки зловмисник викрадає хеш пароля облікового запису AD і використовує його для автентифікації користувача, не знаючи реального пароля. Цю атаку можна здійснити шляхом перехоплення мережевого трафіку, отримання доступу до

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

скомпрометованої машини або використання шкідливого програмного забезпечення. Після отримання доступу до облікового запису, зловмисник може видачі себе за законного користувача та отримати доступ до конфіденційних ресурсів. Щоб уникнути атак передачі хешу, організації повинні використовувати надійні алгоритми шифрування для захисту хешів паролів, такі як шифрування Kerberos. Крім того, вони повинні впроваджувати ізоляцію домену для запобігання доступу зловмисників до інших машин у мережі після того, як вони скомпрометували одну машину.

DNS-спуфінг, або перехоплення DNS, представляє собою вид атаки, при якій зловмисник перенаправляє запити DNS на підроблений сервер, забезпечуючи можливість перехоплення трафіку та, в кінцевому підсумку, отримання несанкціонованого доступу до конфіденційної інформації. В контексті Active Directory, подібне фальсифікування DNS може використовуватися для перенаправлення запитів автентифікації на підроблений сервер, що дає зловмиснику можливість перехоплення облікових даних для отримання доступу. Для запобігання атакам DNS-спуфінгу рекомендується впроваджувати безпечні протоколи DNS, такі як DNSSEC, і систематично перевіряти журнали DNS на виявлення будь-якої підозрілої активності.

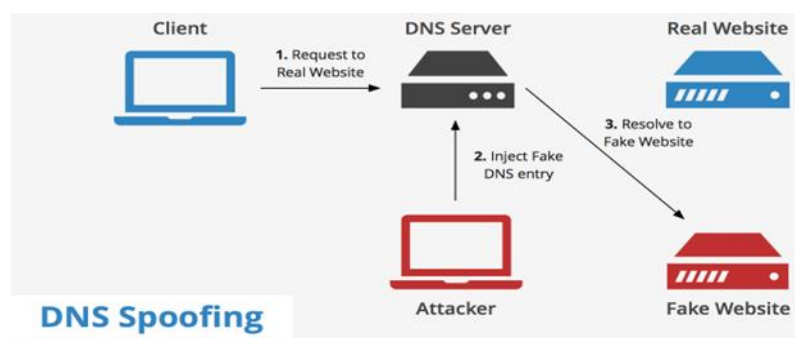


Рисунок 1.7 Приклад атаки DNS-спуфінг

Атаки на об'єкти групової політики (GPO). GPO є важливим елементом Active Directory, використовуваним для управління параметрами користувачів і комп'ютерів. Зловмисники можуть використовувати вразливості в GPO для отримання підвищених привілеїв або встановлення шкідливого програмного забезпечення на цільових комп'ютерах. Наприклад, зловмисник може змінити GPO для встановлення бекдору на всіх машинах у домені. Для уникнення атак на GPO організаціям слід регулярно переглядати налаштування своїх GPO та переконатися,

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

що вони відповідають останнім рекомендаціям з безпеки від Microsoft. Також важливо обмежувати доступ до інструментів управління GPO лише довіреним адміністраторам і використовувати інструменти аудиту для моніторингу змін в GPO.

1.4.3 Мережеві атаки на IT-інфраструктури

Мережеві атаки на IT-інфраструктури представляють собою небажані та шкідливі дії, спрямовані на завдання шкоди, отримання несанкціонованого доступу або втручання в роботу комп'ютерних систем і мереж. Ці атаки можуть бути спрямовані на різноманітні цілі, включаючи корпоративні мережі, державні системи, особисті комп'ютери та інші IT-інфраструктури. Існує безліч методів та типів мережевих атак, деякі з них включають:

- Атака на відмову в обслуговуванні;
- Фішинг;
- Людина-посередині (Man-in-the-Middle);
- Сканування портів та вразливостей;
- Zero-Day атаки;
- Шкідливе програмне забезпечення та віруси;
- Внутрішні мережеві атаки.

Атака на відмову в обслуговуванні

1) DoS-атака:

У цьому випадку атакувальник намагає переповнити ресурси цільової системи, зробивши її недоступною для легітимних користувачів. Це може бути досягнуто різними способами, такими як переповнення мережевого каналу, використання великої кількості запитів чи надмірне використання обчислювальних ресурсів.

Наприклад, атака на веб-сайт може включати відправлення великої кількості запитів на сервер, перевантажуючи його та роблячи його недоступним для інших користувачів.

2) DDoS-атака:

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

DDoS-атака є розширеною формою DoS, де атакується використовуються не один, а багато пристроїв (часто називають ботнетом) для координації атак на цільовий об'єкт. Це дозволяє атакувальникові перевантажити мережеві ресурси значно ефективніше.

Атака може бути організована так, щоб тисячі комп'ютерів, заражених шкідливим програмним забезпеченням, одночасно відправляли запити на сервер цільового веб-сайту. Це призводить до перевантаження сервера та зниження його продуктивності або навіть до відмови в обслуговуванні. [15]

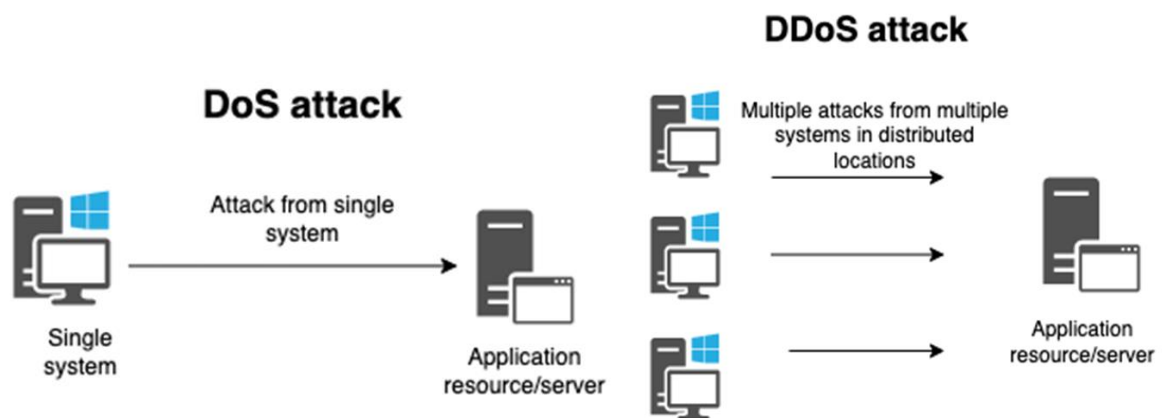


Рисунок 1.8 – Приклад: а – DoS-атаки; б – DDoS-атаки

Фішинг

Фішинг - це метод соціальної інженерії, який використовується зловмисниками для отримання конфіденційної інформації, такої як логіни, паролі, номери кредитних карт, а також інші особисті дані. Цей вид атаки зазвичай використовує обманливі та імітаційні методи з метою виглядати дійсними для потенційних жертв. Детальніші відомості про фішинг:

1) Електронна пошта:

Зловмисники надсилають легітимно виглядаючі електронні листи, які імітують важливі повідомлення від відомих організацій, таких як банки, платіжні системи, соціальні мережі чи урядові установи. Листи можуть містити посилання на фальшиві веб-сайти або прикладеним файлам із шкідливим програмним забезпеченням. Наприклад, фішер може надіслати листа, який виглядає як повідомлення від вашого банку чи іншої установи, з проханням оновити або перевірити ваші облікові дані, надавши посилання на фальшивий веб-сайт.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

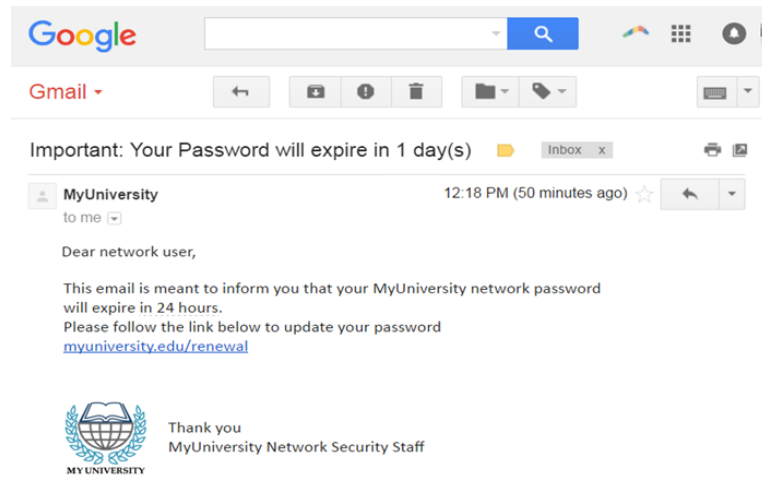


Рисунок 1.9 – Приклад фішингової атаки через електронну пошту

2) Сайт-імітація:

Зловмисники створюють фальшиві веб-сайти, які імітують легітимні ресурси, щоб отримати доступ до логінів та паролів користувачів.

Наприклад, фішер може створити імітацію веб-сайту банку та перенаправити жертву на цей сайт через фішингове повідомлення, яке виглядає як лист від банку.

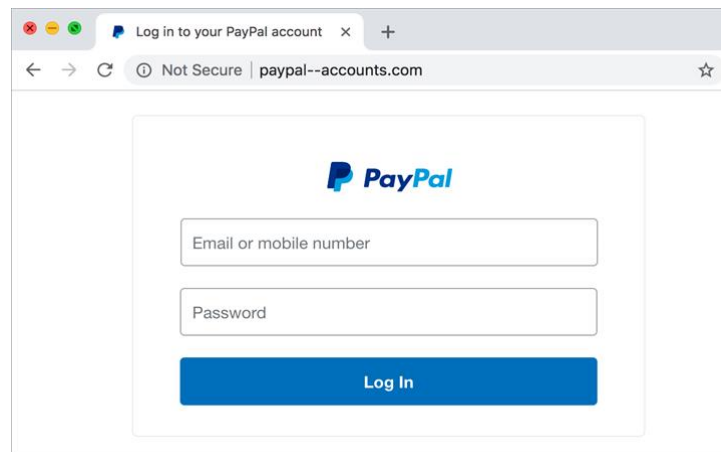


Рисунок 1.10 – Приклад фішингової атаки через сайт-імітацію

3) Соціальні мережі:

Зловмисники можуть використовувати соціальні мережі для створення фальшивих профілів чи використання фішингових повідомлень через особисті повідомлення для збору інформації або введення у користувачів у фальшиві операції.

Наприклад, атаки через соціальні мережі можуть включати фішингові посилання або фальшиві розіграші для вибору логінів і паролів.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

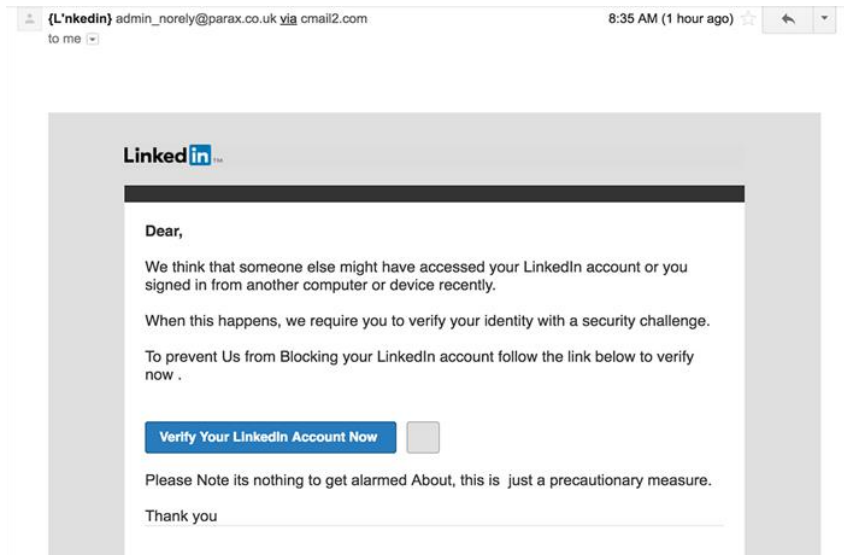


Рисунок 1.11 – Приклад фішингової атаки через соціальні мережі

4) Телефонний фішинг (вішінг):

Зловмисники використовують телефонні дзвінки для обману людей та отримання конфіденційної інформації.

Наприклад, зловмисник може виглядати як представник банку чи іншої організації, яка повідомляє користувача про проблеми з його обліковим записом і просить надати конфіденційну інформацію.

Людина-посередині (Man-in-the-Middle)

Людина посередині (Man-in-the-Middle або MITM) - це атака, при якій зловмисник розташовується між двома комунікуючими сторонами та перехоплює або навіть змінює передавані між ними дані без їхнього відома. Цей вид атаки дає зловмиснику можливість переглядати, вносити зміни чи навіть виводити з ладу передані дані між двома точками.

Основні методи, які використовуються в атаках типу Man-in-the-Middle, включають:

1) Перехоплення трафіку: Зловмисник може перехоплювати трафік між користувачем і сервером, використовуючи різноманітні техніки, такі як аналіз пакетів, отримання необхідних ключів шифрування, або навіть використання шкідливого програмного забезпечення.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

2) Зміна вмісту: Зловмисник може внести зміни в передані дані між сторонами. Це може включати в себе внесення змін в електронні повідомлення, банківські транзакції або інші типи комунікації.

3) Введення шкідливого програмного забезпечення: Зловмисник може вводити шкідливе програмне забезпечення в передавані дані, таке як віруси, троянські коні чи шпигунське програмне забезпечення.

4) SSL Stripping: Атака, при якій зловмисник намагає змусити використовувати незашифрований зв'язок замість захищеного SSL/TLS. Це дозволяє зловмиснику переглядати передавані дані відкритим текстом.

5) Wi-Fi-атаки: Атаки на вразливості в бездротових мережах, такі як розподілена атака захоплення пакетів (WPA-PSK атака), з метою отримання доступу до передаваних даних.

Ці атаки можуть відбуватися в різних сценаріях, включаючи відкриті мережі, де комунікація не зашифрована, або в захищених мережах, де зловмисники намагаються обійти шифрування або використовують соціальну інженерію для отримання доступу до ключів шифрування. [15]

Сканування портів та вразливостей

Сканування портів та вразливостей є однією з основних технік, яку використовують зловмисники для виявлення слабких місць в системі чи мережі. Основна мета цієї атаки - знайти доступні порти та виявити вразливості, які можуть бути використані для незаконного вторгнення. Основні етапи сканування портів та вразливостей:

1) Збір інформації:

– Активний збір інформації: Зловмисники використовують різні техніки, такі як DNS-запити, WHOIS-запити, аналіз мережевого трафіку тощо, для отримання інформації про цільову систему.

– Пасивний збір інформації: Здебільшого використовуються публічно доступні ресурси та інтернет-архіви для отримання інформації без прямого взаємодії з цільовою системою.

2) Сканування портів:

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

– TCP-сканування: Зловмисники відправляють TCP-запити на різні порти системи для визначення того, які порти відкриті та доступні для з'єднань.

– UDP-сканування: Зловмисники можуть використовувати UDP-пакети для визначення доступності та стану UDP-портів на цільовій системі.

3) Виявлення вразливостей:

– Активне виявлення вразливостей: Після визначення активних портів, зловмисники проводять сканування вразливостей, використовуючи різні техніки та інструменти, щоб знайти слабкі місця в системі.

– Використання баз даних вразливостей: Зловмисники можуть використовувати бази даних вразливостей для знаходження відомих проблем у програмах та операційних системах.

4) Експлуатація вразливостей:

Атака: Після успішного виявлення вразливостей зловмисники можуть намагатися експлуатувати ці вразливості, введення шкідливого коду або отримання несанкціонованого доступу.

5) Звітність:

Підготовка звіту: Зловмисники можуть створити документ, в якому вказані результати сканування портів та вразливостей, щоб поділитися з іншими зловмисниками або для використання у подальших атаках. [15]

Zero-Day атаки

Zero-Day атаки — це атаки, які використовують вразливості в програмному забезпеченні, які виробники чи розробники ще не встигли виправити (патчі не були випущені), тобто атакуючий використовує вразливості, про які ніхто не знає (до виявлення зазначеної вразливості). Такі атаки можуть бути дуже небезпечними, оскільки вони дають зловмисникам можливість використовувати слабкі місця в системі, навіть після того, як вони стають відомими для розробників програмного забезпечення.

Основні характеристики Zero-Day атак:

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

1) Неочікувані вразливості: Вразливості, які використовуються в Zero-Day атаках, ще не відомі розробникам програмного забезпечення чи вендорам, тому вони не мають можливості випустити патч для виправлення.

2) Швидкість експлуатації: Оскільки вразливість ще не відома, атакуючі можуть вільно використовувати цю вразливість без будь-якого відповідного заходу з боку розробників програмного забезпечення.

3) Таємно використовується: Зловмисники можуть використовувати Zero-Day вразливості та виконувати атаки, не залишаючи слідів, оскільки ніхто не враховує такий тип вразливостей.

4) Потенційно велика шкода: Оскільки жоден патч не випущений, програми чи системи можуть бути компрометовані, і це може призвести до втрати конфіденційності, цілісності даних та доступності систем.

5) Низька виявленість: Zero-Day атаки можуть бути важко виявити, оскільки вони використовують нові методи та вразливості, про які ще немає відомостей. [15]

Шкідливе програмне забезпечення та віруси

Мальвара (Malware) - це загальний термін, який використовується для опису шкідливого програмного забезпечення, створеного з метою завдання шкоди комп'ютерам, мережам чи користувачам. Мальвара включає в себе різні види загроз, такі як віруси, троянські коні, шпигунське програмне забезпечення, рекламне програмне забезпечення (adware), черв'яки та інші.

Давайте розглянемо деталізованіше два основних види мальвари - віруси та троянські коні:

1) Віруси (Viruses):

Вірус - це програма, яка вбудовується в інші файли або програми та розповсюджується, якщо користувач використовує або запускає заражений файл. Віруси можуть руйнувати дані, перешкоджати нормальному функціонуванню системи та розповсюджуватися через мережі.

Способи поширення: Віруси часто поширюються через заражені файли, відсилані електронною поштою, USB-носії, веб-сайти та інші способи.

Характеристики:

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- Спрограмовані для саморозповсюдження та вбудовування в інші файли.
- Можуть виконувати руйнівні дії, такі як видалення файлів, зміна інформації, шифрування даних тощо.
- Часто використовуються для отримання несанкціонованого доступу до системи.

2) Троянські коні (Trojans):

Троянський конь (або троянець) - це вид шкідливого програмного забезпечення, яке приховано вбудовується в корисний або легітимний файл чи програму. Вони намагаються видавати себе за надійні або корисні програми для отримання доступу до системи.

Способи поширення: Троянські коні можуть бути поширені через віруси, заражені веб-сайти, електронну пошту або схеми соціальної інженерії.

Характеристики:

- Приховуються під корисними програмами чи файлами.
- Можуть створювати бекдор для забезпечення несанкціонованого доступу.
- Здатні виконувати різні завдання, такі як збір конфіденційної інформації, встановлення додаткового шкідливого програмного забезпечення. [15]

Внутрішні мережеві атаки

Внутрішні мережеві атаки - це атаки, що відбуваються всередині компаній, організацій або систем, залучаючи членів внутрішнього кола. Ці атаки можуть бути інсайдерськими, тобто виконуваними особами, які мають доступ до мережі чи системи. Такі атаки можуть бути спрямовані на незаконне отримання, модифікацію, видалення чи витіснення даних, а також порушення цілісності чи конфіденційності інформації всередині мережі чи системи. Серед інсайдерських атак можна виокремити наступні:

1) Зловживання привілеїв адміністратора

Атака полягає в тому, щоб працівник, який має адміністративні привілеї, використовує їх несанкціоновано для отримання доступу до чутливих даних, видалення або зміни налаштувань системи. Це може бути системний адміністратор, що

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

використовує свої привілеї для перегляду конфіденційних фінансових даних без необхідності або дозволу.

2) Перехоплення привілейованих облікових даних

Під час виконання атаки зловмисник перехоплює облікові дані особи або облікові дані з привілейованими доступами для незаконного входу в систему. Основним способом виконання є використання програмного забезпечення для перехоплення паролів адміністраторів під час їх введення.

3) Привілейована ескалація

Атака передбачає отримання більших привілеїв, ніж забезпечено за замовчуванням, шляхом використання вразливостей в системі. Наприклад, зловмисник використовує вразливість в програмному забезпеченні для отримання адміністративних привілеїв на сервері.

4) Внутрішнє шпигунство

Працівник або особа всередині організації намагається отримати несанкціонований доступ до конфіденційної інформації для подальшого використання чи розголошення. Внутрішній шпигун може використовувати свій легітимний доступ або використовувати соціальні інженерії для отримання додаткових прав та доступу. Зазвичай це робітник, що має доступ до конфіденційних даних компанії, копіює чутливу інформацію і передає її конкурентам або використовує для особистої вигоди.

5) Привілейована інформаційна атака

Під час атаки зловмисник використовує свої привілеї для впливу на інформаційні процеси, зокрема, вносить зміни в дані чи впливає на їх цілісність. Зазвичай використовується для псування, фальсифікації чи недостовірного представлення інформації з метою шкоди або вигоди. Це може бути адміністратор баз даних, який вносить некоректні зміни в записи для спотворення інформації. Наприклад, він може змінити фінансові дані компанії, щоб створити штучний образ збитків або вигоди для особистих цілей чи на користь конкурентів. [15]

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

1.4.4 Загальні рекомендації для захисту мережі

Захист мережі є важливим завданням для забезпечення цілісності, конфіденційності та доступності інформації. Однак, не можна обмежуватися захистом від конкретних атак, оскільки кіберзлочинці постійно вдосконалюють свої методи. Додатково до захисту від конкретних загроз, важливо впроваджувати загальні стратегії та рекомендації, що стосуються всієї мережевої інфраструктури. Нижче подано кілька загальних рекомендацій:

Навчання користувачів та обмеження прав доступу

Навчання користувачів на підприємстві - це ключовий елемент успішного впровадження нових технологій, процесів або програмного забезпечення. Це допомагає співробітникам оволодіти новими навичками та знаннями, необхідними для ефективної роботи з інструментами та системами, які вони використовують у своїй роботі. Може включати в себе різноманітні тренінги, вебінари, навчальні матеріали та інші ресурси.

Детальна програма навчання може включати такі елементи:

1. Ознайомлення з основними функціями та можливостями системи.
2. Навчання користувачів, як виконувати конкретні завдання в межах системи, наприклад, створення звітів, редагування даних тощо.
3. Інструкції щодо безпеки даних, використання паролів, обмеження доступу тощо.
4. Надання інформації про доступні ресурси підтримки, а також інструкції з вирішення проблем, що часто зустрічаються.
5. Інформування користувачів про нові версії програмного забезпечення, важливі оновлення та нові функції.

