

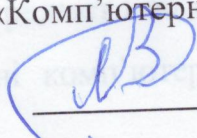
Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

## ПОЯСНЮВАЛЬНА ЗАПИСКА

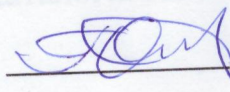
до випускної кваліфікаційної роботи бакалавра  
на тему: «Проект локальної комп'ютерної мережі  
організації на основі служби каталогів Active Directory»

Виконав студент 4-го курсу групи КІ-4

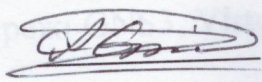
спеціальності 123 «Комп'ютерна інженерія»

 Владислав Яхимович

Керівник доцент кафедри КІ та КБ, к.пед.н.,

 Олена Головня

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

 Андрій Єфіменко

Житомир – 2022

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

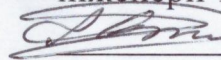
Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної  
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

### ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Яхимович Владислав Сергійович

Тема роботи: «Проект локальної комп'ютерної мережі організації на основі  
служби каталогів Active Directory»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

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

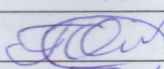
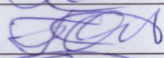
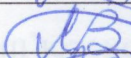
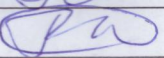
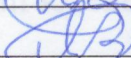
**Об'єктом дослідження** є локальні комп'ютерні мережі на основі ОС  
Windows.

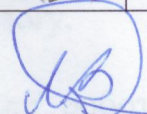
**Предметом дослідження** є сервіси служби каталогів Active Directory та їх  
налаштування.

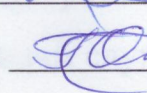
Обладнання та програмне забезпечення:

1. Програмне забезпечення: Симулятор мережі GNS3, VirtualBox
2. Операційні системи: Windows 10, Windows Server 2019
3. Апаратне забезпечення: маршрутизатор Cisco 2901-HSEC+/K9, комутатор  
Cisco WS-C2960-24TT-L, точка доступу MikroTik RBCAPGI-5ACD2ND

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

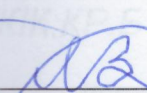
| Розділ | Консультант  | Підпис, дата                                                                              |                                                                                             |
|--------|--------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
|        |              | Завдання видав                                                                            | Завдання прийняв                                                                            |
| 1      | Головня О.С. |  1.03.22 |  1.03.22 |
| 2      | Головня О.С. |  1.03.22 |  1.03.22 |
| 3      | Головня О.С. |  1.03.22 |  1.03.22 |

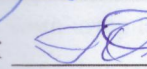
Студент  Владислав Яхимович

Керівник  Олена Головня

### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|-------|-----------------------------------------------|--------------------------------|----------|
| 1     | Постановка завдання                           | 01.03.2022                     |          |
| 2     | Аналіз літературних джерел                    | 11.03.2022                     |          |
| 3     | Аналіз об'єкта дослідження                    | 13.03.2022                     |          |
| 4     | Розробка структурної моделі                   | 20.04.2022                     |          |
| 5     | Розрахунок параметрів адресації               | 24.04.2022                     |          |
| 6     | Вибір сервісів для налаштування в AD          | 29.04.2022                     |          |
| 7     | Вибір апаратного та програмного забезпечення  | 04.05.2022                     |          |
| 8     | Розробка структури домену AD                  | 06.05.2022                     |          |
| 9     | Налаштування мережі та сервісів               | 12.05.2022                     |          |
| 10    | Перевірка працездатності                      | 23.05.2022                     |          |
| 11    | Оформлення пояснювальної записки              | 10.06.2022                     |          |
| 12    | Захист                                        | Згідно з розкладом             |          |

Студент  Владислав Яхимович

Керівник  Олена Головня

## АНОТАЦІЯ

Кваліфікаційна робота бакалавра містить 94 сторінок тексту, 104 рисунків, 4 таблиці, посилання на 21 літературне джерело.

Метою роботи є створення проекту локальної комп'ютерної мережі організації на основі служби каталогів Active Directory.

Результатом виконання кваліфікаційної роботи є розроблена локальна комп'ютерна мережа організації під управлінням служби каталогів Active Directory. Проаналізовані теоретичні аспекти локальних комп'ютерних мереж, досліджено загальні характеристики служби каталогів Active Directory, описано використані сервіси і функції. Проаналізовано та обрано топологію комп'ютерної мережі, розроблено схему адресації пристроїв, розроблено структуру домену, обрано апаратне та програмне забезпечення, необхідне для працездатності мережі. На основі всіх попередніх етапів роботи, налаштовано та протестовано всі функції локальної мережі.

Ключові слова: ЛОКАЛЬНА МЕРЕЖА, МАРШРУТИЗАТОР, КОМУТАТОР, ТОЧКА ДОСТУПУ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СЕРВЕР, ДОМЕН, ACTIVE DIRECTORY.

|           |      |               |                                                                                     |          |                                                                                              |                |      |         |
|-----------|------|---------------|-------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------|----------------|------|---------|
|           |      |               |                                                                                     |          | КІК.КР.Б – 123 – 20 – ПЗ                                                                     |                |      |         |
| Змн.      | Арк. | № докум.      | Підпис                                                                              | Дата     | Проект локальної комп'ютерної мережі організації на основі служби каталогів Active Directory | Лім.           | Арк. | Аркушів |
| Розроб.   |      | Яхимович В.С. |  | 20.06.22 |                                                                                              |                |      |         |
| Керівник  |      | Головня О.С.  |  | 20.06.22 |                                                                                              |                | 4    | 94      |
| Реценз.   |      | Єфіменко А.А. |  | 20.06.22 |                                                                                              | ФІКТ, Гр. КІ-4 |      |         |
| Н. контр. |      | Головня О.С.  |  | 20.06.22 |                                                                                              |                |      |         |
| Затверд.  |      | Єфіменко А.А. |  | 20.06.22 |                                                                                              |                |      |         |

## ANNOTATION

Diploma project contains 94 pages of text, 104 figures, 2 tables, references to 21 literary sources.