Іншим важливим аспектом є оцінка ефективності навчання, щоб переконатися, що користувачі засвоїли необхідні знання та навички.

Обмеження прав доступу - це стратегія контролю доступу, яка дозволяє обмежити користувачам доступ до певних ресурсів або функцій залежно від їхніх ро-

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

лей, обов'язків або потреб. Це може бути досягнуто за допомогою різних механізмів, таких як рольовий доступ, політики безпеки, аутентифікація та авторизація.

Деякі типові практики обмеження прав доступу включають:

1. Призначення користувачам ролей, які відображають їхні обов'язки та повноваження. Наприклад, адміністратори мають широкі повноваження, тоді як звичайні користувачі мають обмежений доступ.

2. Встановлення правил, які визначають, які дії можуть виконувати різні користувачі та які ресурси вони можуть використовувати.

3. Перевірка ідентифікації користувача та надання доступу лише тим, хто має відповідні повноваження.

4. Моніторинг та реєстрація дій користувачів для виявлення неправомірних спроб доступу або використання ресурсів.

Ці практики допомагають забезпечити безпеку даних та зменшити ризик витоку інформації або несанкціонованого доступу до системи. [15]

Використання надійних паролів

Пароль — це перша лінія оборони вашої мережі, тому йому варто приділити особливу увагу. Кілька конкретних кроків, які варто вжити:

1. Що більше символів у паролі, тим він складніший для вгадування. Рекомендована довжина пароля - не менше 12 символів.

2. Не використовуйте прості слова чи фрази зі словника. Хакери використовують програми, які автоматично перебирають слова.

3. Включіть в пароль букви (верхнього та нижнього регістрів), цифри та спеціальні символи. Такий підхід робить пароль більш стійким.

4. Не використовуйте один і той самий пароль для різних акаунтів. В разі взлому одного паролю, усі ваші акаунти будуть вразливі.

5. Використовуйте пароліні фрази, які складаються з кількох слів. Вони можуть бути легкі для запам'ятовування, а в той же час стійкими до атак.

6. Змінюйте паролі періодично. Це зменшить ризик, що хтось зможе отримати доступ до вашого акаунту в разі витоку інформації.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

7. Використовуйте двофакторну автентифікацію там, де це можливо. Це додасть додатковий шар безпеки, навіть якщо хтось зможе вгадати ваш пароль. [15]

Оновлення програмного забезпечення

Всі програми та операційні системи мають важливі патчі та оновлення для закриття вразливостей. Розглянемо детальніше важливість та кроки щодо оновлення програмного забезпечення для забезпечення максимального рівня безпеки в вашій мережі:

1. Налаштуйте автоматичне оновлення для вашої операційної системи та всього встановленого програмного забезпечення, якщо ця опція доступна. Це гарантує, що ви завжди маєте найновіші версії з усіма важливими патчами без додаткового зусилля.

2. Створіть графік регулярних перевірок для оновлень. Визначте час, коли ви можете витратити кілька хвилин для перевірки доступних оновлень та їх установки.

3. Завжди завантажуйте оновлення та патчі з офіційних веб-сайтів та ресурсів розробників. Уникайте сумнівних джерел, оскільки це може призвести до введення шкідливого коду на вашу систему.

4. Не обмежуйтеся лише оновленням операційної системи. Регулярно перевіряйте оновлення для браузерів, додатків та плагінів. Це важливо для запобігання вразливостям, які можуть виникнути через застосунки третіх сторін.

5. Використовуйте системи моніторингу, щоб отримувати сповіщення про доступні оновлення та патчі. Це дозволить вам реагувати оперативно та уникнути використання застарілих версій програм.

6. Перед встановленням великих оновлень чи патчів створюйте резервні копії важливих даних. Це захистить вашу інформацію в разі непередбачених проблем під час процесу оновлення.

7. Для більш складних систем важливо перед оновленням провести тестування на тестових серверах, щоб уникнути можливих конфліктів та збоїв. [15]

Використання антивірусного програмного забезпечення

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Зважаючи на постійно зростаючу загрозу шкідливого коду та вірусів, використання антивірусного програмного забезпечення є важливою частиною стратегії безпеки мережі. Давайте детальніше розглянемо ці практики:

1. Оберіть відомий та довірений антивірусний продукт від визнаного розробника. Добре вивчайте відгуки та рейтинги перед тим, як встановити антивірус.

2. Регулярно оновлюйте бази даних антивірусного програмного забезпечення. Це дозволяє програмі виявляти найновіші види загроз та ефективно захищати вашу систему.

3. Встановіть графік для повних та регулярних сканувань вашої системи. Це допомагає виявляти та вилучати потенційно небезпечні файли, які можуть залишитися непоміченими.

4. Розгляньте вибір антивірусного програмного забезпечення, яке не тільки виявляє віруси, але також має додаткові функції, такі як захист від шкідливих веб-сайтів, файрвол та антиспам.

5. Увімкніть функцію реального часу для постійного моніторингу та виявлення загроз у режимі реального часу. Це допоможе блокувати шкідливий код, ще до того, як він зможе викликати шкоду.

6. Налаштуйте антивірус так, щоб він автоматично сканував вкладені файли у електронних листах та інших джерелах.

7. Перевіряйте активність програм та процесів на наявність підозрілих дій, що можуть свідчити про інфікування системи. [15]

Моніторинг мережі та аудит безпеки

Моніторинг мережі та аудит безпеки є важливими складовими безпеки інформації в будь-якій організації. Ці процеси допомагають виявляти потенційні загрози, слабкі місця та вразливості в інформаційних системах та мережах. Давайте розглянемо їх більш детально:

Моніторинг мережі передбачає постійний збір даних про активність у мережі, такі як трафік, журнали подій тощо. Одним із ключових аспектів моніторингу мережі є аналіз трафіку для виявлення аномальної або підозрілої активності, такої як атаки, спроби несанкціонованого доступу тощо.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Моніторинг допомагає виявляти різноманітні загрози для мережі, включаючи віруси, шкідливі програми, фішингові атаки, атаки з переповнення буфера тощо. Після виявлення підозрілих або аномальних активностей моніторинг мережі дозволяє оперативно реагувати на них, вживаючи відповідних заходів безпеки.

Аудит безпеки включає оцінку вразливостей інформаційних систем та мереж для виявлення можливих точок входу для потенційних атак.

Аудит також включає перевірку відповідності організаційних процедур та політик безпеки стандартам і законодавству, таким як GDPR, HIPAA, PCI DSS тощо.

Проведення тестів проникнення - це важлива частина аудиту, яка полягає в спробах проникнення в інформаційні системи організації для виявлення слабких місць та вразливостей.

Аудит також включає аналіз журналів подій та інших записів для виявлення аномальних дій та потенційно небезпечної активності.

В цілому, моніторинг мережі та аудит безпеки допомагають організаціям не тільки виявляти потенційні загрози, а й приймати вчасні заходи для їх запобігання та мінімізації ризиків для безпеки інформації. [15]

Резервне копіювання та шифрування даних

Резервне копіювання даних та шифрування – це дві важливі практики, які допомагають організаціям забезпечити захист, доступність та конфіденційність їхніх даних у сучасному цифровому середовищі.

Резервне копіювання даних гарантує, що інформація може бути відновлена в разі втрати або пошкодження основних даних через такі фактори, як випадкове видалення, віруси, кібератаки або технічні несправності.

Шифрування забезпечує захист конфіденційності даних, зробивши їх незрозумілими для несанкціонованих осіб, які не мають відповідного ключа для розшифрування.

Регулярне створення резервних копій забезпечує захист від втрати важливих даних, які можуть стати невідновними в разі аварій або катастроф.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Шифрування запобігає несанкціонованому доступу до даних навіть у випадку, якщо хтось отримає фізичний доступ до носія даних або вперушиться в мережу.

Резервне копіювання може здійснюватися на різних рівнях, від копій всієї системи до окремих файлів або баз даних, залежно від потреб організації.

Шифрування може застосовуватися як в режимі покладення на рівні файлів або директорій, так і на рівні цілих дисків або томів, забезпечуючи захист на різних рівнях системи.

Організації повинні мати чіткий план відновлення даних, який включає процедури відновлення, тестування резервних копій та розгортання резервних копій у разі потреби.

Багато секторів, зокрема фінансовий, медичний та галузь обробки особистих даних, мають вимоги щодо шифрування даних відповідно до регулятивних стандартів, таких як GDPR, HIPAA тощо. [15],[16]

Використання VPN та фаєрволів

VPN, або віртуальна приватна мережа, є технологією, яка дозволяє створювати безпечне з'єднання між вашим пристроєм та інтернет-сервером через шифровану тунельну мережу. VPN дозволяє приховати ваш реальний IP-адресу, забезпечуючи анонімність в Інтернеті та унеможливлюючи відстеження вашого мережевого активу. Це забезпечує конфіденційність і безпеку передачі даних між вами та інтернет-ресурсами. VPN забезпечує зашифрування трафіку, що унеможливлює перехоплення особистої інформації, такої як паролі, фінансові дані і зміст повідомлень. Крім того, віртуальна мережа дозволяє обходити географічні обмеження і отримувати доступ до веб-ресурсів, які можуть бути недоступні в вашому регіоні.

Зазвичай VPN і фаєрволи працюють у поєднанні для забезпечення комплексного рівня безпеки мережі. Використання обох цих технологій дозволяє створити ефективний захист в Інтернеті.

Фаєрвол (мережевий екран) - це програма або апаратний пристрій, який контролює та регулює потік мережевого трафіку між комп'ютерами чи мережами з різ-

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

них рівнів безпеки. Основна функція фаєрволу - це фільтрація трафіку, блокування або дозвіл певних видів з'єднань на основі встановлених правил. Це допомагає захищати мережу від несанкціонованого доступу, атак, вірусів та інших шкідливих елементів. Фаєрвол також може використовуватися для моніторингу мережевої активності і налаштування політик безпеки.

Для того, щоб дані технології відмінно працювали у тандемі, варто застосувати декілька правил:

Налаштуйте правила фаєрволу для контролю доступу через VPN. Дозвольте з'єднання тільки від відомих і довірених VPN-серверів та забороняйте доступ для невідомих джерел.

Встановіть правила для ідентифікації та фільтрації VPN-трафіку залежно від типу протоколу (наприклад, OpenVPN, IPSec). Це дозволить ефективно управляти різними видами VPN-з'єднань.

Встановіть правила, які обмежують доступ до конкретних ресурсів або служб лише через VPN. Це забезпечить додатковий шар захисту та контролю над тим, які дані можуть бути передані через VPN-з'єднання.

Використовуйте VPN для шифрування трафіку внутрішньої мережі, особливо при з'єднанні між різними фізичними розташуваннями офісів. Захищайте конфіденційні дані від несанкціонованого доступу.

Встановіть правила, які блокують використання небезпечних або застарілих VPN-протоколів, щоб уникнути потенційних загроз безпеки.

Включіть журналювання подій для VPN-з'єднань, щоб відстежувати та аналізувати активність в мережі через VPN. Це допомагає вчасно виявляти аномалії та можливі атаки.

Періодично переглядайте та оновлюйте правила фаєрволу відповідно до нових загроз та розвитку технологій VPN. Це забезпечить ефективний захист вашої мережі. [16]

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Висновки до першого розділу

В ході написання першого розділу було проведено всебічний аналіз ІТ-інфраструктури та її ключових аспектів. Початково визначено поняття ІТ-інфраструктури, яка включає апаратне забезпечення, програмне забезпечення, мережеві ресурси та сервіси, що забезпечують функціонування і управління ІТ-системами. Основні типи ІТ-інфраструктур включають локальні, хмарні та гібридні рішення, кожне з яких має свої особливості та переваги.

Розглянуто основні вразливості для безпеки ІТ-інфраструктури, такі як несанкціонований доступ, шкідливе програмне забезпечення, фішинг-атаки та інші. Для їх усунення пропонуються різні методи, включаючи використання сучасних антивірусних програм, фаєрволів, систем виявлення вторгнень (IDS), а також проведення регулярних аудитів безпеки.

Окремо розглянуто принципи побудови ІТ-інфраструктури на базі служби каталогів AD, яка є важливим елементом управління мережними ресурсами та безпекою. Active Directory забезпечує централізоване управління обліковими записами користувачів, комп'ютерами та іншими ресурсами, а також можливості для захисту мережних інфраструктур завдяки впровадженню групових політик та інших інструментів безпеки.

Групові політики в AD дозволяють адміністраторам встановлювати правила та обмеження для користувачів і комп'ютерів, що підвищує рівень безпеки та забезпечує контрольоване середовище роботи. Резервне копіювання та відновлення в AD є критично важливими для забезпечення безперервності бізнесу та збереження даних у випадку аварійних ситуацій.

Проаналізовано загрози для ІТ-систем з використанням AD, такі як атаки на облікові записи, підвищення привілеїв та інші. Відповідні заходи для запобігання цим загрозам включають впровадження багатофакторної автентифікації, регулярне оновлення програмного забезпечення, а також моніторинг підозрілої активності.

Розглянуто типові протоколи побудови мережних інфраструктур, вразливості та потенційні ризики використання AD. Мережеві атаки, такі як DDoS, Man-in-

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

the-Middle та інші, можуть суттєво порушити роботу ІТ-інфраструктури. Для їх запобігання рекомендуються заходи, такі як використання шифрування, надійних паролів, регулярне оновлення системи та програмного забезпечення.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

РОЗДІЛ 2 ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ НА БАЗІ MICROSOFT ACTIVE DIRECTORY

2.1 Вибір обладнання для організації роботи мережі

В якості маршрутизатора для рівнів ядра та розподілу було обрано маршрутизатори Cisco 7600 Series. Вони є основою для подальшого розвитку підприємства, забезпечуючи надійний і високоефективний протокол IP, який використовується багатьма обчислювальними центрами для зв'язку. Лінійка маршрутизаторів серії 7600 підходить як для великих компаній, так і для мереж MAN/WAN, завдяки підтримці різних інтерфейсів, адаптації до завантажених мереж і високій ефективності. Серед основних переваг можна також виділити:

- Підтримка повного спектру функцій Cisco IOS™.
- Шасі, сумісне зі стандартом NEBS (для Cisco 7609 – з вентиляцією від передньої до задньої панелі).
- Підтримка розподіленої функціональності Distributed Cisco Express Forwarding (крім Cisco 7603).
- Висока доступність платформи завдяки резервуванню блоків живлення, модулів управління та програмних можливостей ПЗ Cisco IOS™ - Global Resilience IP.
- Апаратне прискорення мережевих послуг завдяки технології Cisco PXF.
- Підтримка технології MPLS.
- Підтримка загальних для серій Catalyst 6500 та Cisco 7600 модулів розширення (повний список наведено у розділі «Комутатори серії Catalyst 6500х»).
- Підтримка спільних для серій Cisco 7200, Cisco 7100, Cisco 7400 та Cisco 7500 інтерфейсних модулів за допомогою модуля FlexWAN. [19]

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52



Рисунок 2.1 – Маршрутизатор Cisco 7600 Series

Для організації комутації на рівні 2 було обрано комутатор Cisco 2960, який дозволяє створити розвинену та надійну локальну мережу як у великих компаніях і корпораціях, так і у системах з філіями. Надійна конфігурація Cisco 2960 забезпечує мережеве підключення на швидкостях від 10 до 100 Мбіт/с. Серед основних технічних характеристик C2960 можна виділити:

- Підтримка Fast та Gigabit Ethernet з варіантами на 8, 24 та 48 портів.
- Можливість передачі електроживлення через кручену пару у версії з 24 портами.
- Покращені функції безпеки, зокрема створення складних списків управління доступом.
- Широкий спектр опцій для керування якістю обслуговування.
- Інтелектуальна сервісна система на межі мережі.
- Гарантійне обслуговування протягом усього терміну служби обладнання.
- Кожен комутатор постачається з програмним забезпеченням Cisco Network Assistant, яке дозволяє структуровано керувати всіма пристроями мережі. Це ПЗ включає безліч майстрів автоматичного та ручного налаштування, що робить процес налаштування та управління комутатором простим і надійним. [20]

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		53



Рисунок 2.2 – Комутатор Cisco Catalyst 2960-24LC-S4

2.2 Розробка проєкту мережі

При проектуванні мережі була використана трирівнева структура, яка включає в себе:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

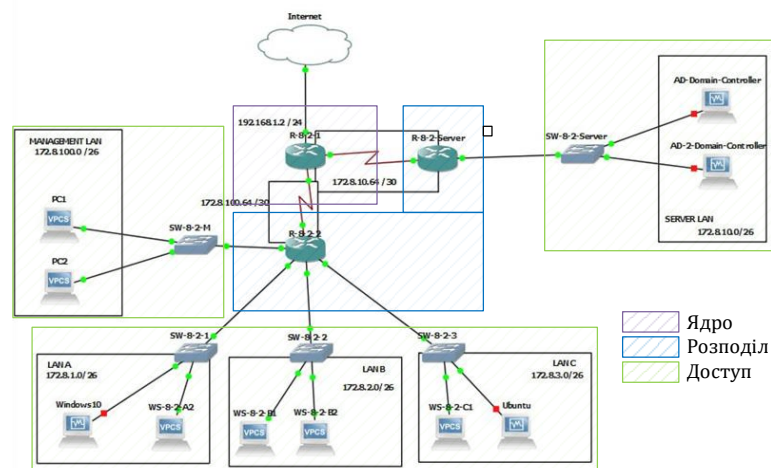


Рисунок 2.3 – Проект мережі

До рівня ядра входять маршрутизатор провайдера. До рівня розподілу входять 2 маршрутизатори, що відповідають за функціонування підмереж. До рівня доступу входить 5 комутаторів для підмереж: Management, LAN A, LAN B, LAN C та серверна мережа. Загалом мережа була створена з 3 маршрутизаторів, 5 комутаторів, 8 робочих станцій та з 2 серверів з Active Directory.

Між пристроями рівня ядра та розподілу встановлено послідовне з'єднання, а на рівні доступу застосовано технологію Ethernet. Загальна схема мережі наведена у додатку А.

Топологія мережі – це фізична чи логічна структура, яка визначає, як взаємодіють та з'єднані комп'ютери та інші пристрої у мережі. Важливість топології мережі для проектування IT-інфраструктури на основі Active Directory полягає в її

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

впливі на ефективність, доступність, стійкість та безпеку мережі. Вибір оптимальної топології допомагає оптимізувати роботу мережі, забезпечуючи надійну та ефективну взаємодію пристроїв. [18]

Топологію нашої мережі можна характеризувати як гнучку гібридну топологію. Вона включає в себе комбінацію:

– деревоподібна топологія – є основною у мережі IT-інфраструктури через свою ефективність та гнучкість. У цій топології комп'ютери та пристрої організовані у вигляді ієрархічної структури, подібно до дерева. Кожен вузол може мати під собою підз'єднані інші вузли, що дозволяє ефективно керувати трафіком та спрощує розширення мережі. Ця топологія також забезпечує високу доступність та стійкість, оскільки відсутній один центральний вузол, від відмови якого може залежати вся мережа.

– зіркової топологія – є простою та легкою у управлінні, тому застосовується у локальних підмережах. У цій топології всі пристрої підключені до центрального вузла-комутатора, утворюючи структуру подібну зірці. Кожен пристрій взаємодіє лише з центральним вузлом, що стабільність роботи мережі. Зіркова топологія також легко розширюється та масштабується при додаванні нових пристроїв.

2.3 Розробка адресації мережі

В ролі протоколу маршрутизації було налаштовано протокол OSPF.

OSPF – протокол динамічної маршрутизації, що базується на технології відстеження стану каналу і використовує для знаходження найкоротшого шляху алгоритм Дейкстри.

Даний протокол є гарним рішенням для мережі з Active Directory завдяки своїй швидкій конвергенції та підтримці великих і складних топологій. Active Directory вимагає швидкого відновлення з'єднання між доменними контролерами у разі змін у мережі, і OSPF забезпечує швидке оновлення маршрутизаційних таблиць. Підтримка розподілу мережі на зони в OSPF допомагає зменшити розмір таблиць та спростити управління складними топологіями великих організацій з чис-

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

ленними підрозділами. Додатково, OSPF забезпечує високу надійність та відмовостійкість, що є критичним для Active Directory. Завдяки використанню кількох шляхів до однієї мети, OSPF гарантує стабільність і доступність мережі. Це важливо для ефективної реплікації даних між доменними контролерами, що потребує стабільних і надійних з'єднань.

Розподіл підмереж наведено та адресація усіх пристроїв мережі наведена у таблиці 2.1.