The purpose of the work is to create a project of the local computer network of the organization based on the Active Directory directory service.

The result of the qualification work is the developed local computer network of the organization under the management of the Active Directory directory service. Theoretical aspects of local computer networks are analyzed, the general characteristics of the Active Directory service are investigated, the used services and functions are described. The topology of the computer network is analyzed and selected, the addressing scheme of devices is developed, the structure of the domain is developed, the hardware and the software which is essential for network operability are chosen. Based on all previous stages of work, all functions of the local network are configured and tested.

Keywords: LOCAL NETWORK, ROUTER, SWITCH, ACCESS POINT, SOFTWARE, SERVER, DOMAIN, ACTIVE DIRECTORY.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 5    |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## ЗМІСТ

|                                                                                                                                                         |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП.....                                                                                                                                              | 8  |
| РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ<br>НА БАЗІ СЛУЖБИ КАТАЛОГІВ ACTIVE DIRECTORY .....                                              | 10 |
| 1.1 Загальна характеристики служби каталогів Active Directory .....                                                                                     | 10 |
| 1.2 Теоретичні аспекти локальних комп'ютерних мереж.....                                                                                                | 12 |
| 1.3 Загальні характеристики сервісів локальних комп'ютерних мереж на базі<br>служби каталогів Active Directory .....                                    | 18 |
| РОЗДІЛ 2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА<br>БАЗІ СЛУЖБИ КАТАЛОГІВ ACTIVE DIRECTORY ТА ВИБІР ОБЛАДНАННЯ,<br>ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ..... | 28 |
| 2.1 Проектування топології мережі .....                                                                                                                 | 28 |
| 2.2 Розробка схеми адресації мережі для протоколів IPv4 та IPv6 .....                                                                                   | 33 |
| 2.3 Створення структури домену в Active Directory .....                                                                                                 | 36 |
| 2.4 Вибір обладнання та програмного забезпечення.....                                                                                                   | 38 |
| РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ЛОКАЛЬНОЇ<br>КОМП'ЮТЕРНОЇ МЕРЕЖІ.....                                                                               | 42 |
| 3.1 Базове налагодження обладнання та програмного забезпечення мережі<br>.....                                                                          | 42 |
| 3.2 Налagodження сервісів локальної комп'ютерної мережі .....                                                                                           | 46 |
| 3.3 Тестування працездатності вузлів та сервісів побудованої локальної<br>комп'ютерної мережі .....                                                     | 74 |
| ВИСНОВКИ.....                                                                                                                                           | 81 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                                                                                                                    | 83 |
| ДОДАТКИ.....                                                                                                                                            | 85 |

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 6    |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЛКМ – Локальна комп'ютерна мережа

ПК – Персональний комп'ютер

FE – Fast Ethernet

GE – Gigabit Ethernet

WLAN – бездротова локальна мережа

AD – Active Directory

OU – Organization unit

GPO – Group Policy Object

IIS – Internet Information Services

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 7    |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## ВСТУП

**Актуальність теми.** Локальні мережі, які працюють під управлінням Active Directory, отримали широке розповсюдження за останні декілька десятиліть. Використання мережевої інфраструктури з контролером домену дуже зручне, оскільки дозволяє системним адміністраторам виконувати гнучкі налаштування привілеїв, дозволів, обмежень, а також політики для всіх користувачів мережі, централізувати управління повноваженнями, спільними ресурсами, резервним копіюванням. Але популярність технології неминуче притягує за собою інтерес до неї з боку зловмисників, які прагнуть проникнути в мережу з різною метою – включаючи використання скомпрометованих даних і викрадення дуже важливої інформації. Тому в наш час дуже потрібні люди, які мають необхідні знання для створення та підтримання такої мережі в робочому стані, а також для її захисту.

**Метою кваліфікаційної роботи** є створення локальної мережі організації з використанням служби каталогів Active Directory на основі навичок та знань, які були здобуті на протязі всього періоду навчання в університеті.

Визначена мета обумовлює наступні завдання:

- Проаналізувати структуру локальних комп'ютерних мереж та служби каталогів Active Directory
- Спроекувати локальну комп'ютерну мережу та структуру домену Active Directory
- Налаштувати компоненти локальної комп'ютерної мережі та сервіси служби каталогів Active Directory
- Перевірити роботу локальної комп'ютерної мережі та сервісів служби каталогів Active Directory

**Об'єктом дослідження** є локальні комп'ютерні мережі на основі ОС Windows.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 8    |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

**Предметом дослідження є сервіси служби каталогів Active Directory та їх налаштування.**

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 9    |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

# РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ НА БАЗІ СЛУЖБИ КАТАЛОГІВ ACTIVE DIRECTORY

## 1.1 Загальна характеристики служби каталогів Active Directory

Active Directory (AD) – це власна служба каталогів, розроблена Microsoft для керування автентифікацією та авторизацією користувачів і машин у мережі домену Windows. Служба каталогів – це велика ієрархічна база даних, що містить інформацію про користувачів, групи користувачів, комп'ютери, а також мережеві ресурси, що працюють у корпоративних мережах з серверами Microsoft. Це не що інше, як збір інформації про користувачів мережі, їхні права на різні типи ресурсів, комп'ютери, на яких вони працюють, конфігурацію цих комп'ютерів тощо. Active Directory дозволяє адміністраторам мережі централізовано з одного комп'ютера (правильно налаштованого сервера) керувати всім набором користувачів у мережі, визначати їхні права на мережеві ресурси та налаштовувати комп'ютери, на яких вони працюють. Цей потужний інструмент, безумовно, полегшує роботу адміністратора в мережах з десятками користувачів і комп'ютерів. Вперше ця служба була випущена в 2000 році і працює на ОС Windows Server.

Розглянемо основні поняття, пов'язані зі службою каталогів Active Directory:

Сховище даних – файл, що зберігається на диску сервера, містить інформацію про об'єкти служби каталогів. Об'єктом служби каталогів може бути користувач, група, організаційний підрозділ або комп'ютер. Файл має назву NTDS.dit і зберігається у папці %SYSTEMROOT%\NTDS.

Контролер – сервер із встановленим Active Directory, який містить копію сховищ даних. Можна виділити контролери типу Global Catalog (глобальний каталог), а також контролери тільки для читання - Read-Only Domain Controller і контролери читання і запису - Writeable Domain Controller.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 10   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Домен (domain) – ділянка мережі, якій виділені певні можливості та ресурси. Він збирає об'єкти Active Directory, такі як користувачі, групи, організаційні підрозділи та комп'ютери, що працюють у ньому. Для створення домену потрібен принаймні один контролер домену.

Ліс (forest) – набір одного або кількох доменів. Перший домен, який буде створений в лісі, буде так званим кореневим доменом лісу, і весь ліс прийме ім'я, таке як основний домен. Наприклад, якщо ми створимо новий домен у новому лісі та назвемо його test.local, весь ліс отримає цю назву.

Дерево (tree) – один домен або кілька доменів, що працюють в одному просторі імен DNS.

Організаційна одиниця (або організаційний підрозділ, англ. Organization unit) - це об'єкт AD, який дозволяє зберігати користувачів, групи користувачів і комп'ютери. Організаційним одиницям можна призначати окремі групові політики і делегувати адміністративні права.

Основним компонентом Active Directory є доменні служби Active Directory (AD DS), які перевіряють доступ, коли користувач входить в систему або намагається підключитися до системи через мережу, а також призначає та застосовує політики безпеки. Інші служби Active Directory включають:

- Active Directory Lightweight Directory Services: Спрощена версія доменних служб Active Directory, орієнтована на надання лише функціональності служб каталогів;
- Active Directory Federation Services: заснована на веб-службах, технологія для надання служб автентифікації з єдиним входом в систему у межах організації
- Active Directory Certificate Services: служба для надання послуг реєстрації та відкликання цифрових сертифікатів на підтримку інфраструктури відкритих ключів (PKI);
- Active Directory Rights Management Services: служба для керування правами доступу користувачів до документів організації.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 11   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Дані зберігаються в Active Directory як об'єкти, що організовані за іменами та атрибутами. Для зломисників Active Directory є “охоронцем коштовностей”. Коли суб'єкти загроз компрометують мережу, вони зазвичай намагаються підвищити рівень своїх привілеїв, щоб зможти перейти до більш важливих систем, отримати доступ до конфіденційних даних. В результаті атака на Active Directory і отримання доступу на рівні адміністратора є однією з головних цілей зломисників. Зазвичай це робиться за допомогою таких інструментів, як BloodHound, який являє собою додаток з відкритим вихідним кодом, що використовується для аналізу безпеки доменів Active Directory і виявлення можливостей для збільшення прав доступу. Як тільки кібератаки виявляють приховані або складні шляхи, які потенційно можуть поставити під загрозу безпеку мережі, використовують такі інструменти, як Mimikatz, для крадіжки необхідних облікових даних.

## 1.2 Теоретичні аспекти локальних комп'ютерних мереж

Локальна мережа – це комп'ютерна мережа, що складається з точок доступу, кабелів, маршрутизаторів і комутаторів, які зв'язані між собою, дозволяють пристроям підключатися до веб-серверів і внутрішніх серверів в межах однієї будівлі, кампуса або домашньої мережі, а також до інших локальних мереж через глобальні мережі (WAN) або міські мережі (MAN). Пристрої в локальній мережі, зазвичай персональні комп'ютери і робочі станції, можуть обмінюватися файлами і отримувати доступ один до одного через одне підключення до Інтернету. [9]

Існують такі типи локальних мереж:

- дротові локальні комп'ютерні мережі;

В мережах такого типу підключення відбувається завдяки кабелю. Маршрутизатор призначає IP-адреси кожному пристрою в мережі і забезпечує спільне підключення до інтернету між усіма підключеними пристроями. Мережевий комутатор підключається до маршрутизатора і полегшує обмін даними між підк-

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 12   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

люченими пристроями, але не обробляє налаштування IP-адреси локальної мережі або спільне використання підключень до Інтернету. Комутатори використовуються для збільшення кількості портів локальної мережі, доступних в мережі.