Таблиця 2.1 – Адресація мережі

Мережа/Пристрій	Інтерфейс/Шлюз	IP-адреса	Маска	Префікс
INTERNET LAN	-	192.168.1.0	255.255.255.0	/24
Internet	Ethernet	192.168.1.1	255.255.255.0	/24
R-8-2-1	FastEthernet0/0	192.168.1.2	255.255.255.0	/24
R1-TO-RServer	-	172.8.10.64	255.255.255.252	/30
R-8-2-1	Serial6/1	172.8.10.65	255.255.255.252	/30
R-8-2-Server	Serial6/1	172.8.10.66	255.255.255.252	/30
R1-TO-R2	-	172.8.100.64	255.255.255.252	/30
R-8-2-1	Serial6/0	172.8.100.65	255.255.255.252	/30
R-8-2-2	Serial6/0	172.8.100.66	255.255.255.252	/30
SERVER LAN	-	172.8.10.0	255.255.255.192	/26
R-8-2-Server	FastEthernet0/0	172.8.10.1	255.255.255.192	/26
SW-8-2-Server	Vlan 1	172.8.10.2	255.255.255.192	/26
	Шлюз за замовч.	172.8.10.1	-	-
	Основ. DNS-сервер	172.8.10.3	-	-
AD-Domain-Controller	Мережний адаптер	172.8.10.3	255.255.255.192	/26
	Шлюз за замовч.	172.8.10.1	-	-
AD-2-Domain-Controller	Мережний адаптер	172.8.10.4	255.255.255.192	/26
	Шлюз за замовч.	172.8.10.1	-	-
MANAGEMENT LAN	-	172.8.100.0	255.255.255.192	/26
R-8-2-2	FastEthernet0/0	172.8.100.1	255.255.255.192	/26
SW-8-2-M	Vlan 1	172.8.100.2	255.255.255.192	/26
	Шлюз за замовч.	172.8.100.1	-	-
	Основ. DNS-сервер	172.8.10.3	-	-
WS-8-2-M-1	Мережний адаптер	172.8.100.3	255.255.255.192	/26
	Шлюз за замовч.	172.8.100.1	-	-
	Основ. DNS-сервер	172.8.10.3	-	-
WS-8-2-M-2	Мережний адаптер	172.8.100.4	255.255.255.192	/26
	Шлюз за замовч.	172.8.100.1	-	-
	Основ. DNS-сервер	172.8.10.3	-	-
LAN A	-	172.8.1.0	255.255.255.192	/26
R-8-2-2	FastEthernet1/0	172.8.1.1	255.255.255.192	/26
SW-8-2-1	Vlan 1	172.8.1.2	255.255.255.192	/26
	Шлюз за замовч.	172.8.1.1	-	-

	Основ. DNS-сервер	172.8.10.3	-	-
--	-------------------	------------	---	---

Продовження таблиці 2.1

Мережа/Пристрій	Інтерфейс/Шлюз	ІР-адреса	Маска	Префікс
WS-8-2-A1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
	Основ. DNS-сервер			
WS-8-2-A2	Мережний адаптер			
	Шлюз за замовч.			
	Основ. DNS-сервер			
LAN B	-	172.8.2.0	255.255.255.192	/26
R-8-2-2	FastEthernet1/1	172.8.2.1	255.255.255.192	/26
SW-8-2-2	Vlan 1	172.8.2.2	255.255.255.192	/26
	Шлюз за замовч.	172.8.2.1	-	-
	Основ. DNS-сервер	172.8.10.3	-	-
WS-8-2-B1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
	Основ. DNS-сервер			
WS-8-2-B2	Мережний адаптер			
	Шлюз за замовч.			
	Основ. DNS-сервер			
LAN C	-	172.8.3.0	255.255.255.192	/26
R-3	FastEthernet2/0	172.8.3.1	255.255.255.128	/25
SW-8-2-3	Vlan 1	172.8.3.2	255.255.255.128	/25
	Шлюз за замовч.	172.8.3.1	-	-
	Основ. DNS-сервер	172.8.10.3	-	-
WS-8-3-C1	Мережний адаптер	DHCP		
	Шлюз за замовч.			
	Основ. DNS-сервер			
WS-8-3-C2	Мережний адаптер			
	Шлюз за замовч.			
	Основ. DNS-сервер			

2.4Проектування служб та сервісів прикладного рівня

2.4.1 Налагодження DHCP-серверів

В якості DHCP-серверу було обрано маршрутизатор R-8-2-2.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

```
R-8-2-2(config)#ip dhcp excluded-address 172.8.1.1 172.8.1.10
R-8-2-2(config)#ip dhcp excluded-address 172.8.2.1 172.8.2.10
R-8-2-2(config)#ip dhcp excluded-address 172.8.3.1 172.8.3.10
R-8-2-2(config)#ip dhcp pool LAN-A
R-8-2-2(dhcp-config)#network 172.8.1.0 255.255.255.192
R-8-2-2(dhcp-config)#default-router 172.8.1.1
R-8-2-2(dhcp-config)#domain-name havrylyuk.net
R-8-2-2(dhcp-config)#dns-server 172.8.10.3
R-8-2-2(dhcp-config)#exit
R-8-2-2(config)#ip dhcp pool LAN-B
R-8-2-2(dhcp-config)#network 172.8.2.0 255.255.255.192
R-8-2-2(dhcp-config)#default-router 172.8.2.1
R-8-2-2(dhcp-config)#domain-name havrylyuk.net
R-8-2-2(dhcp-config)#dns-server 172.8.10.3
R-8-2-2(dhcp-config)#exit
R-8-2-2(config)#ip dhcp pool LAN-C
R-8-2-2(dhcp-config)#network 172.8.3.0 255.255.255.192
R-8-2-2(dhcp-config)#default-router 172.8.3.1
R-8-2-2(dhcp-config)#domain-name havrylyuk.net
R-8-2-2(dhcp-config)#dns-server 172.8.10.3
R-8-2-2(dhcp-config)#exit
```

Рисунок 2.4 – Налаштування DHCP

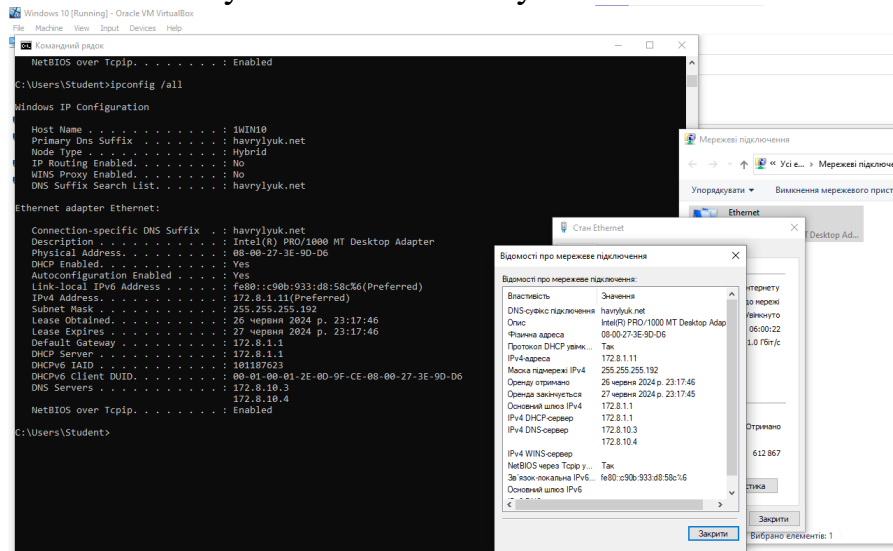


Рисунок 2.5 – Підключення робочої станції

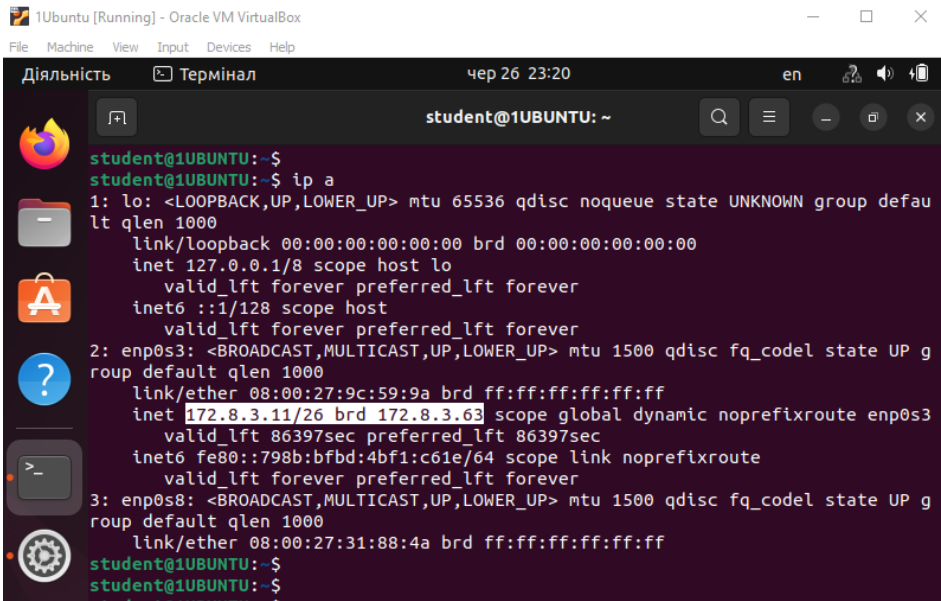


Рисунок 2.6 – Підключення робочої станції

```

WS-8-2-A2> ip dhcp
DORA IP 172.8.2.11/26 GW 172.8.2.1

WS-8-2-A2> show ip

NAME          : WS-8-2-A2[1]
IP/MASK       : 172.8.2.11/26
GATEWAY       : 172.8.2.1
DNS           : 172.8.10.3
DHCP SERVER   : 172.8.2.1
DHCP LEASE    : 86397, 86400/43200/75600
DOMAIN NAME   : havrylyuk.net
MAC           : 00:50:79:66:68:05
LPORT        : 10039
RHOST:PORT    : 127.0.0.1:10040
MTU           : 1500

```

Рисунок 2.7 – Підключення робочої станції

```

WS-8-2-A2> ping 172.8.1.11
84 bytes from 172.8.1.11 icmp_seq=1 ttl=127 time=20.779 ms
84 bytes from 172.8.1.11 icmp_seq=2 ttl=127 time=21.895 ms
84 bytes from 172.8.1.11 icmp_seq=3 ttl=127 time=17.067 ms

WS-8-2-A2> ping 172.8.3.11
84 bytes from 172.8.3.11 icmp_seq=1 ttl=63 time=21.836 ms
84 bytes from 172.8.3.11 icmp_seq=2 ttl=63 time=14.318 ms
84 bytes from 172.8.3.11 icmp_seq=3 ttl=63 time=12.664 ms

WS-8-2-A2> ping 172.8.10.4
84 bytes from 172.8.10.4 icmp_seq=1 ttl=125 time=61.951 ms
84 bytes from 172.8.10.4 icmp_seq=2 ttl=125 time=61.929 ms
84 bytes from 172.8.10.4 icmp_seq=3 ttl=125 time=61.919 ms

WS-8-2-A2> █

```

Рисунок 2.8 – Перевірка зв'язку

2.4.2 Налагодження Syslog-серверу

Syslog — це стандартний протокол, який використовується для надсилання повідомлень про події або системних журналів на визначений сервер. Основне його призначення — збір журналів з різних пристроїв і систем, а також зберігання їх в одному центральному місці для подальшого моніторингу та аналізу.

В проекті передбачено розгортання Syslog-серверу на станції Ubuntu Linux за допомогою утиліти RSyslog.

Rsyslog — це вдосконалена версія системного логгера для UNIX-подібних операційних систем, що забезпечує збір, фільтрацію та зберігання системних логів. Він дозволяє передавати логи на віддалені сервери і має гнучкі налаштування для обробки логів.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

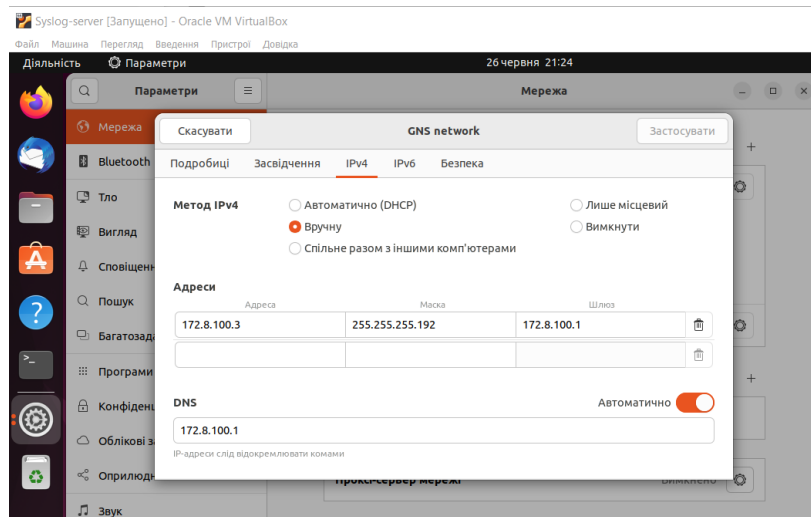


Рисунок 2.9 – Налаштування адреси Syslog-серверу

```
R-8-2-2(config)#logging 172.8.100.3
R-8-2-2(config)#exit
R-8-2-2#
*Mar 1 00:01:36.495: %SYS-5-CONFIG_I: Configured from console by console
R-8-2-2#
*Mar 1 00:01:37.495: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.8.100.3
stopped - CLI initiated
*Mar 1 00:01:37.495: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.8.100.3
started - CLI initiated
```

Рисунок 2.10– Приклад увімкнення логування

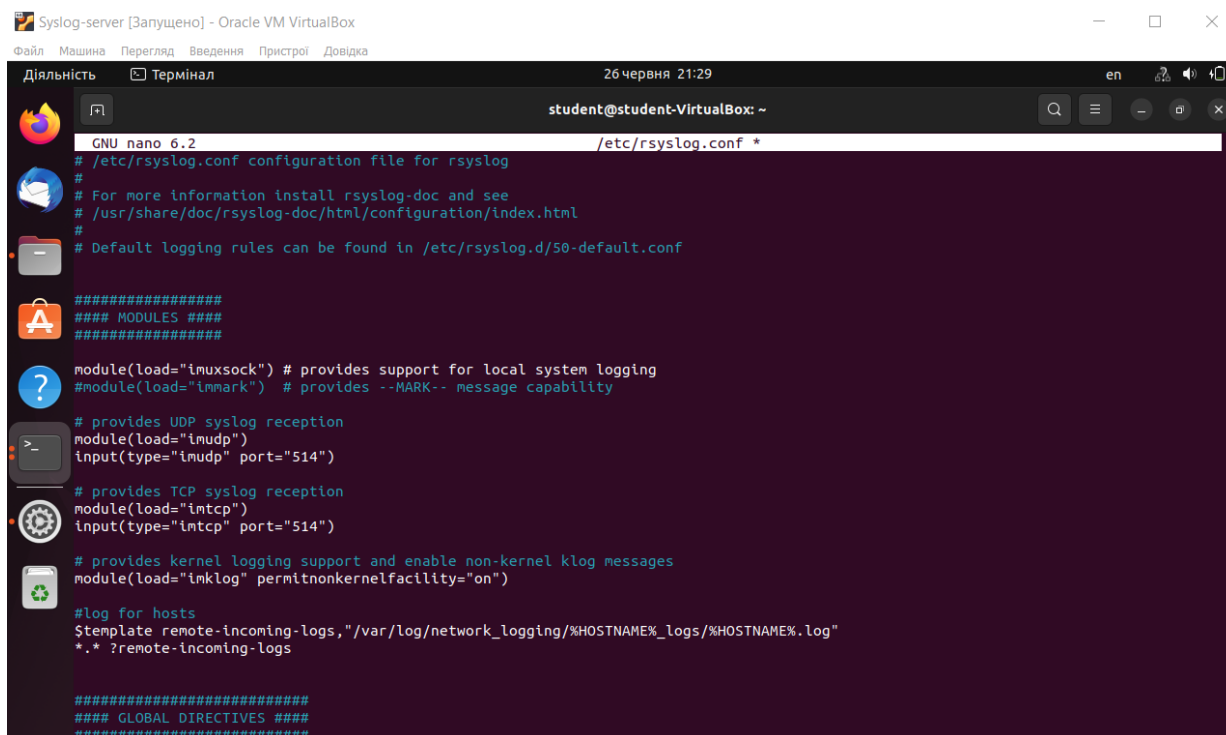


Рисунок 2.11 – Робота у конфігураційному файлі sudo nano /etc/rsyslog.conf

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

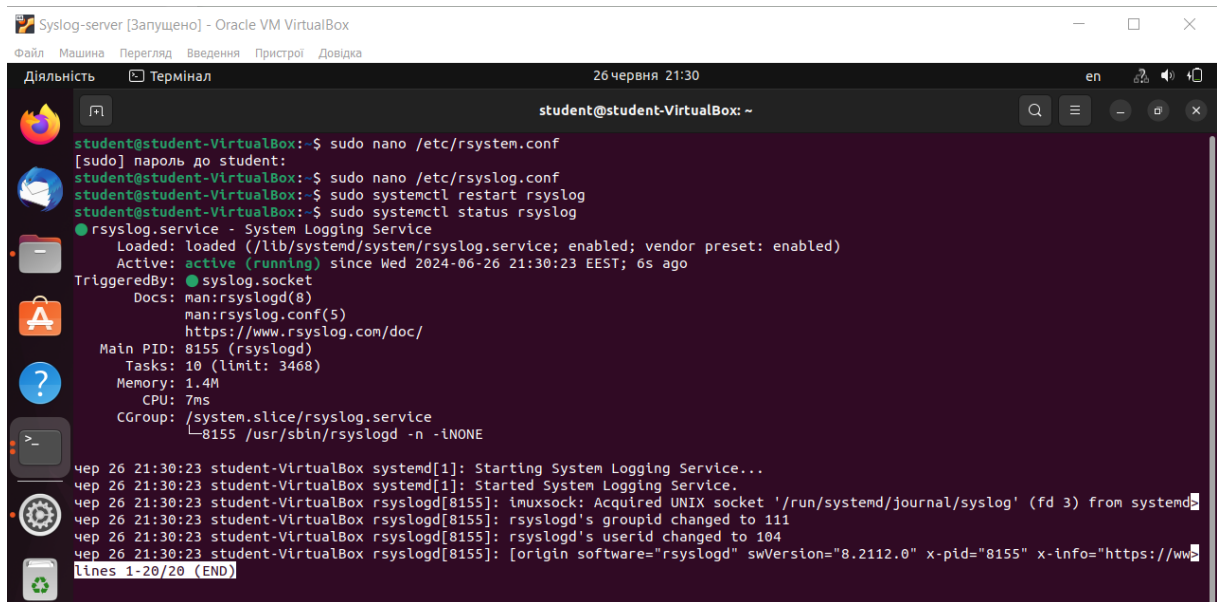


Рисунок 2.12 – Перезавантаження серверу (після внесення змін)

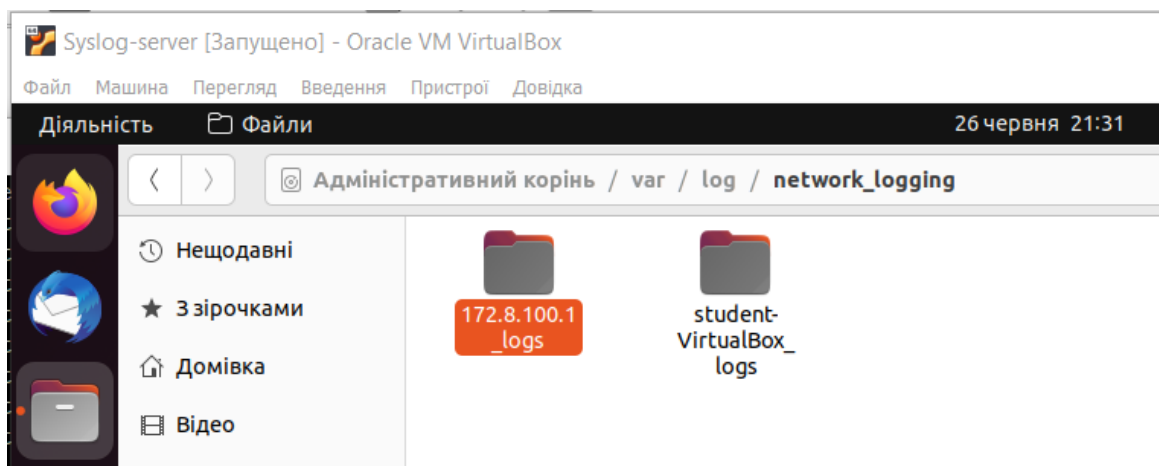


Рисунок 2.13 – Результат налаштування

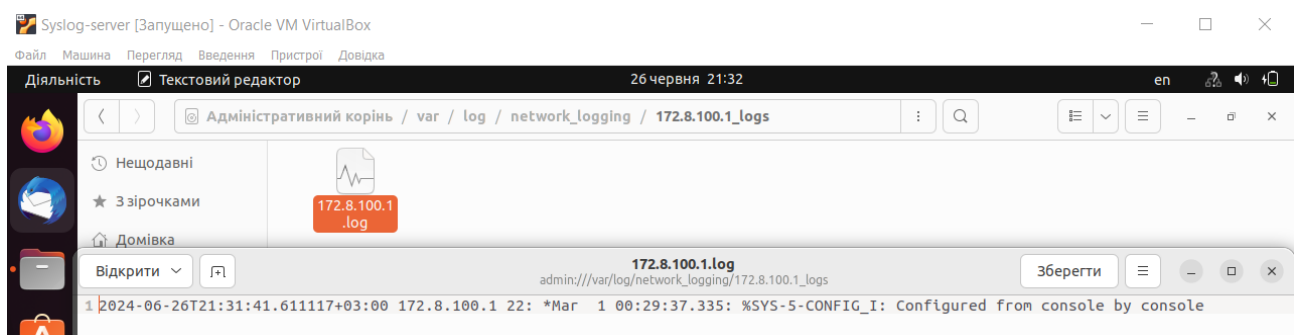


Рисунок 2.14 – Результат налаштування

Висновки до другого розділу

У ході написання другого розділу було розглянуто ключові етапи та аспекти, пов'язані з організацією роботи мережі. Перш за все, було проаналізовано вибір

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

обладнання для мережевої інфраструктури. Основну увагу приділено маршрутизаторам Cisco 7600 Series та комутаторам Cisco Catalyst 2960-24LC-S4, які є потужними рішеннями для забезпечення високої продуктивності, масштабованості та надійності мережі.

Далі, детально висвітлено процес розробки проєкту мережі. Включено аналіз вимог до мережі, проектування топології, вибір відповідних мережевих пристроїв та визначення місць їх встановлення.

Розробка адресації мережі є ще одним важливим аспектом, розглянутим у цьому розділі. Правильне планування IP-адресного простору забезпечує ефективне управління мережевими ресурсами та зменшує ризик конфліктів адрес. Було розглянуто методи планування адресації для різних підмереж.

Налагодження DHCP-серверів було виділено як ключовий етап для автоматизації процесу призначення IP-адрес клієнтським пристроям. DHCP-сервери забезпечують динамічне та централізоване управління адресним простором, що спрощує адміністрування мережі та знижує ймовірність помилок, пов'язаних з ручним налаштуванням IP-адрес.

Особливу увагу приділено налаштуванню Syslog-сервера, який є важливим компонентом для моніторингу та управління мережею. Syslog-сервер дозволяє збирати, зберігати та аналізувати журнали подій з різних мережевих пристроїв. Це сприяє своєчасному виявленню та реагуванню на проблеми, що виникають у мережі, а також допомагає у проведенні аудиту та забезпеченні відповідності політикам безпеки.