- бездротові локальні комп'ютерні мережі;

WLAN або бездротова локальна мережа, – це мережа, яка дозволяє пристроям підключатися та спілкуватися бездротовим способом. На відміну від традиційної дротової локальної мережі, в якій пристрої спілкуються через кабелі Ethernet, пристрої в мережі WLAN спілкуються через Wi-Fi.

Хоча WLAN може виглядати інакше, ніж традиційна локальна мережа, вона функціонує так само. Нові пристрої зазвичай додаються та налаштовуються за допомогою DHCP. Вони можуть спілкуватися з іншими пристроями в мережі так само, як і в дротовій мережі. Основна відмінність полягає в тому, як передаються дані. У локальній мережі дані передаються по фізичних кабелях у серії пакетів Ethernet. У WLAN пакети передаються по без використання кабельних з'єднань.

Оскільки бездротові пристрої стали дуже популярні, так і потреба в бездротових мережах також зросла. Насправді більшість проданих маршрутизаторів тепер є бездротовими маршрутизаторами. Бездротовий маршрутизатор служить базовою станцією, забезпечуючи бездротове з'єднання з будь-якими пристроями з підтримкою Wi-Fi в межах діапазону бездротового сигналу маршрутизатора. Сюди входять ноутбуки, планшети, смартфони та інші бездротові пристрої, такі як розумні прилади та контролери розумного будинку. Бездротові маршрутизатори часто підключаються до кабельного модему або іншого пристрою, підключеного до Інтернету, щоб забезпечити доступ до Інтернету підключеним пристроям.

Захист у бездротових локальних мережах.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 13   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

MAC-фільтрація – це метод безпеки, заснований на контролі доступу. При цьому кожній адресі призначається 48-бітова адреса, яка використовується для визначення того, чи можемо ми отримати доступ до мережі чи ні. Це допомагає в переліку набору дозволених пристроїв, які потрібні у нашій Wi-Fi мережі, і списку заборонених пристроїв, які ми не хочемо використовувати у своїй мережі. Це допомагає запобігти небажаному доступу до мережі. У певному сенсі ми можемо заборонити або дозволити список певних комп'ютерів на основі їх MAC-адреси. Ми можемо налаштувати фільтр, щоб дозволити підключення лише до тих пристроїв, які включені в білий список. Білі списки забезпечують більшу безпеку, ніж заборонені списки, оскільки маршрутизатор надає доступ лише вибраним пристроям.

На сьогоднішній день існує декілька типів шифрування бездротових каналів зв'язку Wi-Fi. Давайте розглянемо, чим відрізняються між собою різні стандарти шифрування Wi-Fi, і який з цих стандартів є найбільш захищеним.

### Шифрування за WEP

Wired Equivalent Privacy, або скорочено WEP, вважається найслабкішим стандартом шифрування. Стандарт WEP з'явився дуже давно, і по суті є одним з перших алгоритмів шифрування Wi-Fi каналів. Незважаючи на те, що стандарт є застарілим, багато користувачів досі використовують його. Однак слід пам'ятати, що шифрування за допомогою WEP-алгоритму забезпечує захист, не набагато надійніший, ніж використання відкритого каналу бездротового зв'язку. Справа в тому, що злом мережі, захищеної по стандарту WEP, не вимагає наявності особливих навичок в сфері програмування і серйозного програмного забезпечення. Окрім того, для того, щоб отримати доступ до такої мережі, зловмисникові потрібно відносно короткий проміжок часу - приблизно кілька десятків хвилин. Така ненадійність стандарту WEP обумовлена перш за все особливостями організації самого шифрування. По каналу, зашифрованого через WEP, разом з пакетами даних передається і кілька байт самого ключа шифрування, тому при наявності

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 14   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

достатньої кількості перехоплених пакетів даних можна легко отримати повний ключ, що дає доступ до мережі.

### Шифрування за WPA і WPA2

WPA, або Wi-Fi Protected Access - це новіший стандарт захисту бездротового зв'язку, який прийшов на зміну стандарту WEP. Основні відмінності WPA полягають у набагато кращому захисті пакетів даних і застосуванням більш сучасної технології аутентифікації користувачів в бездротовій мережі.

Стандарт WPA підтримує два різних алгоритми шифрування переданих даних: TKIP і CCMP. TKIP є протокол інтеграції тимчасового ключа, він надає користувачам бездротової мережі трохи кращий захист, ніж при використанні WEP, але все ж таки сильно не дотягує до нового протоколу CCMP. В порівнянні протокол CCMP є найбільш передовим на сьогоднішній день засобом захисту бездротової мережі. Це протокол з блочним шифруванням, який використовується переважно в стандарті WPA2, який є вдосконаленою версією стандарту WPA.

В WPA і WPA 2 для захисту мережі як правило використовується режим початкової аутентифікації PSK (Pre-Shared Key). Він дуже зручний для використання, оскільки дозволяє здійснювати вхід за введеним паролем, який використовується користувачем під час початкового підключення. Однак для корпоративних мереж набагато краще підходить режим аутентифікації Enterprise, в якому присутні кілька ключів, які зберігаються на окремому сервері.

### Технологія WPS

Технологія WPS (Wi-Fi Protected Setup), звана також QSS (Quick Security Setup), являється протоколом шифрування бездротового каналу зв'язку зі спрощеною системою авторизації користувачів. При використанні цієї технології, можна практично миттєво здійснити підключення до бездротової мережі без будь-яких додаткових налаштувань або паролів. Достатньо лише натиснути відповідні

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 15   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

кнопки на Wi-Fi роутер і підключення між з пристроями буде створено автоматично.

Оскільки такий спосіб підключення і захисту бездротової мережі дуже простий і зручний, потрібно розуміти, що у порівнянні зі стандартом WPA2, він не дуже надійний. При наявності хоча б малого досвіду і знань, злоумисник може без великих проблем перехопити пароль від нашої Wi-Fi мережі, що в подальшому дозволить йому в автоматичному режимі підключатися до неї в будь-який час. Тому в цілях безпеки краще тримати функцію WPS відключеною і включати її тільки по мірі необхідності. Отже, із всіх стандартів захисту бездротової мережі, самим надійним є WPA2.

### Переваги WLAN

Найбільш очевидна перевага WLAN полягає в тому, що пристрої можуть підключатися бездротовим способом, усуваючи потребу в кабелях. Це дозволяє будинкам і підприємствам створювати локальні мережі без підключення до будівлі за допомогою Ethernet. Він також забезпечує можливість для невеликих пристроїв, таких як смартфони та планшети, підключатися до мережі. Бездротові локальні мережі не обмежені кількістю фізичних портів на маршрутизаторі і тому можуть підтримувати десятки або навіть сотні пристроїв. Діапазон WLAN можна легко розширити, додавши один або кілька ретрансляторів. Нарешті, бездротову локальну мережу можна легко оновити, замінивши маршрутизатори новими версіями – це набагато легше та дешевше рішення, ніж оновлення старих кабелів Ethernet.

### Недоліки WLAN

Бездротові мережі, природно, менш безпечні, ніж дротові мережі. Будь-який бездротовий пристрій може здійснити підключення до WLAN, тому важливо обмежити доступ до мережі, якщо це викликає занепокоєння. Зазвичай це робиться за допомогою бездротової аутентифікації, наприклад WEP або WPA, яка шифрує зв'язок. Також можна приховати SSID мережі, щоб його треба було

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 16   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

вводити вручну. Крім того, бездротові мережі більш сприйнятливі до перешкод від інших сигналів або фізичних бар'єрів, таких як бетонні стіни. Оскільки локальні мережі пропонують найвищу продуктивність і безпеку, вони все ще використовуються в багатьох корпоративних і державних мережах.

### Топологія мережі

Схема локальної обчислювальної мережі, також відома як топологія локальної обчислювальної мережі, описує фізичний і логічний спосіб, за яким пристрої і сегменти мережі пов'язані між собою. Локальні мережі зазвичай складаються з кабелів і комутаторів, які можуть бути підключені до маршрутизатора, кабельного модему або ADSL-модему для доступу в інтернет. Локальні мережі також можуть включати в себе такі мережеві пристрої, як брандмауери, балансувальники навантаження і пристрої для виявлення мережевих вторгнень. Функція локальних мереж полягає в об'єднанні комп'ютерів і наданні загального доступу до принтерів, файлів та інших служб. За архітектурою розрізняють однорангові мережі та клієнт-серверні мережі. У локальній мережі клієнт-сервер кілька клієнтських пристроїв підключені до центрального сервера, на якому здійснюється управління доступом до додатків, доступом до пристроїв, сховища файлів і мережевого трафіку.

Програми, що працюють на сервері локальної мережі, надають такі послуги, як доступ до бази даних, спільний доступ до документів, електронна пошта та друк. Пристрої в одноранговій локальній мережі обмінюються даними безпосередньо з комутатором або маршрутизатором без використання центрального сервера.

Локальні мережі можуть з'єднуватися з іншими локальними мережами через виділені лінії і служби або через Інтернет з використанням технологій віртуальної приватної мережі. Ця система підключених локальних мереж класифікується як глобальна локальна мережа або міська мережа. Локальні і глобальні мережі розрізняються за своїм діапазоном дії.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 17   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Створення локальної мережі допомагає вирішити безліч завдань:

- швидкий доступ до даних для кожного користувача;
- швидкісна передача даних між безліччю підрозділів однієї організації;
- можливість використовувати файли одночасно на різних пристроях;
- високошвидкісна комунікація;
- комфортне використання та доступ до різних мережевих пристроїв;
- віддалене управління документами та програмними засобами;
- безпека та надійний захист важливих даних організації.

Оскільки у мережі часто зберігаються дані та цінна інформація, які можуть бути під загрозою під час атак з боку конкурентів, то останній пункт дуже важливий у роботі.

### **1.3 Загальні характеристики сервісів локальних комп'ютерних мереж на базі служби каталогів Active Directory**

Служба каталогів Active Directory має багато налаштувань та сервісів, які необхідні для нормального та безпечного функціонування мережі. В цьому пункті ми розглянемо самі основні з них.