У підсумку, розглянуті питання забезпечують комплексний підхід до організації та управління мережею. Вибір відповідного обладнання, правильне планування адресації, автоматизація управління IP-адресами та ефективний моніторинг мережевих подій є ключовими аспектами для створення надійної та продуктивної мережевої інфраструктури.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОЕКТУ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ

3.1 Налаштування мережі

Для правильного функціонування мережі, потрібно налаштувати усі пристрої.

```
R-8-2-Server(config)#int fa0/0
R-8-2-Server(config-if)#ip addr 172.8.10.1 255.255.255.192
R-8-2-Server(config-if)#no sh
R-8-2-Server(config-if)#exit
R-8-2-Server(config)#int se6/1
R-8-2-Server(config-if)#ip addr 172.8.10.66 255.255.255.252
R-8-2-Server(config-if)#no sh
R-8-2-Server(config-if)#exit
R-8-2-Server(config)#
*Jun 25 17:40:47.543: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun 25 17:40:47.743: %LINK-3-UPDOWN: Interface Serial6/1, changed state to up
*Jun 25 17:40:48.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R-8-2-Server(config)#
*Jun 25 17:40:48.751: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial6/1, changed state to up
```

Рисунок 3.1 – Приклад налаштування адресації маршрутизатора

```
R-8-2-Server(config)#router ospf 2
R-8-2-Server(config-router)#network 172.8.10.0 0.0.0.63 area 0
R-8-2-Server(config-router)#network 172.8.10.64 0.0.0.3 area 0
R-8-2-Server(config-router)#exit
R-8-2-Server(config)#
```

Рисунок 3. 2 – Приклад налаштування маршрутизації

```
R-8-2-1(config)#enable secret strongpass99
R-8-2-1(config)#service password-encryption
R-8-2-1(config)#no service password-recovery
Password recovery disable mode is not supported by the current ROMMON.
Please upgrade the ROMMON if you want to use this feature.

R-8-2-1(config)#username admin privilege 15 secret adminpass99
R-8-2-1(config)#username technic privilege 7 secret techpass88
R-8-2-1(config)#
R-8-2-1(config)#line console 0
R-8-2-1(config-line)#password conpass88
R-8-2-1(config-line)#login
R-8-2-1(config-line)#exit
R-8-2-1(config)#
R-8-2-1(config)#line vty 0 4
R-8-2-1(config-line)#password vtypass77
R-8-2-1(config-line)#login
R-8-2-1(config-line)#transport input ssh
R-8-2-1(config-line)#transport output ssh
R-8-2-1(config-line)#exec-timeout 60 0
R-8-2-1(config-line)#exit
R-8-2-1(config)#
```

Рисунок 3.3 – Приклад налаштування паролів, локальної аутентифікації та паролів на лініях

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

3.2 Встановлення і налаштування Active Directory

Далі налаштовуємо Active Directory для централізованого управління обліковими записами користувачів і комп'ютерів, забезпечення безпеки, контролю доступу до ресурсів мережі, автоматизації адміністративних задач та покращення загальної ефективності і керованості ІТ-інфраструктури.

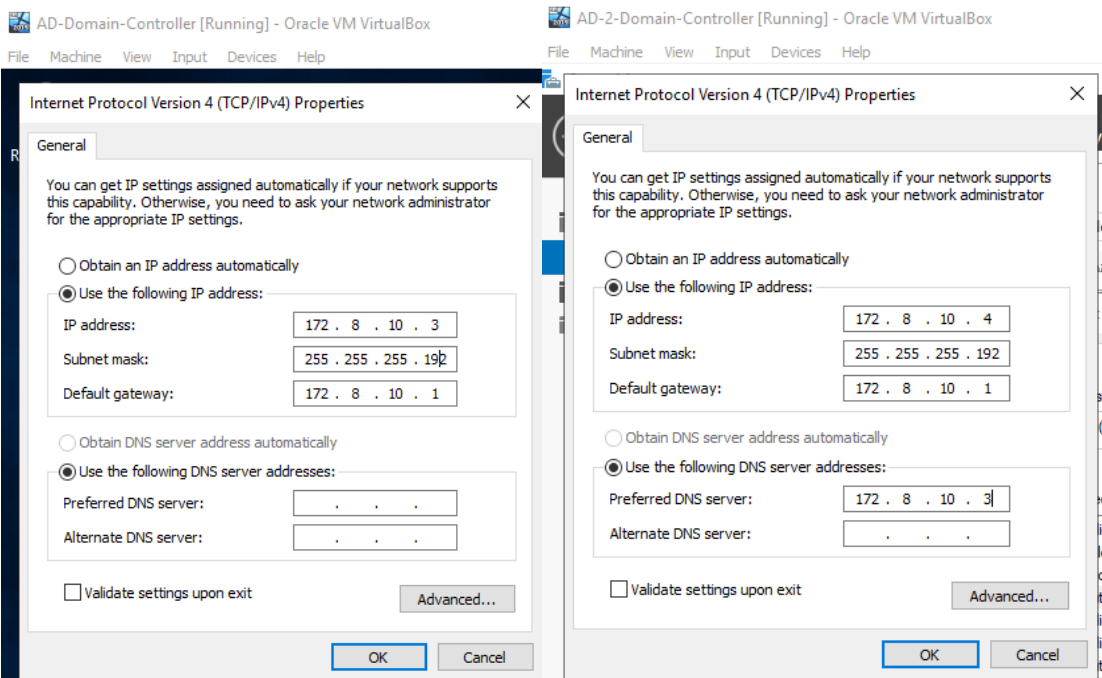


Рисунок 3.4 – Налаштування адресації контролерів домену

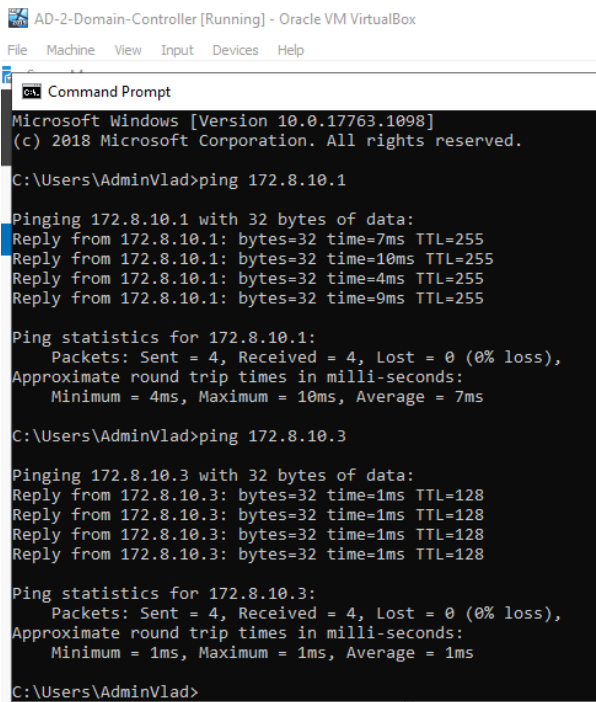


Рисунок 3.5 – Перевірка зв'язку

Встановлення та налаштування служб AD є важливим для централізованого управління обліковими записами користувачів і комп'ютерів. Це забезпечує єдиний точку аутентифікації та дозволяє адміністраторам керувати доступом до ресурсів мережі. Крім того, AD спрощує автоматизацію адміністративних задач, таких як призначення прав доступу, розгортання програмного забезпечення та оновлень, а також підтримує політики безпеки і забезпечує цілісність та захист даних. Це значно підвищує ефективність і керованість IT-інфраструктури організації.