#### **DHCP у Active Directory**

Протокол динамічної конфігурації хоста (DHCP) дозволяє клієнту автоматично отримувати IP-адресу від DHCP-сервера. Цей процес дозволяє уникнути помилок конфігурації, які можуть бути викликані ручним налаштуванням кожного комп'ютера. DHCP допомагає запобігти конфліктам адрес, які виникають при повторному використанні ідентичної IP-адреси для налаштування нового комп'ютера в мережі. У випадку користувачів з портативними пристроями, які часто змінюють своє розташування (і згодом потребують оновлення клієнтських конфігурацій), процес продовження оренди DHCP допомагає забезпечити ефективні та автоматичні оновлення. Якщо сервер надає адреси пристроям з різних підмереж, то потрібно налаштувати DHCP relay на маршрутизаторі. [4]

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 18   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

DHCP relay agent - працює як інтерфейс між DHCP клієнтами і сервером, передає DHCP повідомлення між клієнтами і серверами в різних IP-мережах.

### Remote Desktop Services (RDS)

Служби віддаленого робочого столу (RDS), раніше відомі як служби терміналів (terminal services), є одним із компонентів Windows, що дозволяє користувачеві контролювати віддалений комп'ютер або віртуальну машину через мережеве з'єднання.

Такий доступ надається через:

- віддалений робочий стіл (Remote Desktop Session Host)
- віддалену роботу в окремих застосунках (RemoteApp)

RDS-середовище може сумісно працювати з Active Directory (у деяких випадках використання AD обов'язкове). Основні складові частини RDS-середовища на базі Windows Server:

- протокол RDP
- RDSH-сервери (Remote Desktop Session Host)
- Remote Desktop Connection Broker
- Remote Desktop Licensing
- Remote Desktop Gateway
- Remote Desktop Web Access
- Remote Desktop Virtualization Host

### Remote Desktop Session Host

Містить програми та робочі столи на основі сеансів, якими ви ділитесь з користувачами. Користувачі отримують доступ до цих робочих столів та програм через один із клієнтів віддаленого робочого столу, що працюють у Windows, MacOS, iOS та Android. Користувачі також можуть підключатися через браузер, що підтримується, за допомогою веб-клієнта.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 19   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## Remote Desktop Connection Broker

Дозволяє рівномірно розподіляти навантаження між вузлами (при підключенні до RDS, користувача перенаправляє на менш завантажений сервер), забезпечує доступ користувачів до VDI та RemoteApp, Також RDCB дозволяє користувачам здійснювати перепідключення до своїх сесій: при підключенні до RDS, RDCB перевіряє наявність незавершеної сесії на інших серверах, та направляє його на попередню сесію.

## Remote Desktop Licensing

Керує клієнтськими ліцензіями для отримання доступу до служб віддаленого робочого столу. RD Licensing встановлює, випускає та контролює доступність ліцензій на сервері ліцензій віддаленого робочого столу за допомогою диспетчера ліцензування RD.

## Remote Desktop Gateway

Сервер, на якому працює програмне забезпечення Windows Server. Його завдання – забезпечити маршрутизацію трафіку RDP (протокол віддаленого робочого столу). Основний принцип роботи полягає в тому, що користувач підключається до RDP-сервера за допомогою клієнтського програмного забезпечення. Для того, щоб сервер цього типу не був доступний безпосередньо з Інтернету, використовується більш складна схема підключення, яка передбачає, що замість прямого підключення до сервера RDP користувач спочатку підключається до сервера RDG. Там також проводиться аутентифікація. Після успішного завершення цього процесу відбувається пересилання трафіку на певний сервер, до якого користувач хоче підключитися. При такому підході лише сервер RDG повинен бути загальнодоступним з Інтернету. Це зменшує ризик атаки на сервер.

## Remote Desktop Web Access

За допомогою RD Web Access для віддаленого робочого столу, користувачі мають можливість отримати доступ до RemoteApp та підключитися до віддаленого робочого столу через веб-браузер на комп'ютері.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 20   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## Remote Desktop Virtualization Host

Служба ролей, яка підтримує Virtual Desktop Infrastructure (VDI) і дозволяє декільком користувачам запускати програми під управлінням Windows на віртуальних машинах, які розміщені на сервері під керуванням Windows Server та, за потреби, Hyper-V.

### Переваги RDS

#### 1. Подібний інтерфейс.

Так як RDS реалізовано на платформі Microsoft, інтерфейс користувача такий же, як і в ОС Windows. Веб-інтерфейс за замовчуванням показує опубліковані робочі столи та віддалені програми. Це означає, що всі користувачі отримають доступ до схожого інтерфейсу, пропонуючи їм безперебійну роботу. Хоча зміна налаштувань інтерфейсу користувача заборонена, користувачі можуть змінювати деякі параметри, щоб підвищити зручність використання для себе.

#### 2. Покращена продуктивність системи

Користувачі мають доступ до віддаленого робочого столу через високопродуктивні сервери. Використання технології забезпечує чудову альтернативу для пристроїв, які можуть мати чи не мати потужну машину для запуску програм. Завдяки платформі Microsoft, вона також полегшує доступ до програм, які використовуються тільки для Windows, у системах, які працюють не на Windows, як до прикладу Android, iOS, macOS тощо.

#### 3. Віддалений доступ

Реалізація RDS пропонує економічне рішення для організації. За допомогою цього сервісу дозволяє своїм співробітникам працювати віддалено або впровадити політику BYOD. Обидва варіанти дозволяють співробітникам використовувати свої персональні пристрої для роботи в офісі.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 21   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

#### 4. Безпека

RDS пропонує кінцевим користувачам підвищену безпеку даних. Існують розширені функції безпеки, такі як новітні брандмауери та антивіруси, антиви-магачі, системи захисту від злову тощо. [10]

##### Domain Name System (DNS)

DNS – це служба доменних імен. Якщо ми намагаємося знайти сайт в інте-рнеті, більш ймовірно, що ми пам'ятаємо його ім'я, наприклад, [www.mi-crosoft.com](http://www.microsoft.com), ніж IP-адресу, яка може виглядати як 207.46.230.219. Однак комп'ю-теру для з'єднання з веб-сайтом Microsoft потрібно знати його IP-адресу. Служба DNS виконує цей переклад. Користувач повідомляє своєму браузеру ім'я комп'ютера, з яким він хотів би з'єднатися, а DNS перетворює це ім'я на відповідну IP-адресу.

DNS використовує ієрархічний простір імен для пошуку комп'ютерів. На рис. 1.1 показаний приклад організації простору імен. Кореневий домен позначається точкою. Він являє собою верхній рівень DNS, решта імен розташовується нижче. На наступному рівні під кореневим доменом розташовуються домени першого рівня, включаючи основні доменні ім'я (com, edu, net, org), близько двохсот скорочень назв країн (ua, uk, fr, br), і декілька інших доменів (biz, info, pro, тощо).

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 22   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

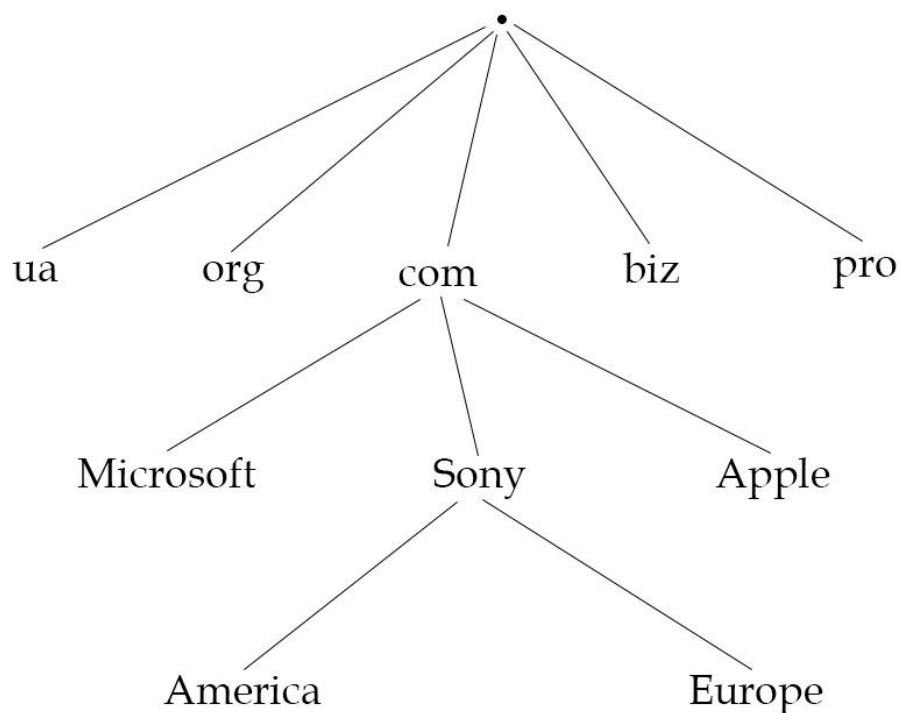


Рисунок 1.1 – ієрархічний простір імен DNS

Нижче домену верхнього рівня розташовані домени другого рівня, які зазвичай відносяться до назв компаній і мають бути зареєстровані організацією, яка керує доменним ім'ям. Нижче доменів другого рівня розміщуються піддомени. Піддомени зазвичай належать до відділів або підрозділів у межах компанії. Ці піддомени реєструються та управляються з DNS-серверів, які містять інформацію про домени другого рівня.

Іншим способом представлення ієрархічного простору імен є певне ім'я домену (FQDN – Fully Qualified Domain Name), наприклад, `www.America.Sony.com`. FQDN представляє повне ім'я, яке можна використовувати для ідентифікації певного комп'ютера в межах всього простору імен DNS. Щоб зрозуміти, як FQDN ідентифікує комп'ютер у просторі імен DNS, прочитайте його справа на ліво. Справа знаходиться точка («.»), яка ідентифікує кореневий домен, вона передуює імені домену першого рівня. За нею слідують домен `com` першого рівня, домен `Sony` другого рівня та піддомен `America`. Зліва в імені FQDN знаходиться `www` ім'я певного комп'ютера.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 23   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Служба каталогів Active Directory має можливість налаштування DNS-сервера. Щоб AD функціонував належним чином, необхідна правильна конфігурація DNS. Можна встановити DNS на контролерах домену, включаючи сервери, що не належать до Windows, установка DNS на контролери домену дозволяє використовувати зони пошуку, інтегровані в AD, щоб підвищити безпеку та спростити реплікацію зони. Неправильно налаштований DNS-сервер може викликати різноманітні проблеми, включаючи помилки входу, проблеми з обробкою групової політики та проблеми з реплікацією. [7]

### Зони DNS в Active Directory

DNS має розподілену базу даних, це означає, що інформація про всі домени, субдомени та зіставлення хостів зберігається не лише на одному DNS-сервері, а розподіляється між кількома серверами. Управління базою даних DNS полегшується, розділяючи простір імен DNS на кілька зон і призначаючи відповідальність за зону на певний сервер. Зона AD DNS – це набір ієрархічних доменних імен з кореневим доменом, делегованим одному або кільком серверам імен. Зона містить всю інформацію про домен, за винятком частин домену, делегованих іншим серверам імен.