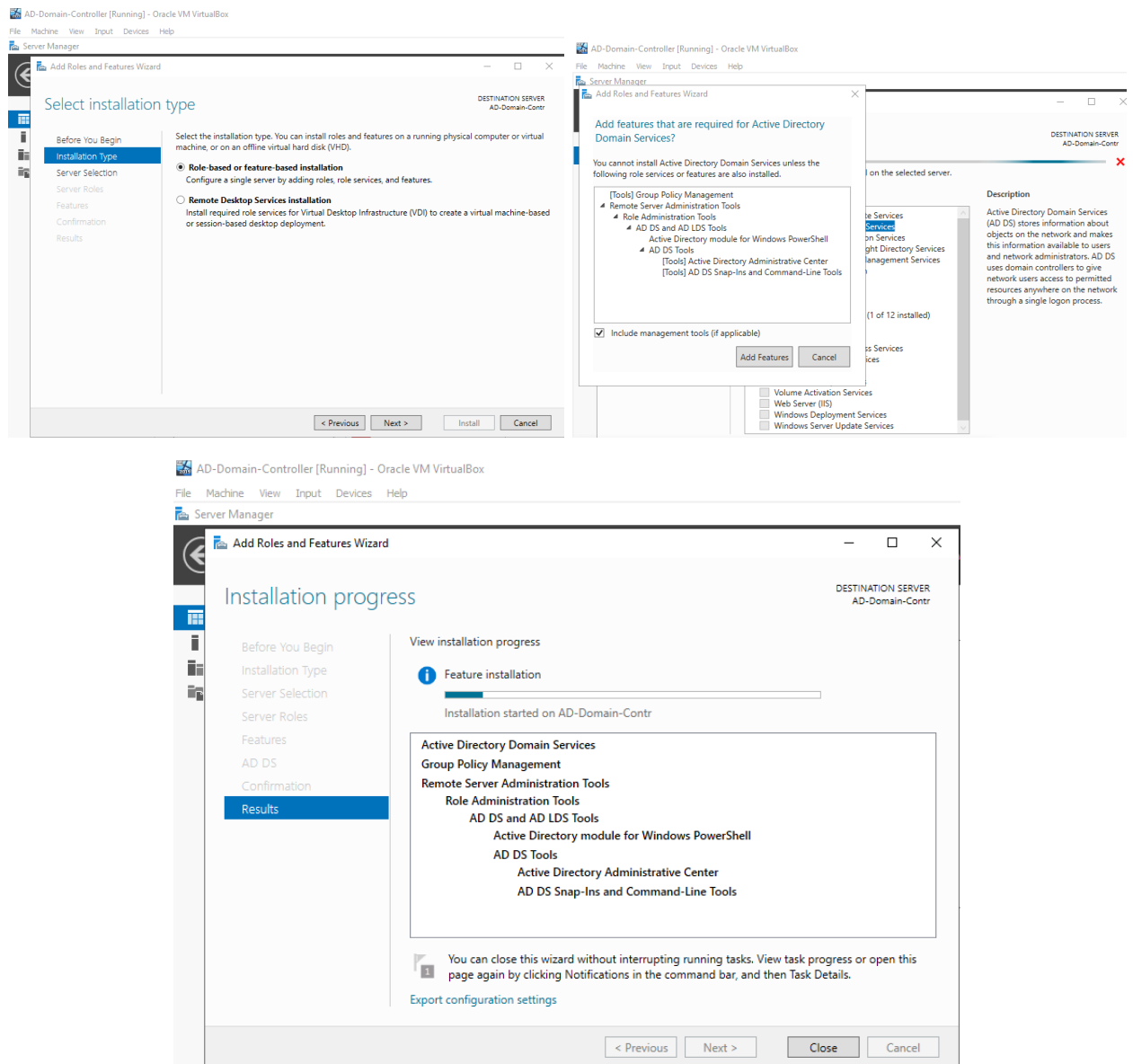


Рисунок 3.6 – Встановлення необхідних служб на 1 контролер домену

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

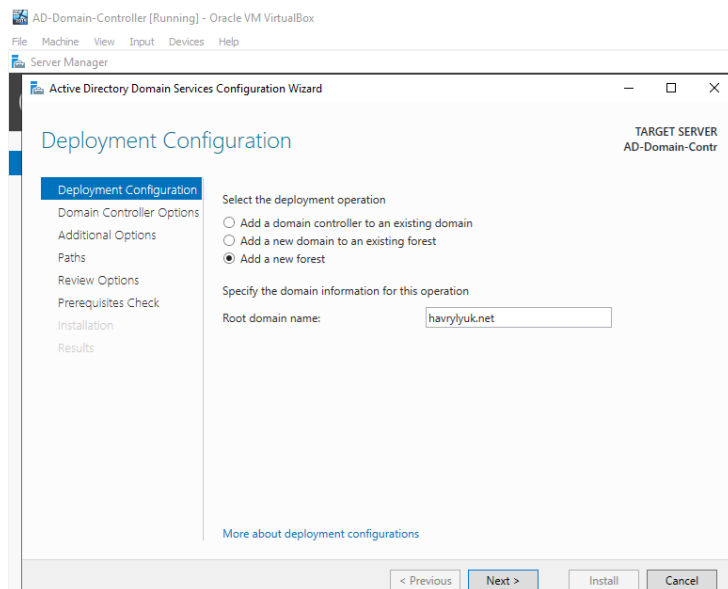


Рисунок 3.7 – Створення нового домену

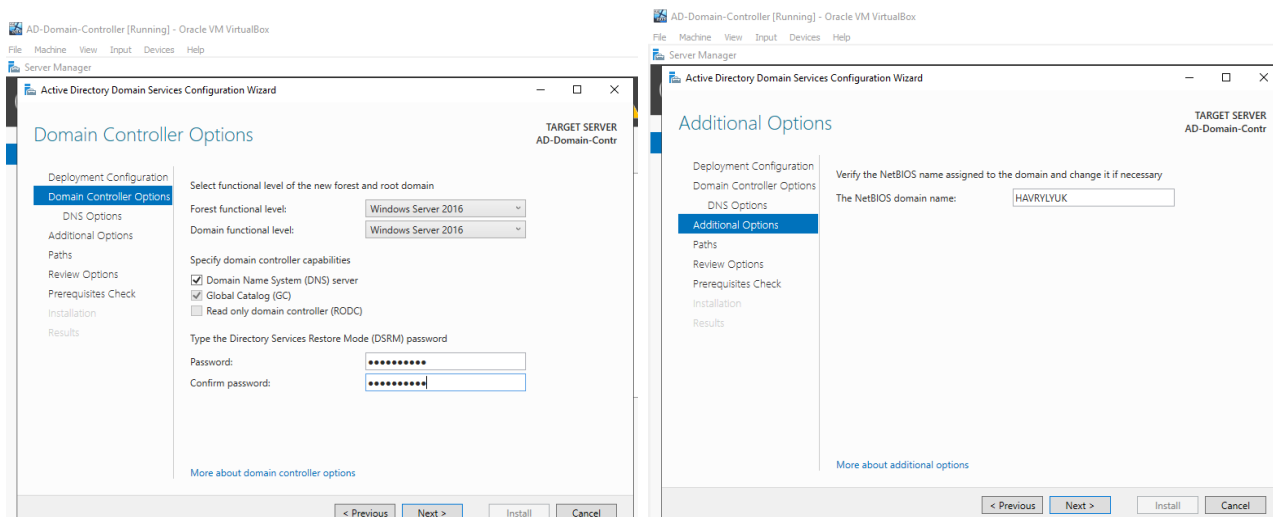


Рисунок 3.8 – Процес налаштування домену

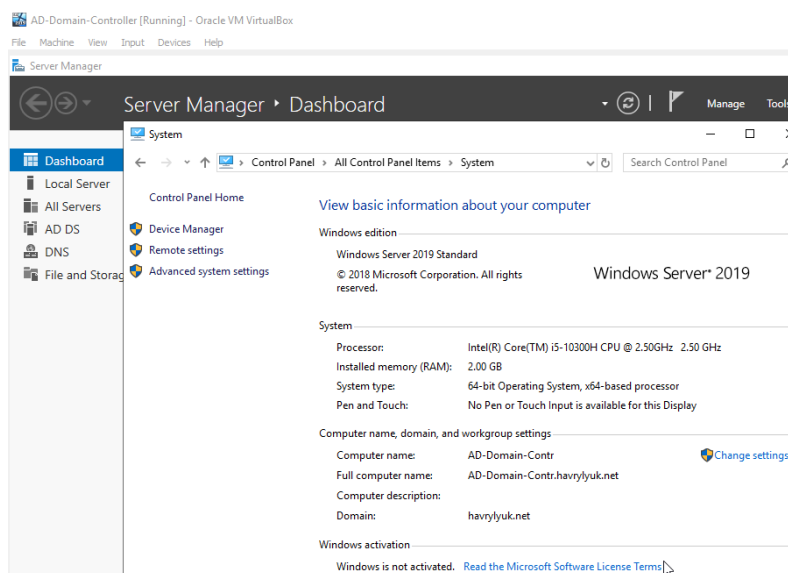


Рисунок 3.9 – Перевірка

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

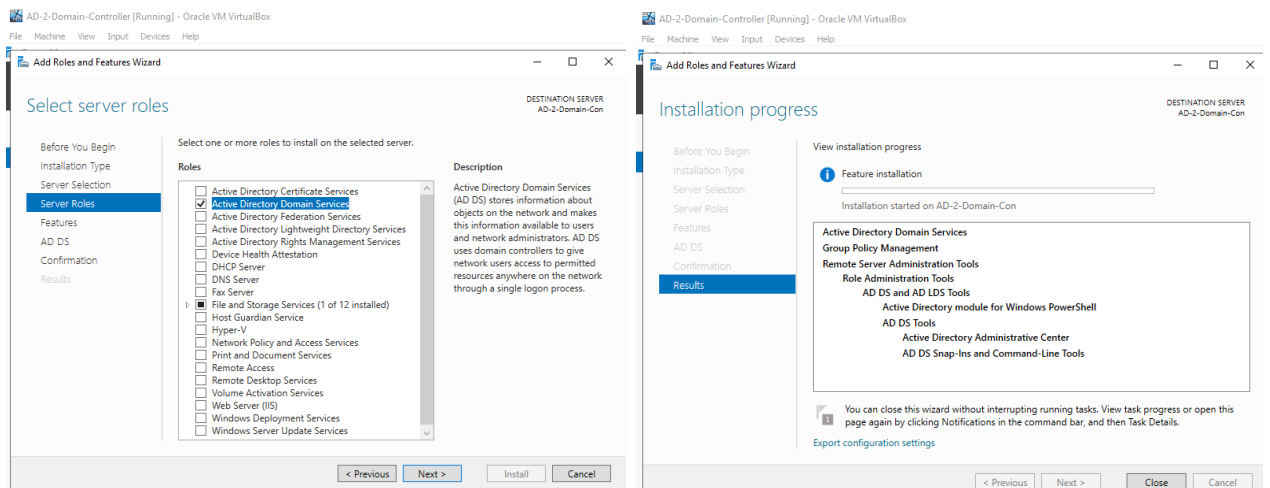


Рисунок 3.10 – Встановлення необхідних служб на 2 контролер домену

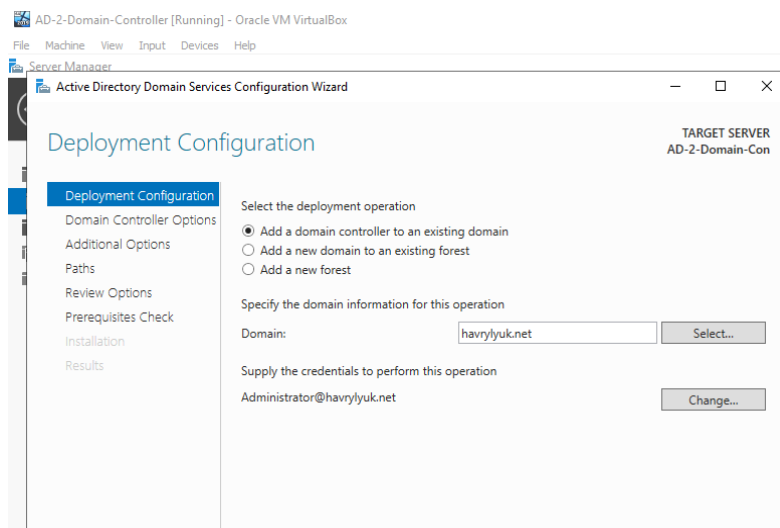


Рисунок 3.11 – Додавання 2 контролеру домену до існуючого домену

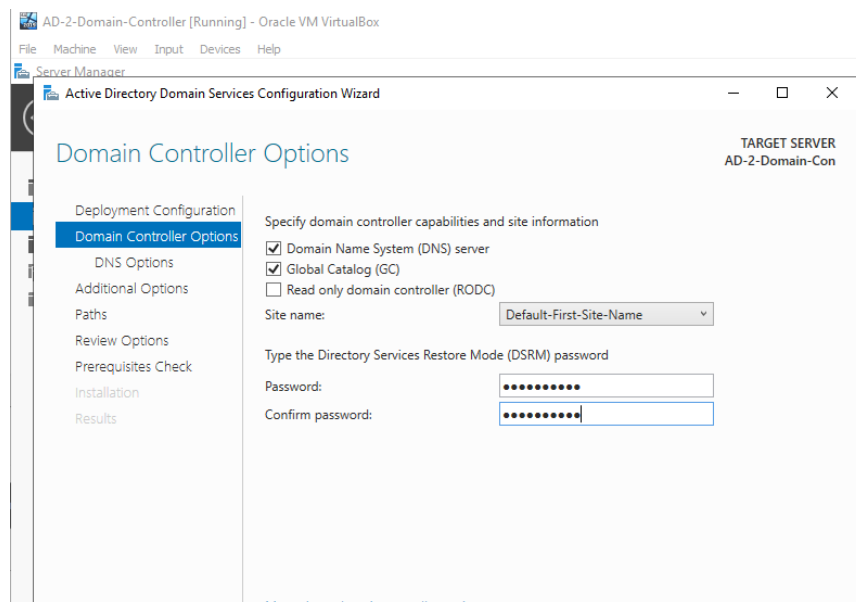


Рисунок 3.12 – Налаштування підключення

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

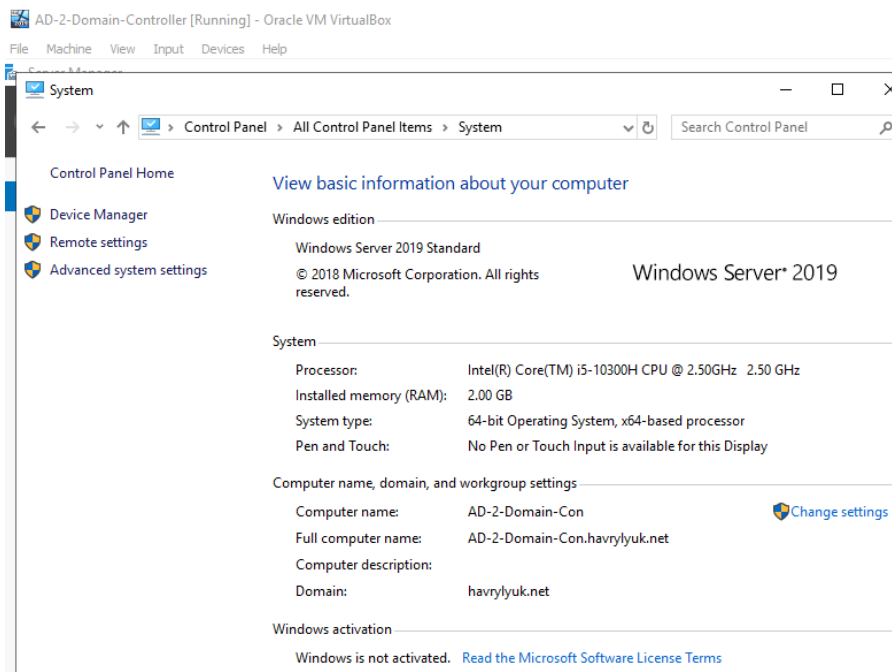


Рисунок 3.13 – Перевірка

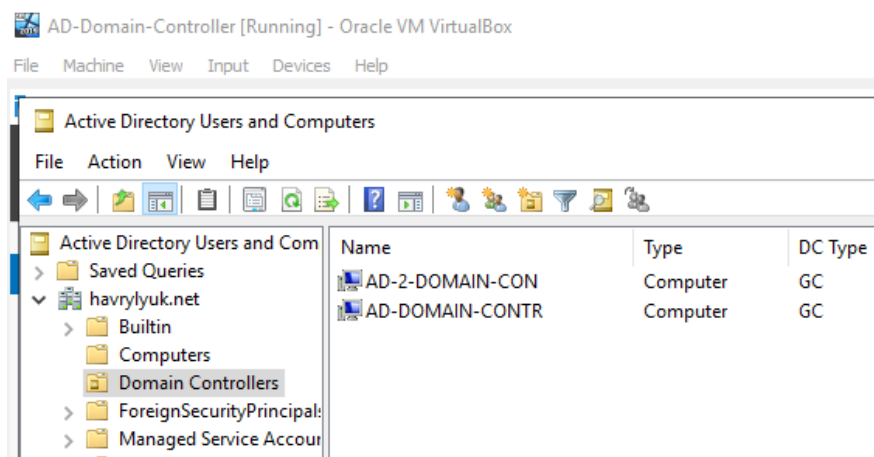


Рисунок 3.14 – Перевірка наявності контролерів

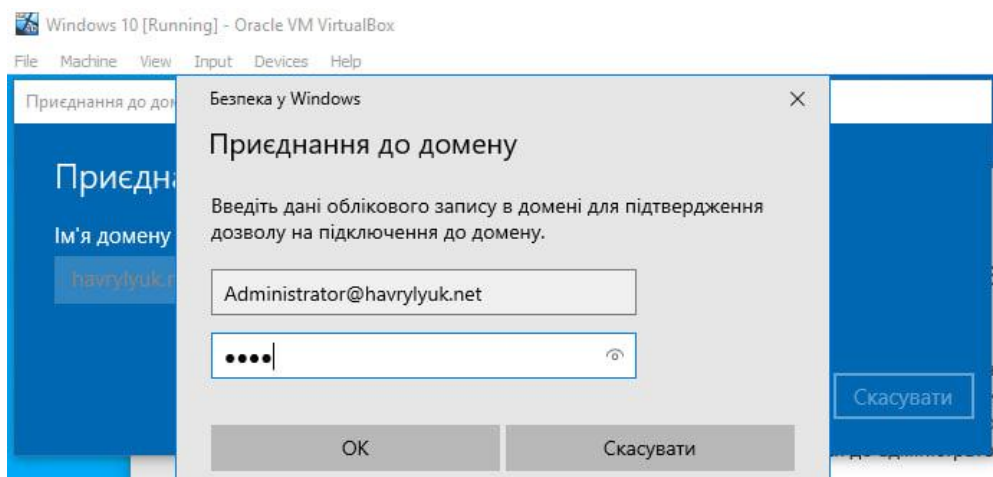
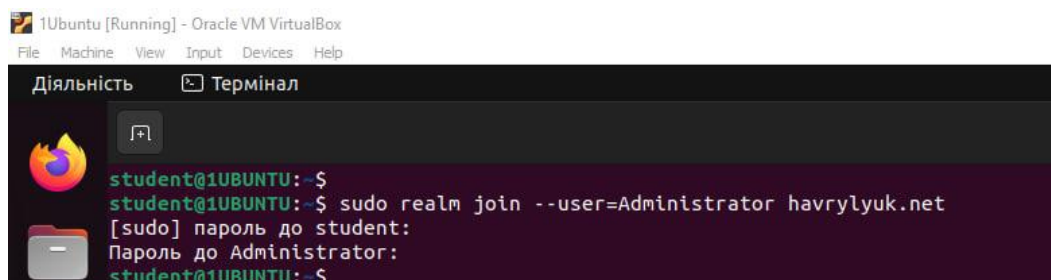
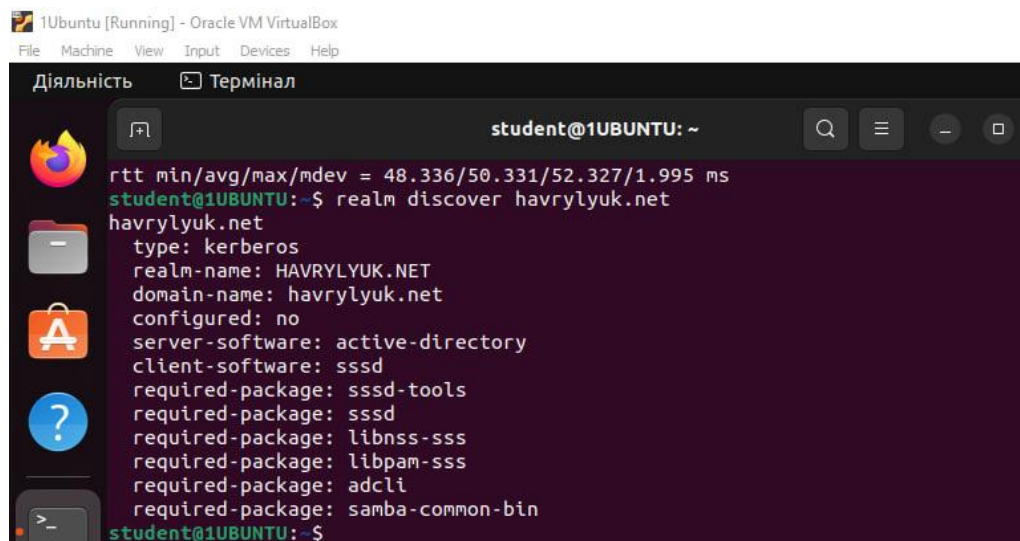
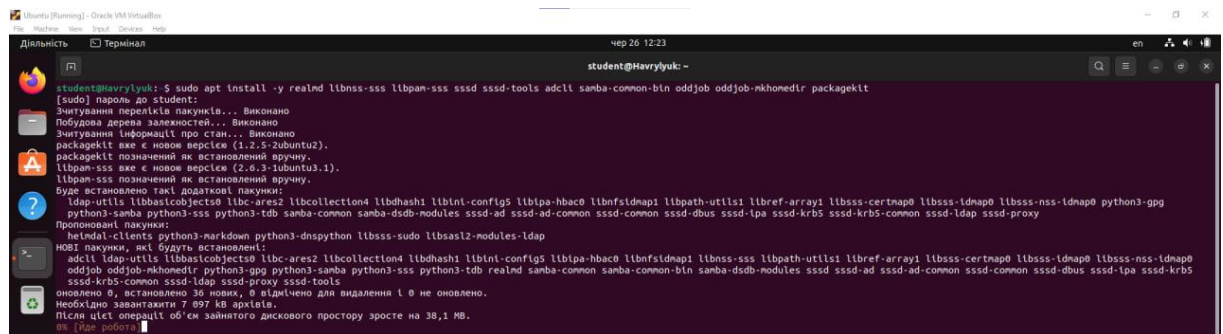
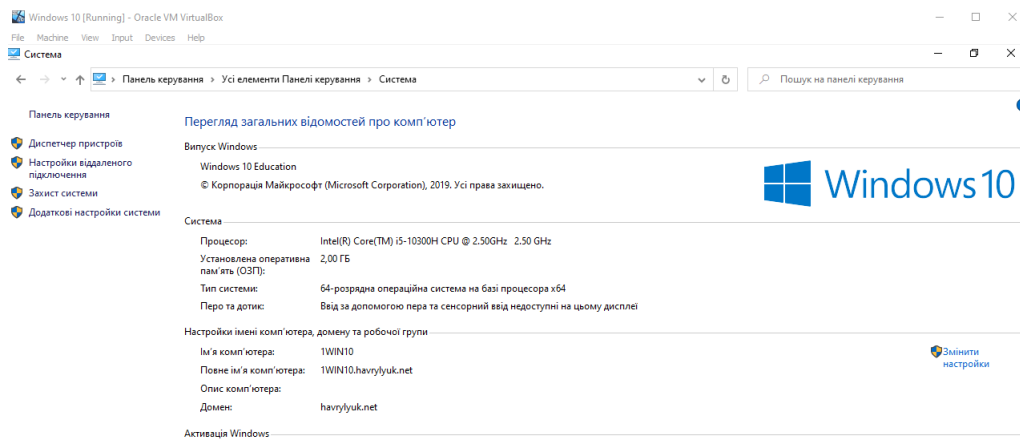


Рисунок 3.15 – Додавання робочої станції Windows до домену

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				68
Змн.	Арк.	№ докум.	Підпис	Дата		



		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковский І.Г.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

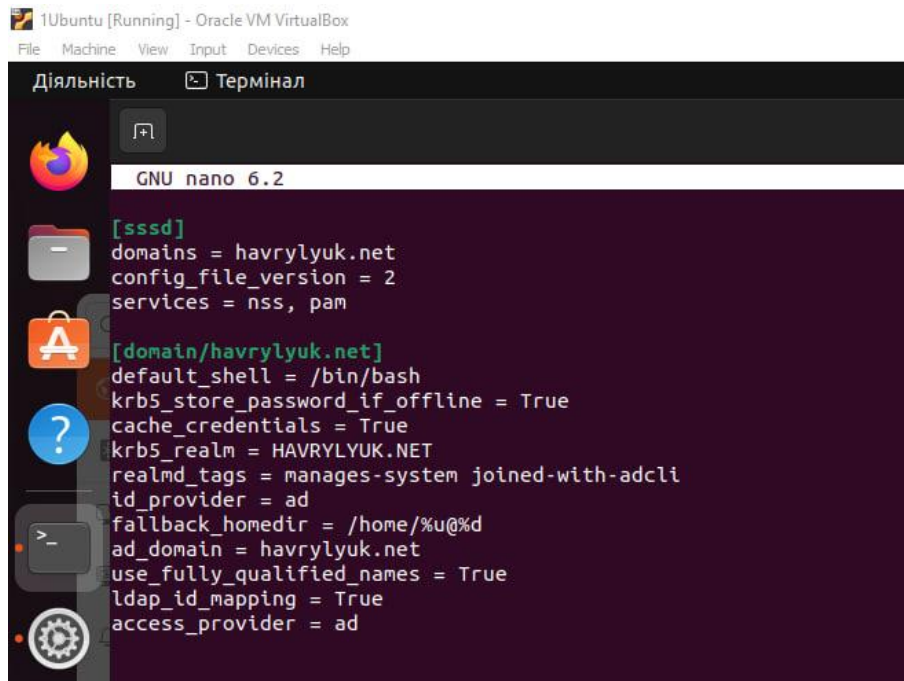


Рисунок 3.20 – Налаштування SSSD (/etc/sss/sss.conf)

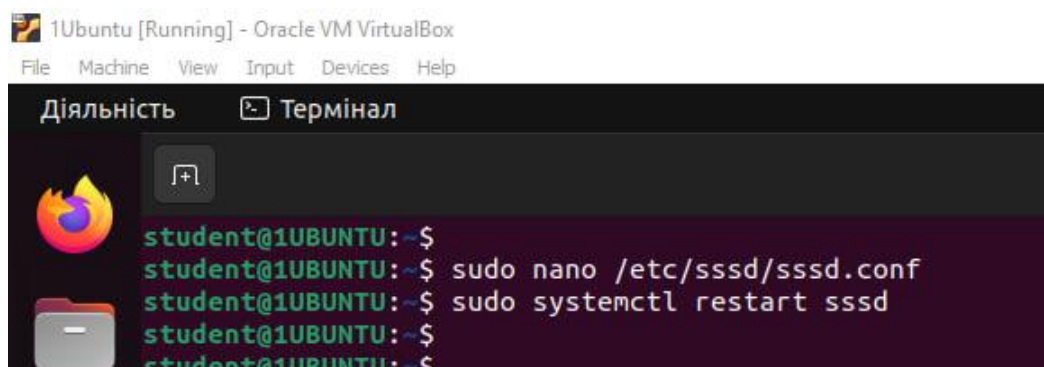


Рисунок 3.21 – Перезапуск служби

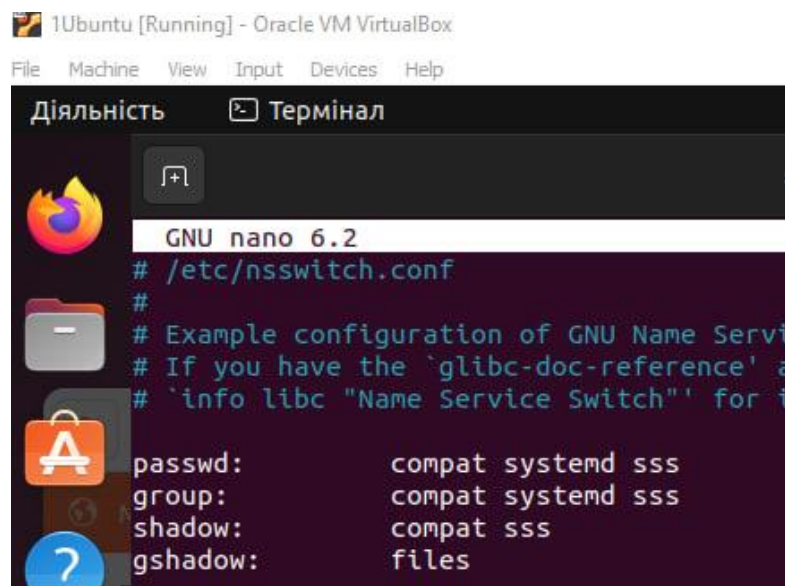


Рисунок 3.22 – Налаштування NSS і PAM (/etc/nsswitch.conf)

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

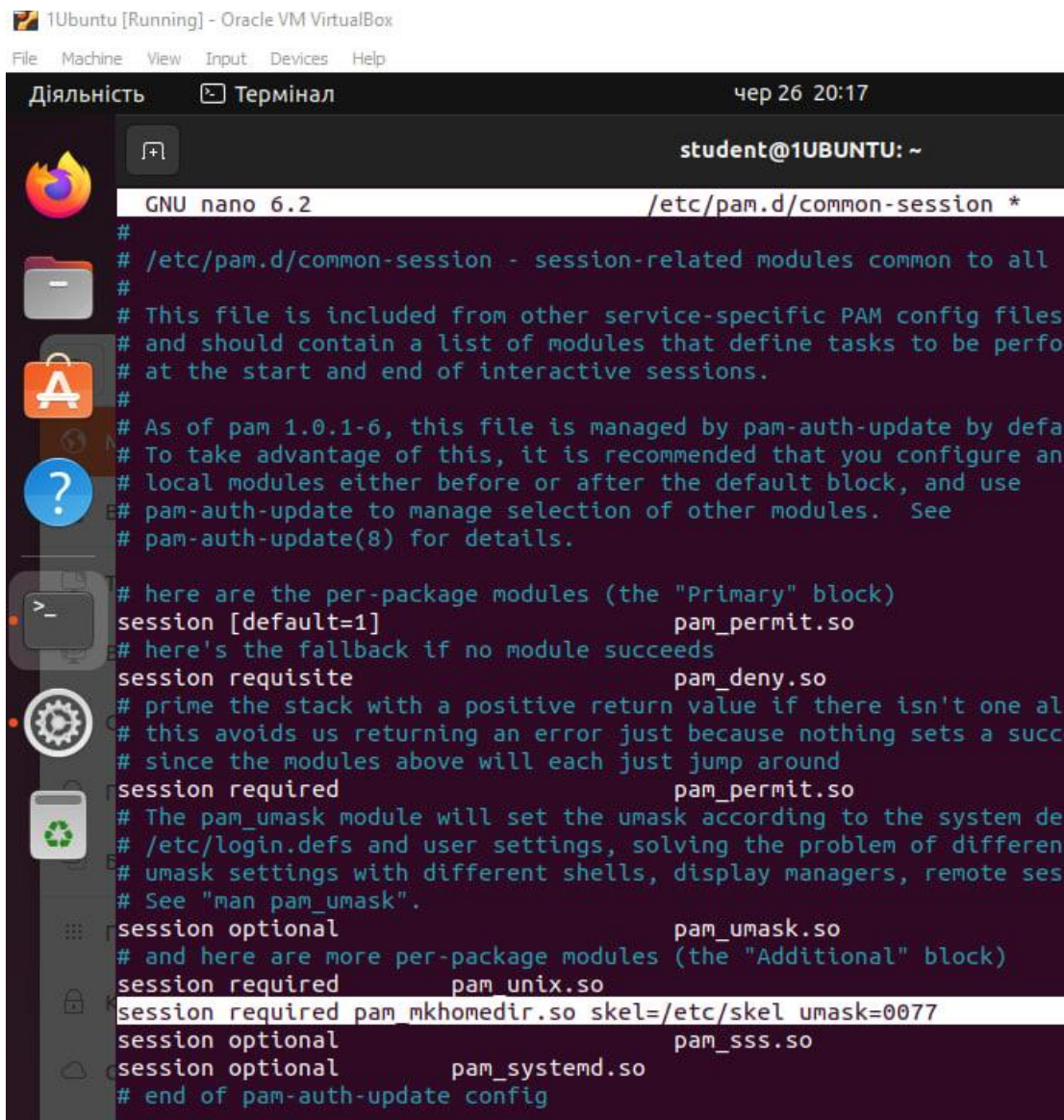


Рисунок 3.23 – Редагування /etc/pam.d/common-session

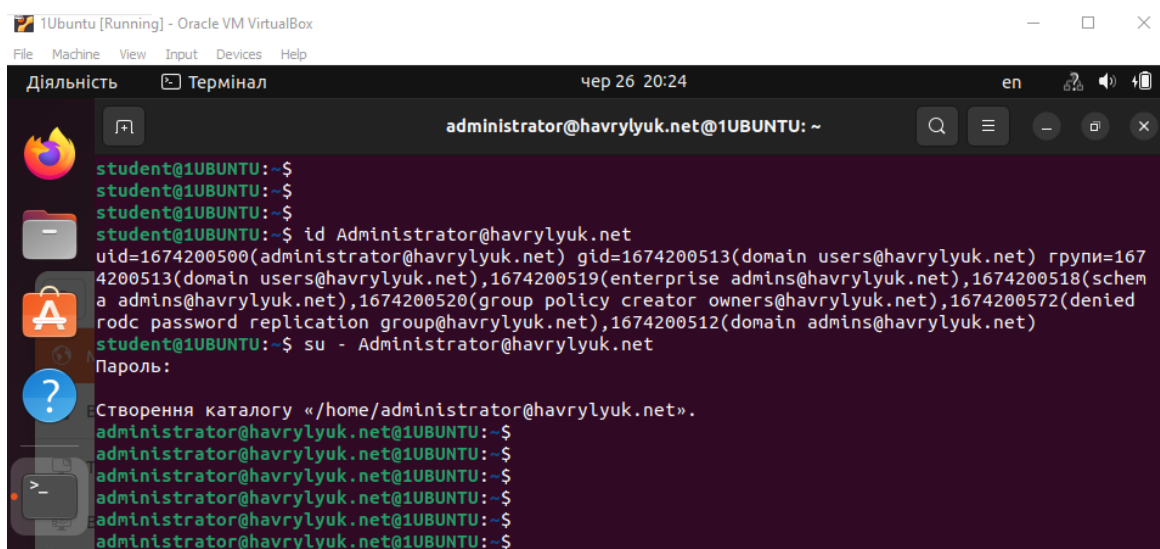


Рисунок 3.24 – Перевірка підключення

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

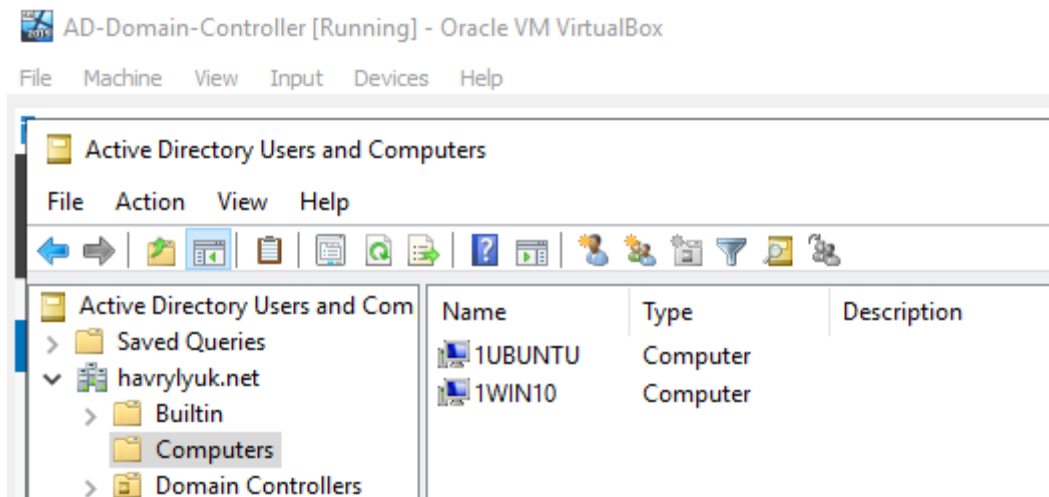


Рисунок 3.25 – Підключені робочі станції до AD

3.3 Проектування доменної структури Active Directory

Добре спроектована доменна структура дозволяє чітко визначити ієрархію та взаємозв'язки між об'єктами, спрощуючи адміністрування та підтримку. Вона допомагає централізовано керувати обліковими записами користувачів, групами, комп'ютерами та іншими ресурсами, а також забезпечує контроль доступу до них. Проектування включає розробку логічної та фізичної структури доменів, організаційних одиниць і сайтів, що дозволяє оптимізувати процеси автентифікації та реплікації даних. Крім того, добре продумана структура підвищує рівень безпеки, дозволяючи точно налаштовувати політики безпеки та права доступу, а також спрощує масштабування і модернізацію мережі в майбутньому.

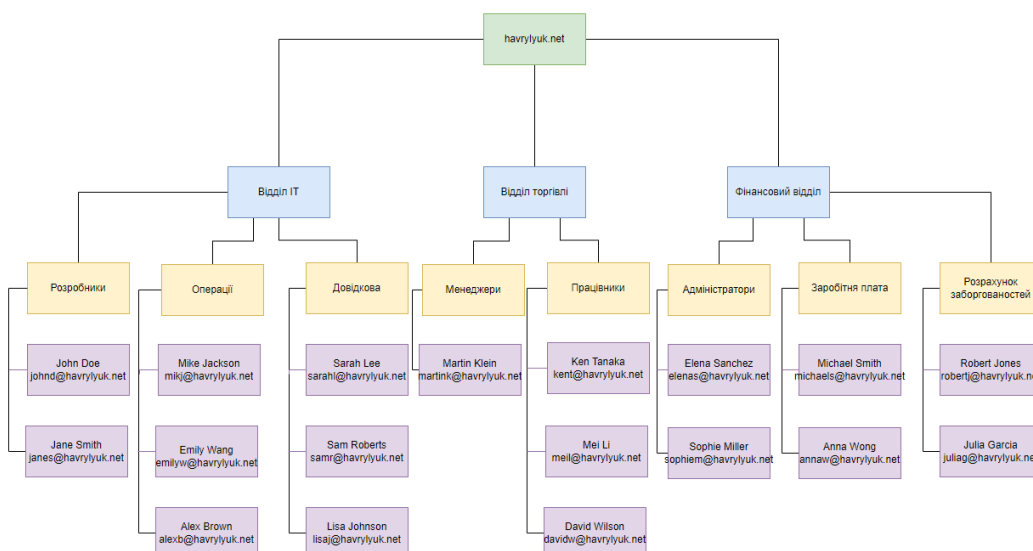


Рисунок 3.26 – Структурна діаграма домену

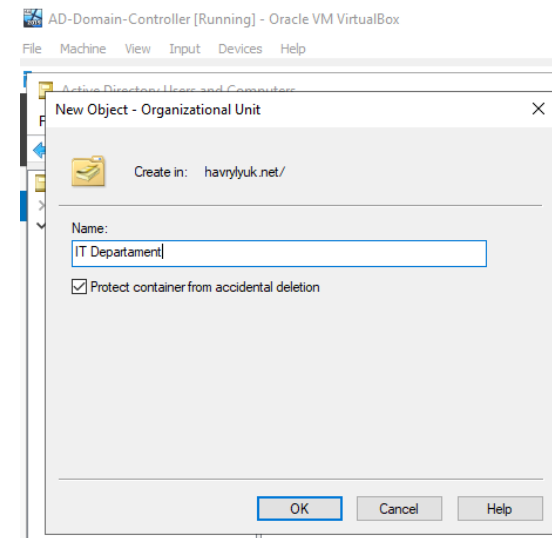


Рисунок 3.27 – Приклад створення організаційної одиниці (відділ)

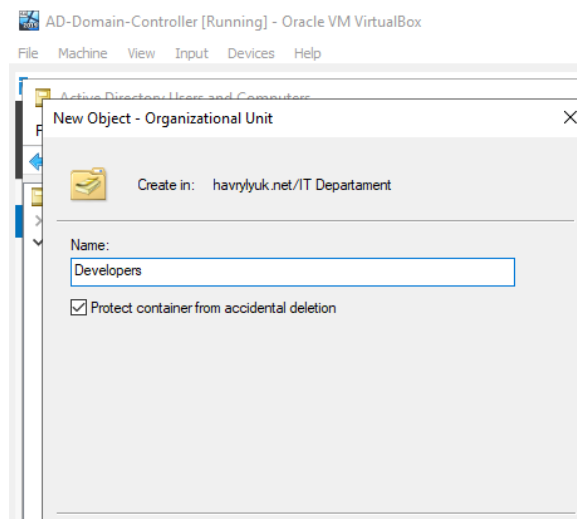


Рисунок 3.28 – Приклад створення організаційної одиниці (підрозділ)

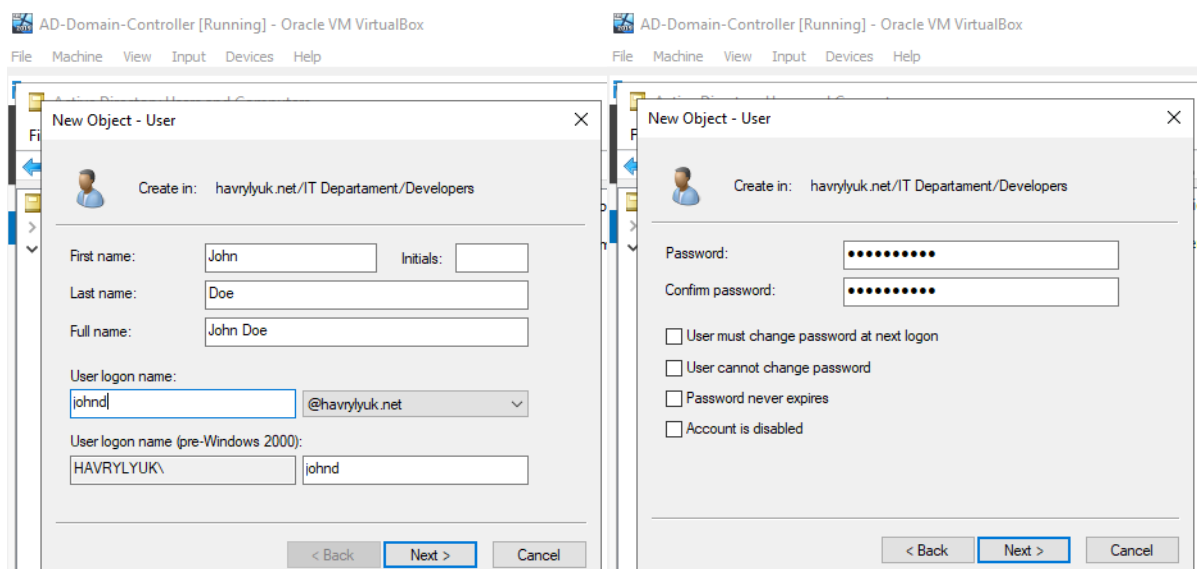


Рисунок 3.29 – Приклад створення користувача

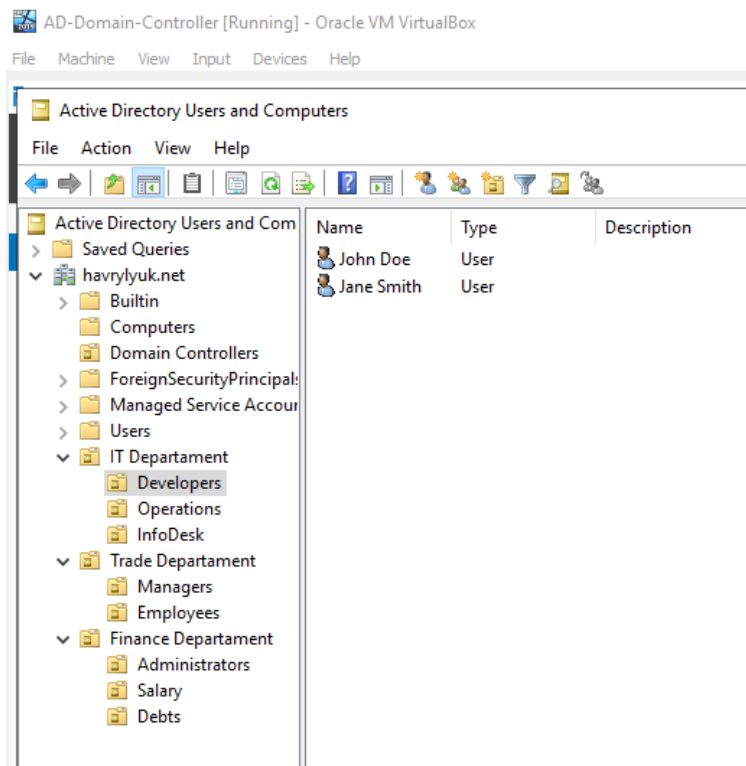


Рисунок 3.30 – Побудована структура

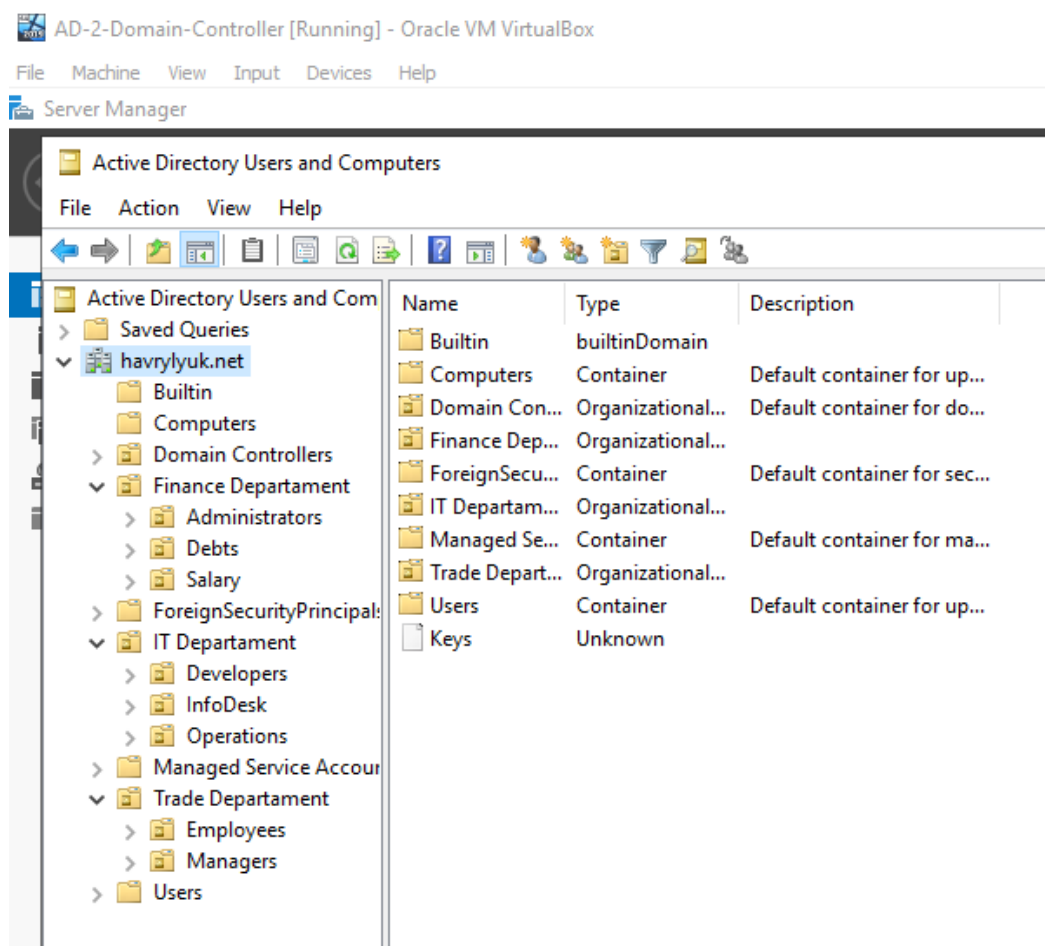


Рисунок 3.31 – Відображення структури на 2 контролері

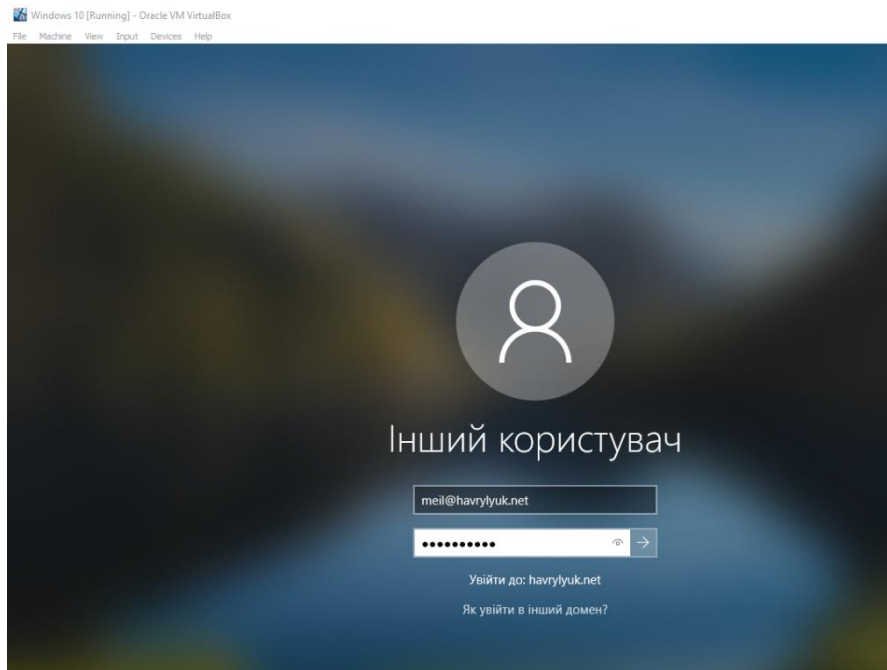


Рисунок 3.32 – Перевірка авторизації (Windows)

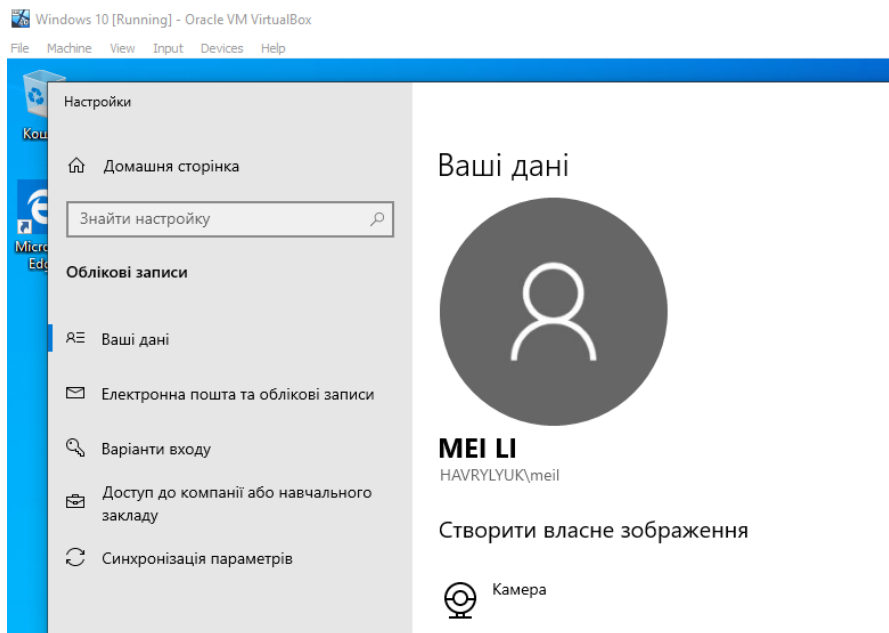


Рисунок 3.33 – Перевірка авторизації (Windows)

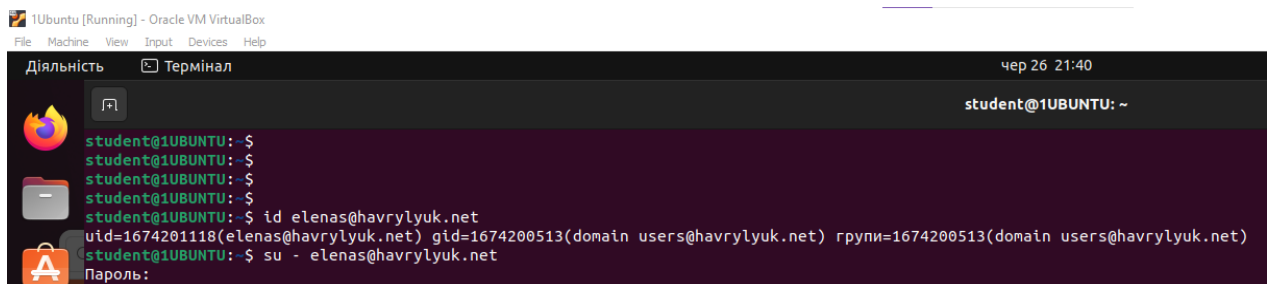


Рисунок 3.34 – Перевірка доступності

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

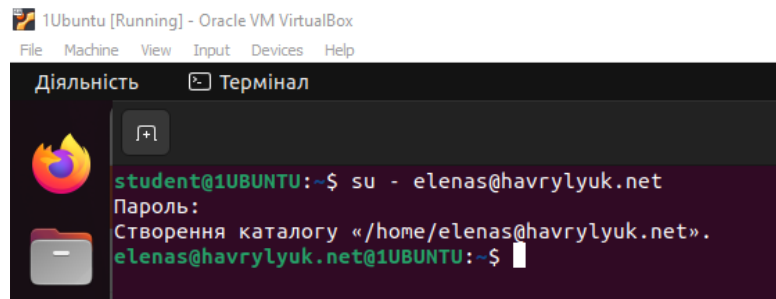


Рисунок 3.35 – Перевірка авторизації (Ubuntu)

Реплікація це важлива функція для забезпечення надійності і доступності даних в облачних сервісах, мережевих системах, базах даних та інших ІТ-системах. Вона дозволяє забезпечити резервне копіювання даних, швидку відновлюваність після аварій, розподіл навантаження між серверами та забезпечення безперебійної роботи систем під час ремонтних робіт чи обслуговування.

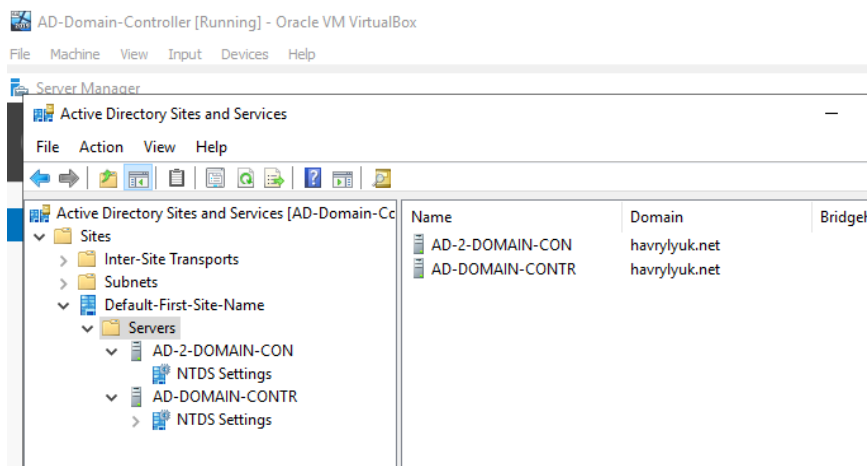


Рисунок 3.36 – Перевірка налаштувань реплікацій

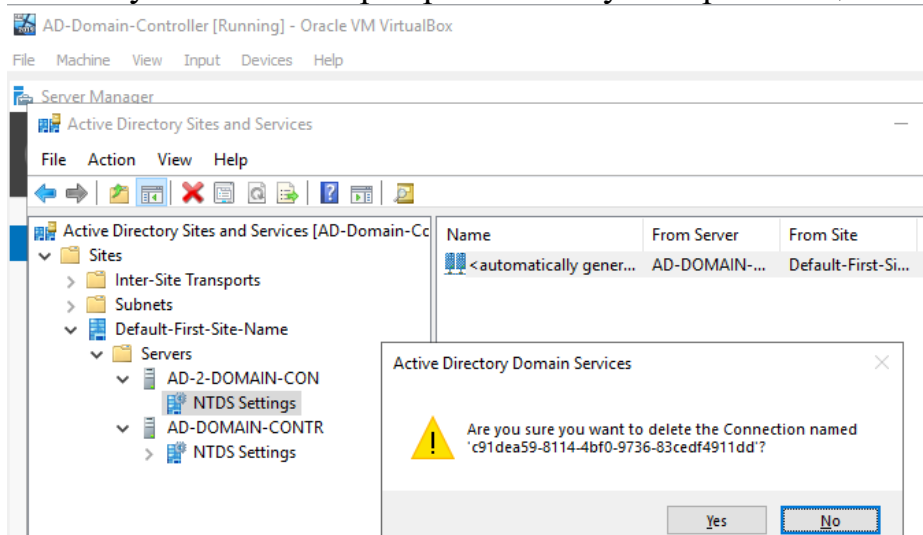


Рисунок 3.37 – Видалення з'єднань

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

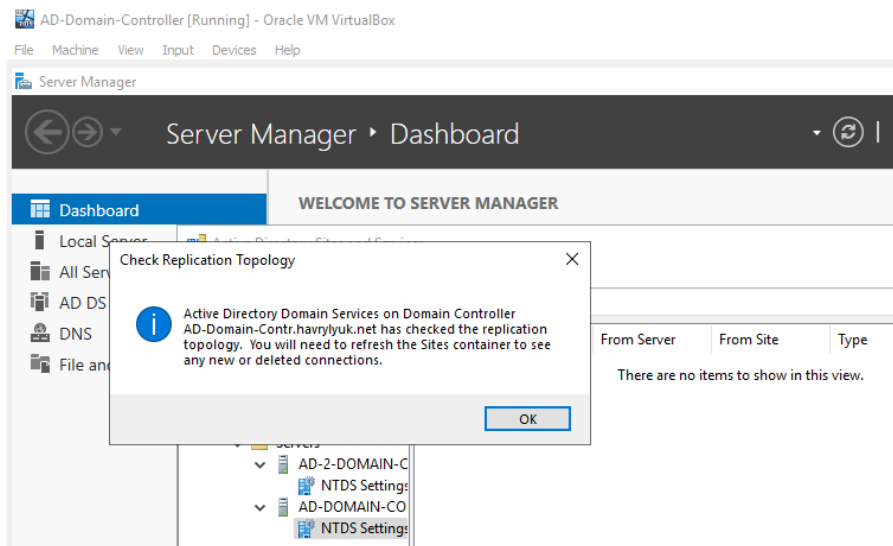


Рисунок 3.38 – Примусова перевірка з'єднань

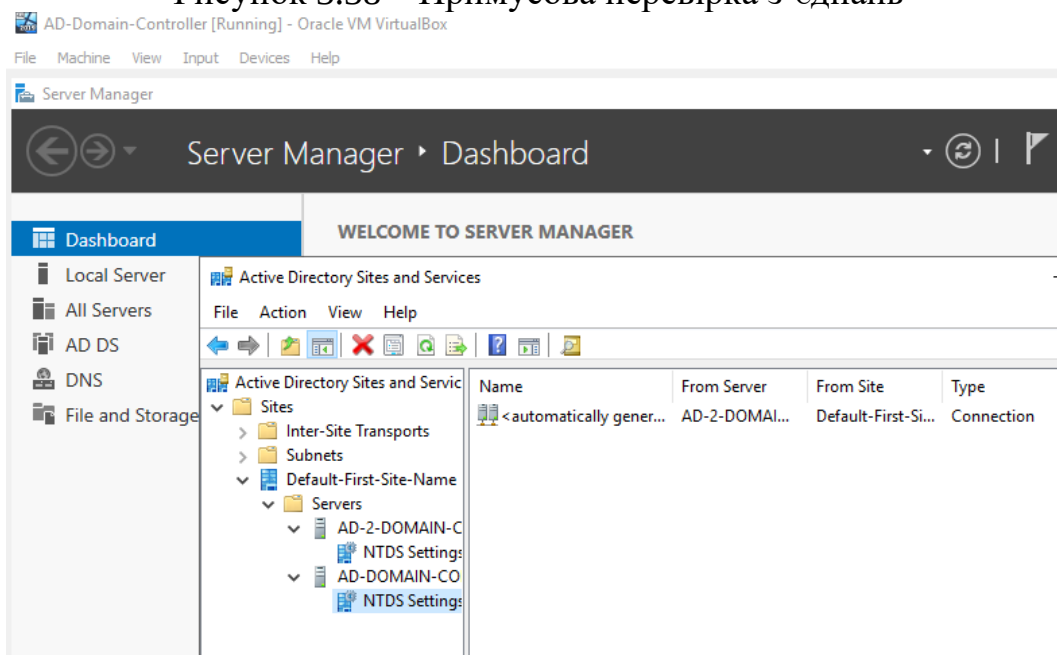


Рисунок 3.39 – Результати перевірки

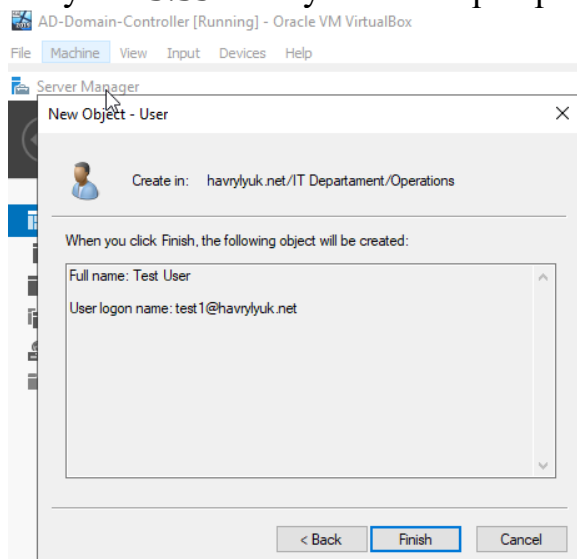


Рисунок 3.40 – Створення тестового користувача

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

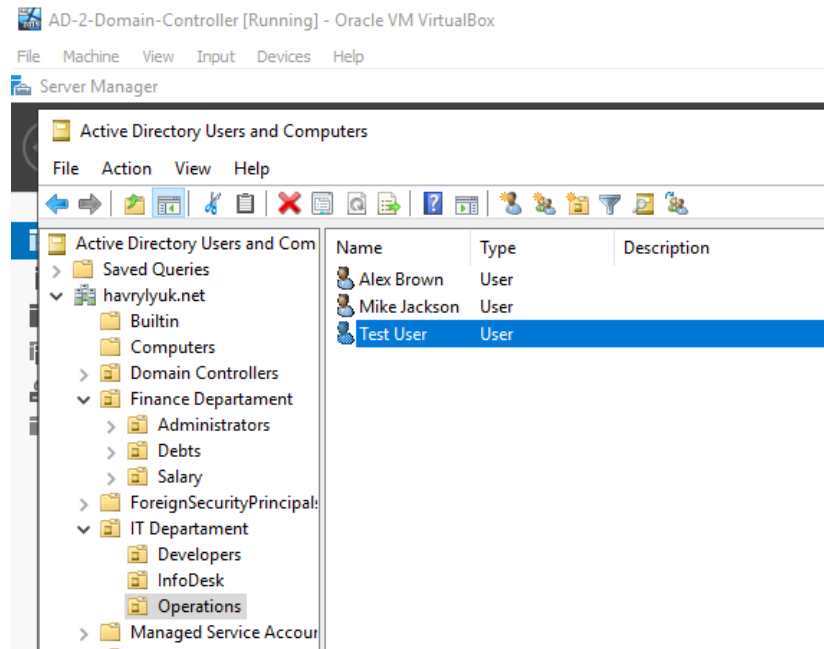


Рисунок 3.41 – Перевірка (користувач відображається на 2 контролері)

DNS - це система, що використовується в Інтернеті для перетворення людських читабельних доменних імен на числові IP-адреси, які використовуються комп'ютерами для ідентифікації вузлів у мережі. DNS є основною складовою інфраструктури Інтернету, що дозволяє ефективною пересилання даних і взаємодію між комп'ютерами та іншими пристроями у мережі.

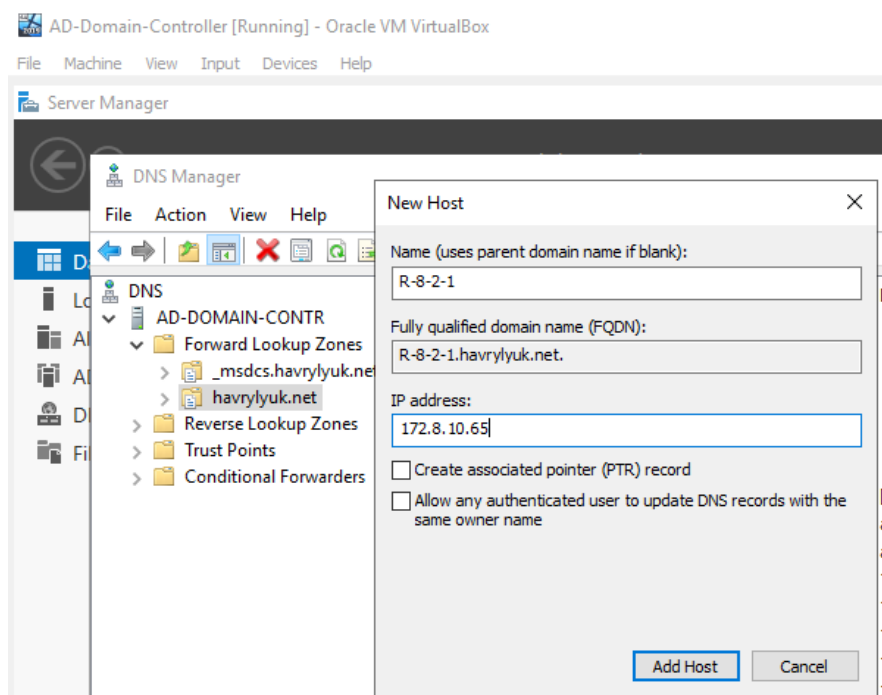


Рисунок 3. 42 – Приклад додавання DNS записів

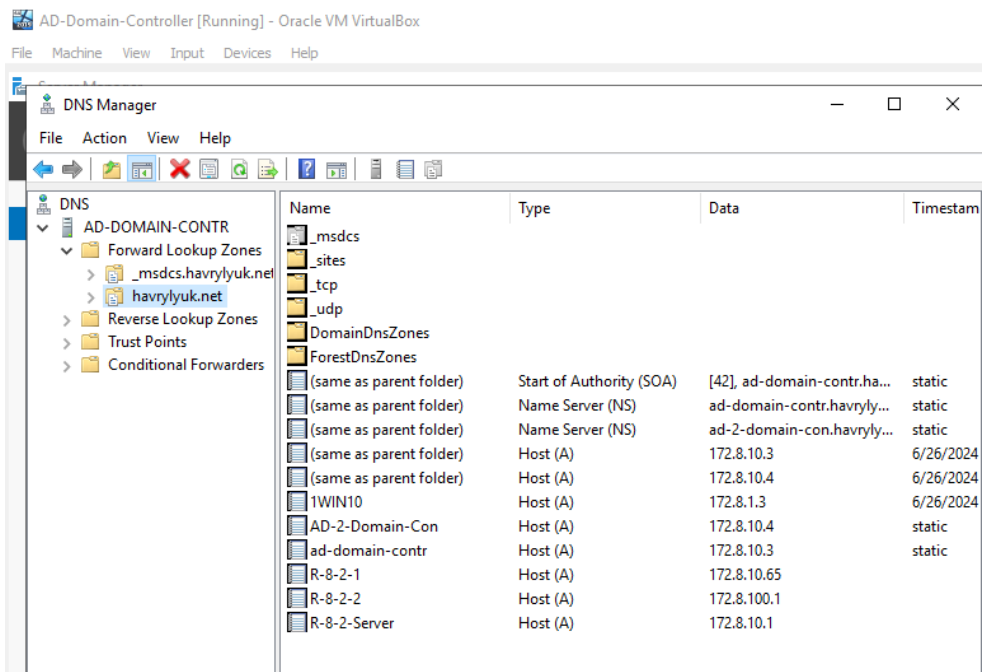


Рисунок 3.43 – Додані записи

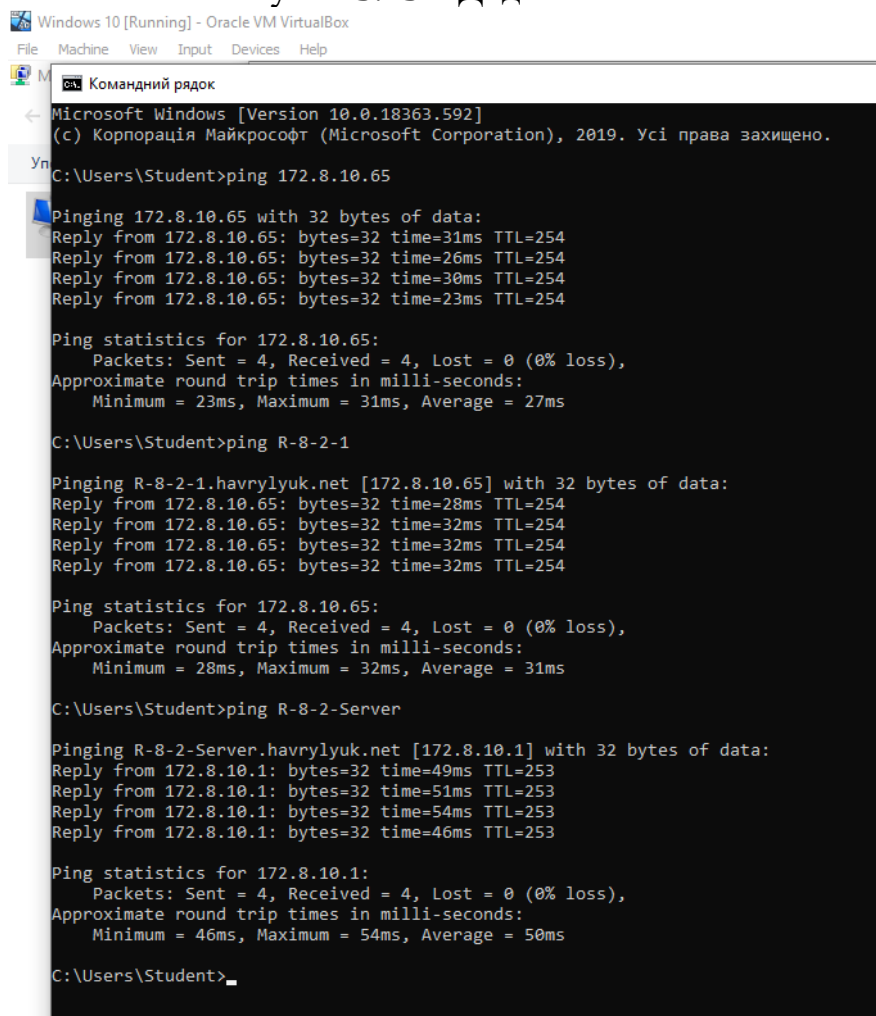


Рисунок 3.44 – Перевірка працездатності

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

Додавання принтера в середовище AD є корисним, оскільки це дозволяє централізовано керувати доступом до принтерів і спрощує їхнє адміністрування. Завдяки інтеграції з AD, принтери можуть бути автоматично виявлені та налаштовані на клієнтських комп'ютерах, що значно знижує навантаження на IT-відділ. Адміністратори можуть використовувати групові політики для керування доступом до принтерів, забезпечуючи, що тільки певні користувачі або групи можуть ними користуватися. Це також полегшує моніторинг і аудит використання принтерів, підвищуючи загальну безпеку та ефективність мережі.

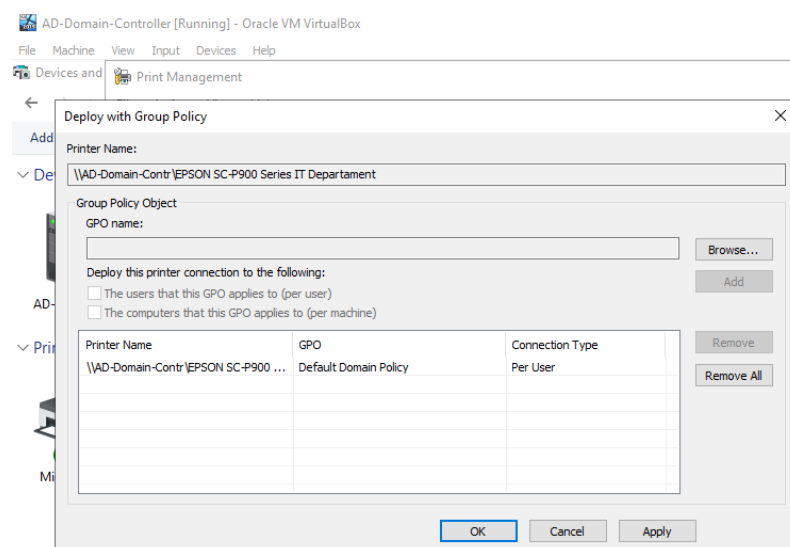


Рисунок 3.45 – Приклад додавання принтера в домен та налаштування політики

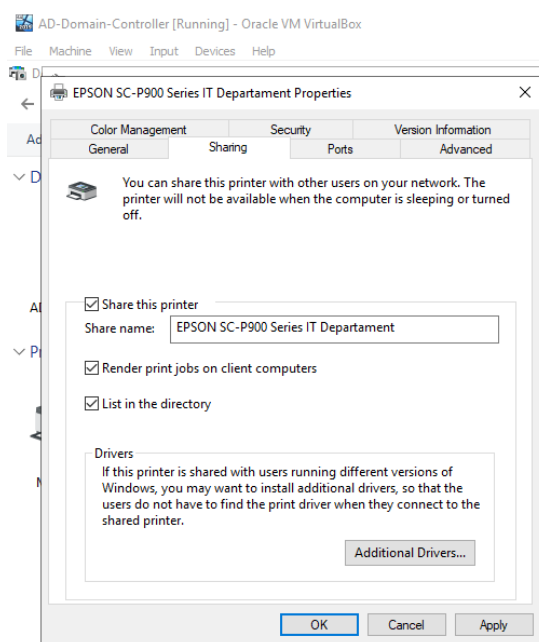


Рисунок 3.46 – Приклад налаштування спільного доступу до принтера

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

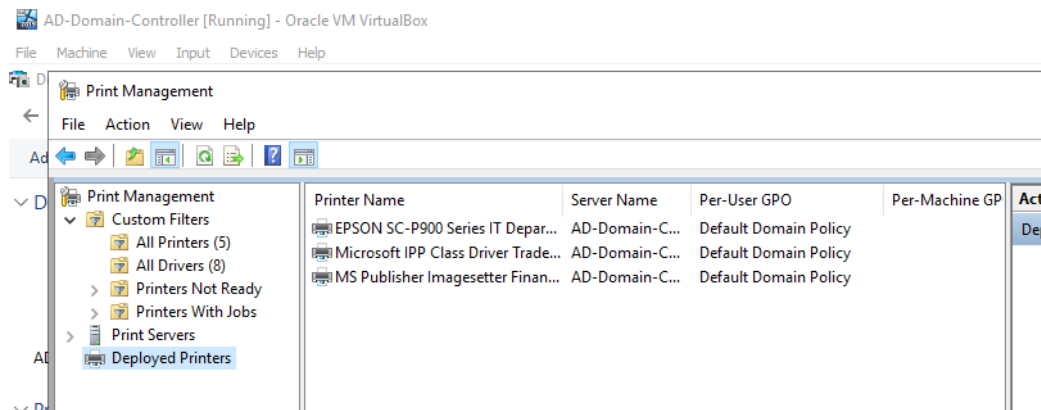


Рисунок 3.47 – Готові до використання принтери

Групові політики безпеки дозволяють забезпечити стандартизацію і контроль за поведінкою користувачів і комп'ютерів в мережі. Для всіх користувачів встановлено автоматичне блокування екрану після 10 хвилин простою та автоматичне встановлення оновлень щоп'ятниці. Відділ ІТ має адміністративний доступ до конкретного принтера, паролі довжиною 12 символів з терміном дії 90 днів. Іншим співробітникам відділу ІТ також надано доступ до принтера, їхні паролі також мають довжину 12 символів і термін дії 90 днів, але заборонено доступ до панелі керування. У відділу торгівлі всі користувачі мають доступ до конкретного принтера з паролями довжиною 10 символів і терміном дії 60 днів, з обмеженням змін робочого столу. У фінансовому відділі всі користувачі мають доступ до конкретного принтера з паролями довжиною 14 символів і терміном дії 45 днів, при цьому заборонено встановлення програм.

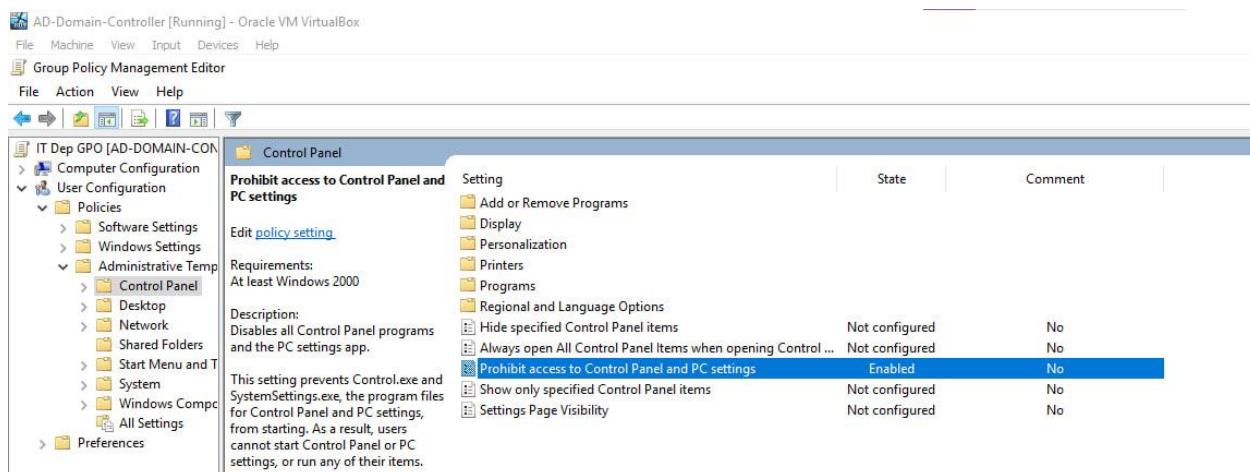


Рисунок 3.48 – Приклад налаштування групової політики

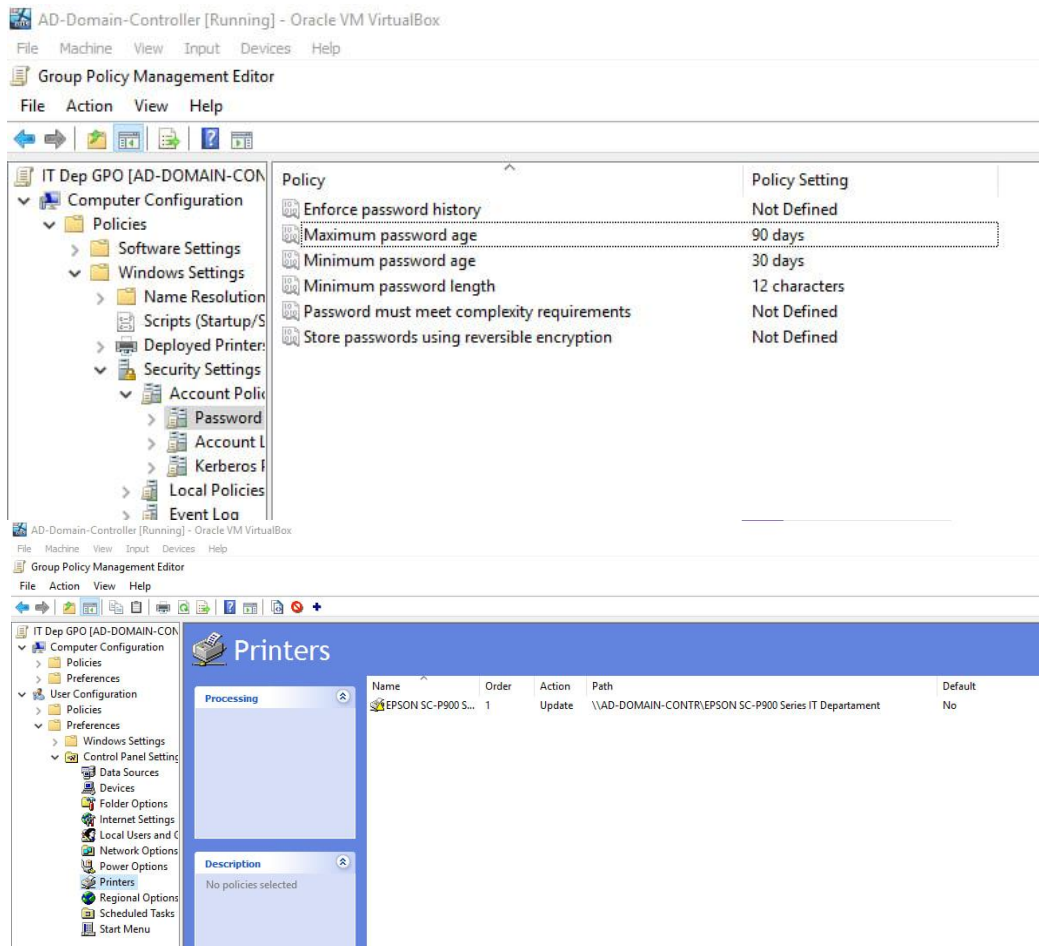


Рисунок 3.49 – Приклад налаштування групової політики

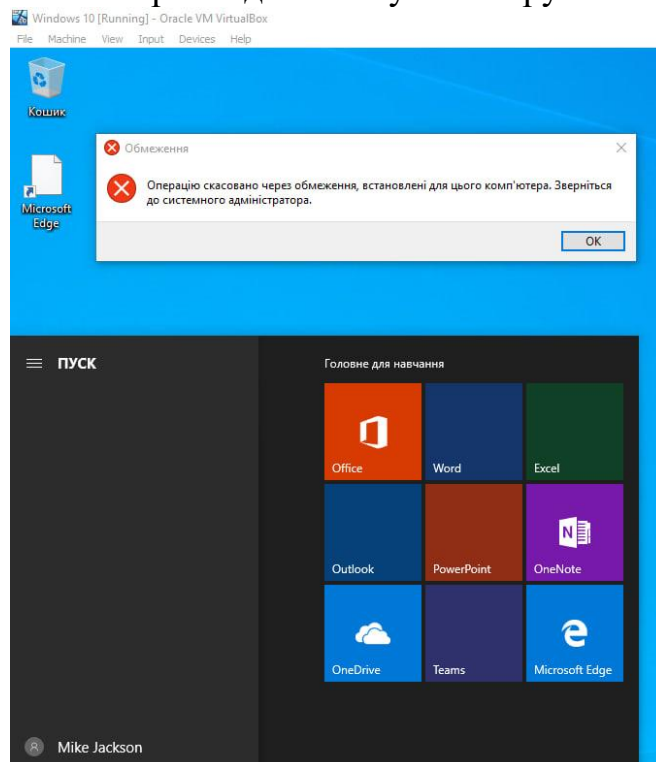


Рисунок 3.50 – Перевірка запуску панелі керування (ІТ відділ, працівник)

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

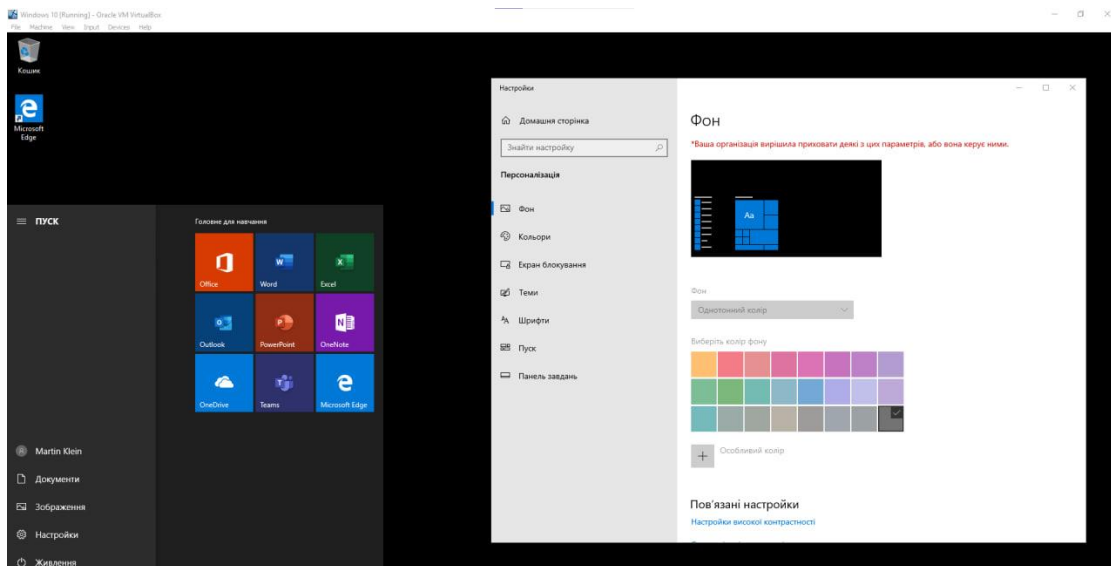


Рисунок 3.51 – Спроба змінити фонове зображення (відділ торгівлі)

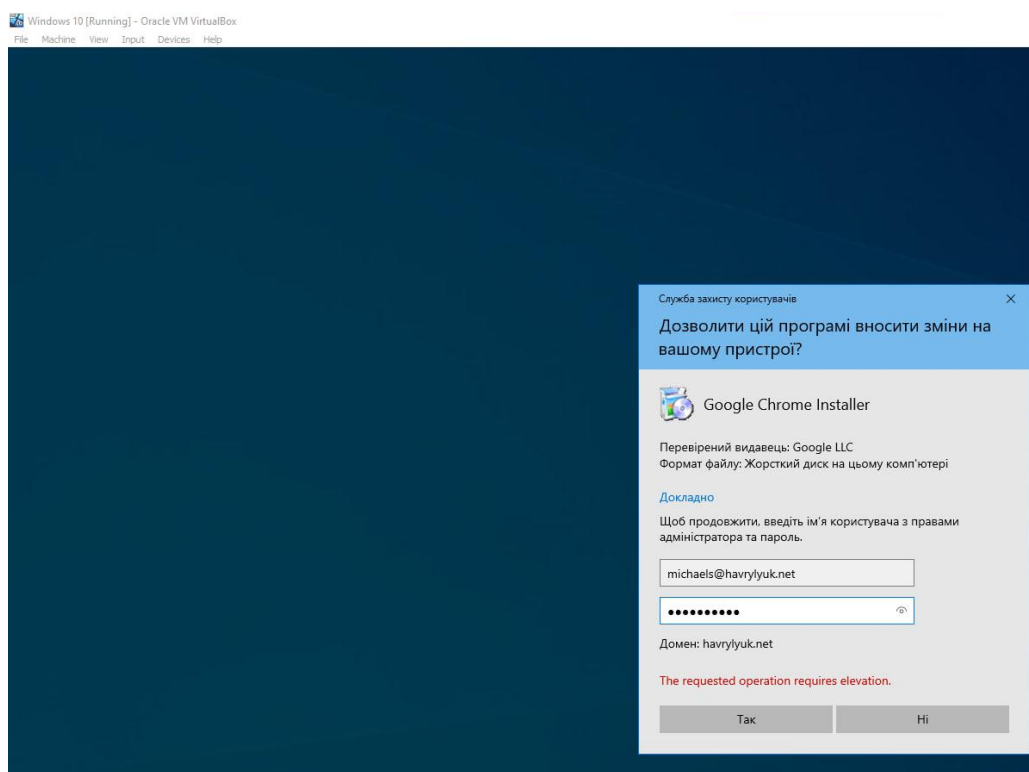


Рисунок 3.52 – Спроба встановити сторонню програму (фінансовий відділ)

3.4 Подальший розвиток

Планування включає впровадження нових політик безпеки та вдосконалення мережеских рішень для забезпечення високого рівня захисту і продуктивності. Однією з ключових ініціатив є впровадження шифрування для конфіденційних файлів, що дозволить захистити важливі дані від несанкціонованого доступу. Також

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

варто реалізувати системи відстеження успішних та невдалих спроб входу в систему, що допоможе швидко виявляти і реагувати на потенційні загрози. Обов'язкове збереження історії браузера для користувачів дозволить здійснювати моніторинг і аналіз інтернет-активності для забезпечення відповідності корпоративним політикам.

Також можна обмежити доступ до корпоративних ресурсів з мобільних пристроїв, які не відповідають політикам безпеки, щоб запобігти можливим витокам даних. Заборона доступу до соціальних мереж під час робочого часу допоможе підвищити продуктивність співробітників і зосередити їхню увагу на виконанні робочих завдань. Автоматичне резервне копіювання важливих документів на мережевий диск забезпечить збереження і відновлення даних у разі аварійних ситуацій. Встановлення проксі-сервера дозволить здійснювати моніторинг і контроль доступу до інтернету, забезпечуючи додатковий рівень захисту і управління трафіком.

Перспективні рішення налаштування мережі включають мережеву сегментацію шляхом створення окремих VLAN для різних відділів і типів трафіку, що дозволить покращити управління і безпеку мережі. Конфігурація брандмауера допоможе забезпечити захист від зовнішніх загроз і несанкціонованого доступу. Використання VPN забезпечить безпечний доступ віддалених співробітників до корпоративних ресурсів. Система виявлення та запобігання вторгненням (IDS/IPS) дозволить своєчасно виявляти і нейтралізувати загрози.

Також варто вдосконалити резервне копіювання для забезпечення збереження критичних даних, впровадити рішення для захисту кінцевих точок від шкідливого програмного забезпечення і кібератак, а також використання протоколу TACACS+ для централізованого контролю доступу до мережевих пристроїв. Ці заходи допоможуть нам створити більш безпечну, надійну і ефективну мережеву інфраструктуру, що відповідає сучасним вимогам та викликам.

Висновки до третього розділу

В ході написання третього розділу було детально розглянуто ключові аспекти налаштування та інтеграції мережевої інфраструктури з використанням технології

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

Active Directory, а також визначено перспективні рішення для подальшого розвитку і забезпечення безпеки ІТ-середовища. Початково, було проведено налаштування самої мережі, включаючи встановлення потрібного обладнання і програмного забезпечення для забезпечення надійності та продуктивності мережевого середовища.

Особлива увага була приділена встановленню і налаштуванню Active Directory, який став основою для централізованого управління обліковими записами користувачів, групами та іншими ресурсами. Цей етап включав розгортання доменного контролера та забезпечення надійності, що покладає основу для ефективного адміністрування та забезпечення безпеки мережі.

Окрема увага була приділена проектуванню доменної структури Active Directory, що включало розробку логічної організації доменів, організаційних одиниць та груп. Цей процес дозволив оптимізувати керування доступом та політиками безпеки, підвищуючи ефективність управління ІТ-середовищем і забезпечуючи відповідність з бізнес-потребами.

Плани на майбутнє включають впровадження рішень, таких як шифрування конфіденційних файлів, відстеження успішних і невдалих спроб входу в систему, обов'язкове збереження історії браузера для користувачів, обмеження доступу до корпоративних ресурсів з мобільних пристроїв, встановлення проксі-сервера для моніторингу та контролю доступу до інтернету. Такі заходи сприятимуть підвищенню захищеності і ефективності мережевої інфраструктури, забезпечуючи відповідь на сучасні виклики і вимоги безпеки.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

ВИСНОВКИ

У кваліфікаційній роботі на тему «Проект захищеної IT-інфраструктури компанії на базі рішень Microsoft Active Directory» було розглянуто теоретичні аспекти створення захищеної IT-інфраструктури, проектування мережі та її реалізацію.

У першому розділі було детально проаналізовано поняття IT-інфраструктури, її основні складові та типи. Було виділено основні вразливості для безпеки IT-інфраструктури та запропоновано методи їх усунення. Особлива увага була приділена принципам побудови IT-інфраструктури на базі служби каталогів Active Directory, можливостям Active Directory для захисту мережних інфраструктур, включаючи множинний фактор аутентифікації (MFA), групові політики, резервне копіювання та відновлення. Проведено аналіз загроз для IT-систем з використанням Active Directory, визначено типові протоколи побудови мережних інфраструктур, вразливості та потенційні ризики, а також загальні рекомендації для захисту мережі.

Другий розділ роботи присвячено проектуванню захищеної IT-інфраструктури на базі Microsoft Active Directory. Було вибрано обладнання, розроблено проект мережі та адресації, а також спроектовано служби та сервіси прикладного рівня. Висновки цього розділу підкреслюють важливість ретельного планування та вибору відповідного обладнання для забезпечення надійного функціонування IT-інфраструктури.

У третьому розділі було здійснено реалізацію та тестування проекту захищеної IT-інфраструктури. Проведено налаштування мережі, встановлення і налаштування Active Directory, проектування доменної структури. Також розглянуто подальші кроки для розвитку IT-інфраструктури. Практична частина роботи підтвердила теоретичні знання і дозволила перевірити ефективність розроблених рішень.

Отже, проведені дослідження та реалізація проекту показали, що використання рішень Microsoft Active Directory дозволяє створити надійну та захищену IT-інфраструктуру, здатну забезпечити високий рівень безпеки та ефективності функціонування корпоративної мережі.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Курс комп'ютерних мереж університету “Житомирська політехніка”
[Електронний ресурс] – Режим доступу:
<https://learn.ztu.edu.ua/course/view.php?id=1890>
2. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч.2 / підг. А. А. Єфіменко. – Житомир: ЖВІ, 2017.
3. Що таке IT-інфраструктура? Основи та Бізнес-кейси. SIM-Networks – Your Goals, our Tech. IT Infrastructure from German Provider. URL: <https://www.sim-networks.com/ukr/blog/it-infrastructure>.
4. IT-інфраструктура. Автоматизація бізнесу - ДА КОМПАНІ - Комплексні рішення. URL: <https://daco.com.ua/services/it-%20infrastructure/>.
5. Що таке CRM-система та як вона працює? | Creatio. No-Code Platform to automate workflows and CRM | Creatio. URL: <https://www.creatio.com/ua/crm/what-is-crm>.
6. Обчислення - IT-Solutions, Україна. IT-Solutions, Україна. URL: <https://it-solutions.ua/it-infrastruktura/fizichna/obchislennya/>.
7. IT-інфраструктура – RCI-Consulting. RCI-Consulting. URL: <https://rci-c.com/technology/it-infrastruktura/>.
8. Як виправити уразливості IT-інфраструктури малого та середнього бізнесу - TechExpert. TechExpert. URL: <https://techexpert.ua/how-improve-infrastructure-it/>.
9. КМ: Лекція 22. Архітектура служби каталогів Active Directory. Інформаційний портал Технічного фахового коледжу. URL: <https://e-tk.lntu.edu.ua/mod/page/view.php?id=3576>.
10. Active Directory forest: What it is and best practices for managing it. The Quest Blog. URL: <https://blog.quest.com/active-directory-forest-what-it-is-and-best-practices-for-managing-it/>.
11. Different types of Trusts in an Active Directory | Zindagi Technologies. Zindagi Technologies | Cloud Solutions | Cybersecurity Services | Managed IT Services

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

| DevOps Services. URL: <https://zindagitech.com/different-types-of-trusts-in-an-active-directory/>.

12. Guidance for securing Microsoft Active Directory services in your organization - ITSM.60.100 - Canadian Centre for Cyber Security. Canadian Centre for Cyber Security. URL: <https://www.cyber.gc.ca/en/guidance/guidance-securing-microsoft-active-directory-services-your-organization-itsm60100>.

13. Vijayan A. What is the Role of Active Directory in Cyber Security?. LinkedIn: Log In or Sign Up. URL: <https://www.linkedin.com/pulse/what-role-active-directory-cyber-security-aswin-vijayan-0kqaf/>.

14. Active Directory. CyberArk. URL: <https://www.cyberark.com/what-is-active-directory/>.

15. Види мережевих атак. prezi.com. URL: <https://prezi.com/p/ey-bl8dsofny/presentation/>.

16. Network Protocols & How They Can Benefit Your Business. CDW.com. URL: <https://www.cdw.com/content/cdw/en/articles/networking/types-of-network-protocols.html>.

17. Goss M. 12 common network protocols and their functions explained | TechTarget. Networking. URL: <https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained>.

18. What is network infrastructure? Design and trends - DriveNets. DriveNets. URL: <https://drivenets.com/resources/education-center/what-is-network-infrastructure/>.

19. CISCO 7600 SERIES [Електронний ресурс] – Режим доступу до ресурсу: <https://циско.com.ua/router/cisco-7600-series>.

20. Комутатор Cisco WS-C2960+24LC-S [Електронний ресурс] – Режим доступу до ресурсу: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24lc-s>.

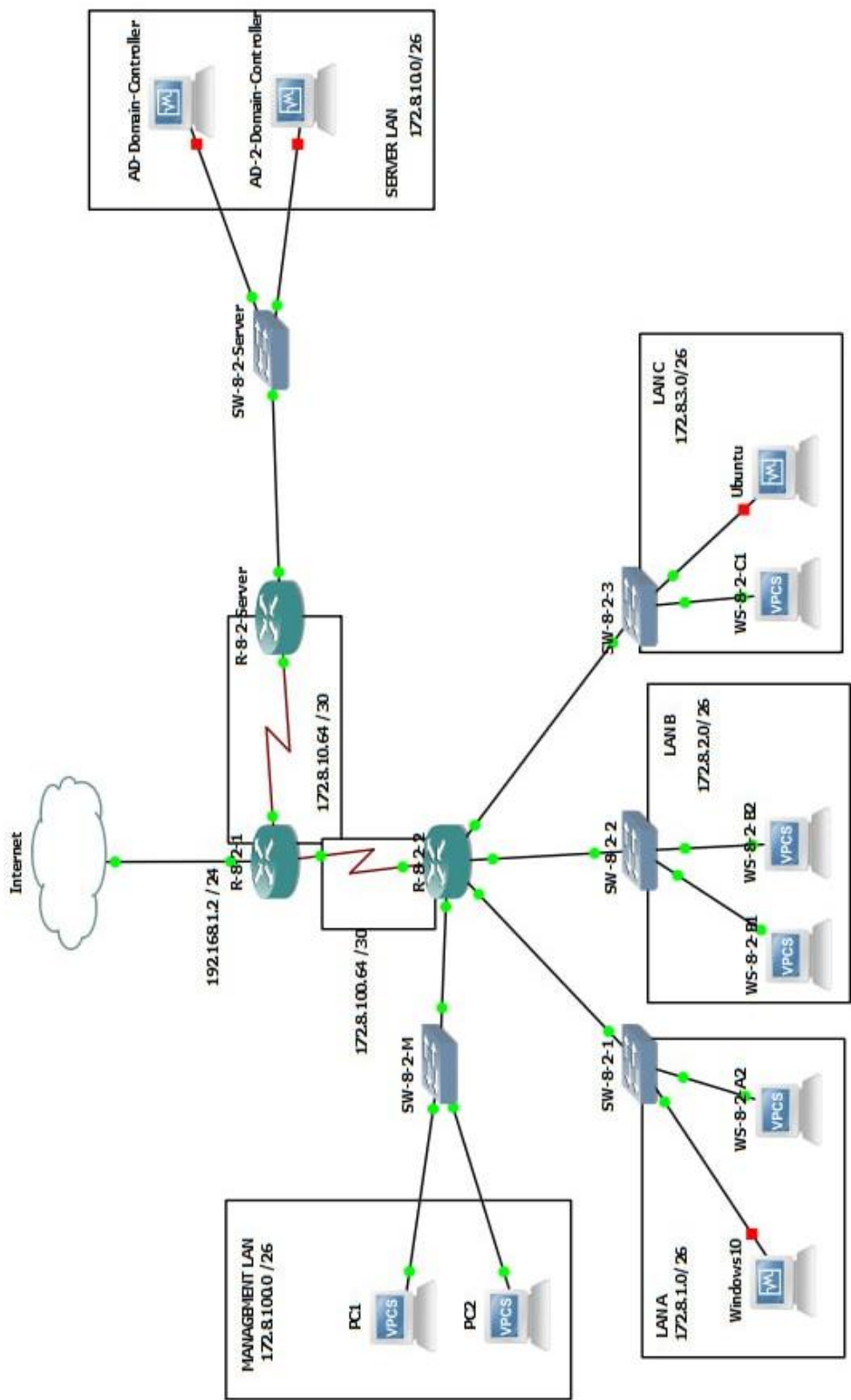
21. Основи IT-інфраструктури: Від А до Я (Частина 1) - HackYourMom. HackYourMom. URL: https://hackyourmom.com/osvita/osnovy-it-infrastruktury-vid-a-do-ya-chastyna-1/#google_vignette.

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

ДОДАТКИ

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

Схема мережі



Технічні характеристики пристроїв

Таблиця 1. Технічні характеристики маршрутизатора CISCO7603S

Розробник:	Cisco
ID:	CISCO7603
Опис:	7603 chassis- Bundles or Configurable Options
Тип:	Маршрутизатор
I/O Розширення	
Загальна кількість слотів розширення:	4
Управління та протоколи	
Пам'ять	
Стандартна пам'ять:	8 MB
Максимальна пам'ять:	512 MB
Технологія пам'яті:	DRAM
Флеш-пам'ять:	16 MB
Підтримка карти пам'яті:	CompactFlash (CF) Card
Фізичні характеристики	
Сумісний стійковий блок:	4U
Форм-фактор:	Rack-mountable
Висота:	7"
Ширина:	21.8"
Довжина:	17.4"
Вага (приблизно):	27 lb
Різне	
Додаткова інформація:	• Spare Product • 2 MB programmable Flash • Gigabit Ethernet (GE): 4-port Gigabit Ethernet WAN (GBIC) • ATM Port Adapters: 2-port OC12-c, STM-4c ATM MM and SM-IR • Processor: Supervisor Engine 2 w/MSFC2 and PFC2 (Multi-service Feature Card 2 with Policy Feature Card 2) Slot Details: • Slot 1 is reserved for the supervisor engine • Slot 2 can contain a redundant supervisor engine that can act as a backup • Slot 2 is available for an OSM or other supported Catalyst 6500 series modules

Таблиця 2. Технічні характеристики комутатора Cisco WS-C2960-24TT-L

Розробник:	Cisco
ID:	WS-C2960-24TT-L
Опис:	Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image
Тип:	Комутатор
Інтерфейси/Порти	
Кількість портів:	24
Uplink Port:	Так
RJ-45 порти:	24
Слоти детальніше:	24 x Fast Ethernet Network
	2 x Gigabit Ethernet Uplink
Медіа та продуктивність	
Тип носія, що підтримується:	Вита пара
Стандарт кабелю вита пара:	Категорія 5
Технологія Ethernet	Fast Ethernet
Мережеві технології:	10Base-T
	10/100/1000Base-T
Мережа та зв'язок	
Підтримуваний рівень:	2
Управління та протоколи	
Керований:	Так
Функції безпеки:	• Cisco Network Assistant • CiscoWorks Support • Device manager • Cisco Express Setup • CiscoView application • Cisco Network Assistant Software • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches • Cisco IOS CLI support provides a common user interface and command set with all Cisco routers and Cisco Catalyst desktop switches • Cisco Service Assurance Agent (SAA) support facilitates server-level management throughout the LAN • Switching Database Manager templates for security and QoS allow administrators to easily adjust memory allocation to the desired features based on deployment-specific requirements • VLAN trunks can be created from any port using standards-based 802.1q tagging • Up to 255 VLANs per switch or stack and up to 128 spanning-tree instances per switch are supported. • Four thousand VLAN IDs are supported • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches • SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management • Cisco Discovery Protocol Versions 1 and 2 help enable a CiscoWorks network-management station for automatic switch discovery
Опис потужності	
Вхідна напруга:	110 V AC
	220 V AC
Джерело живлення:	Power Supply
Резервне джерело живлення:	Так

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

Фізичні характеристики	
Висота:	1.7»
Ширина:	17.5»
Довжина:	9.3»
Вага (приблизно):	8 lb
Різне	
Додаткова інформація:	• 64 MB DRAM • 32 MB flash memory • LAN Base Image installed • Configurable up to 8000 MAC addresses • Configurable up to 255 IGMP groups • Cisco Catalyst 2960-24TT: 282,416 hr • Superior Redundancy for Fault Backup • Integrated Cisco IOS Software Features for Bandwidth Opti- ation • Advanced QoS • Granular Rate Limiting Networkwide Security Features

		Гаврилюк В.Б.			ККІКБ.КР.Б – 123 – 2 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		93