### Делегування DNS Active Directory

Імена в межах зони можуть бути делеговані іншій зоні, яка підтримується іншим сервером. Таким чином, відповідальність субдомену може бути передана іншому серверу імен, який оброблятиме запити на ресурсні записи через процес, який називається AD DNS delegation. Делегування може бути введено в дію за допомогою ресурсних записів типу NS і A.

### Internet Information Services (IIS)

Інформаційні служби Інтернету, також відомі як IIS, – це веб-сервер Microsoft, який працює на операційній системі Windows і використовується для

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 24   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

обміну статичним і динамічним веб-вмістом з користувачами Інтернету. IIS можна використовувати для розміщення, розгортання та керування веб-додатками за допомогою таких технологій, як ASP.NET і PHP.

IIS використовує різні протоколи для зв'язку та обміну даними з віддаленими клієнтами або комп'ютерами, наприклад HTTP, SMTP і FTP. Як основний продукт Windows, IIS інтегрується з Windows Server і працює на ОС Windows. Ви можете використовувати сторонні утиліти для запуску IIS через Linux і macOS, але вони часто пропонують меншу стабільність і низьку продуктивність.[15]

#### Переваги використання сервера IIS

Безпека. IIS постачається з вбудованими функціями автентифікації, авторизації та контролю доступу для посилення безпеки веб-програм. Ви можете створювати облікові записи адміністратора системи та програм окремо для поглибленого доступу. Інші функції безпеки включають фільтрацію запитів до трафіку білого/чорного списку, динамічне блокування IP-адреси, шифрування SSL і TLS, стиснення веб-сторінок та засоби керування безпекою, специфічні для FTP.

Пули програм. Це допоможе вам розділити ваші веб-програми в IIS для кращої безпеки та доступності. Пул додатків містить одну або кілька програм, якими керує один або кілька робочих процесів у IIS. Робочий процес обробляє запити клієнта, специфічні для пулу програм. Ізоляція гарантує, що збій програми в певному пулі не впливає на програми в інших пулах.

Масштабованість і надійність. Ви можете реалізувати масштабовану та надійну веб-інфраструктуру за допомогою IIS Web Farm, яка дозволяє розміщувати веб-сайти з високим трафіком на кількох серверах IIS з балансуванням навантаження та маршрутизацією запитів додатків (ARR). Балансувальник навантаження розподіляє трафік між кількома серверами в фермі серверів IIS за допомо-

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          |      |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          | 25   |

гою складних алгоритмів. У той же час ARR визначає найкращий сервер для кожного запиту. Ферма серверів IIS також дозволяє додавати або видаляти сервери, щоб динамічно масштабувати можливості обробки трафіку веб-сайту.

Моніторинг продуктивності веб-сервера IIS. Має вирішальне значення для забезпечення більш плавної роботи веб-сайту для користувачів. Будь-яка невелика помилка на вашому сервері може призвести до повільного часу відповіді та часу очікування, що змусить користувачів швидко покинути ваш веб-сайт. Ви можете контролювати продуктивність веб-додатків за допомогою перевірок HTTP ping та програмного забезпечення для моніторингу продуктивності. Перший надає вам основні можливості моніторингу, а другий надає більш детальну інформацію про продуктивність вашого сервера.

#### Внутрішньосайтова реплікація (intrasite replication)

Є здебільшого автоматичною. Задля надійності внутрішньосайтова реплікація організована надлишковим чином: якщо контролерів домену більше двох, то з'єднання для реплікації автоматично створюються таким чином, аби кожний контролер домену був сполучений принаймні з двома іншими контролерами. Зазвичай реплікація автоматично розпочинається через певний час після того, як на контролері домену відбулися зміни, однак її можна запустити примусово. Важливо враховувати, що мережний трафік між контролерами домену може бути досить інтенсивним. Саме тому й існує рекомендація щодо максимально стабільного та швидкого з'єднання всередині сайту Active Directory. Для передавання даних внутрішньосайтова реплікація використовує протокол IP.

#### Міжсайтова реплікація (intersite replication)

З'єднання між різними сайтами не створюються автоматично - їх вручну задає адміністратор.

Сервер-плацдарм (bridgehead server) - сервер, через яких відбувається реплікація між цим сайтом та іншими сайтами. Сервер-плацдарм обирається авто-

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          |      |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          | 26   |

матично, однак адміністратор може задати сервер-плацдарм, якому треба надавати перевагу під час вибору (preffered bridgehead server). Втім, якщо такий сервер виявиться недоступний, міжсайтова реплікація не відбудеться. Для міжсайтової реплікації можна задавати розклад (наприклад, такий, аби реплікація відбувалася не в період найбільш інтенсивних операцій - скажімо, у неробочі години). Також можна обирати протокол (у більшості випадків - RPC over IP, іноді, для старих мереж - SMTP). Більшість операцій з реплікації всередині сайту та частину операцій з міжсайтової реплікації виконує компонент КСС (Knowledge Consistency Checker)

### Висновки розділу

В першому розділі було розглянуто загальні характеристики служби каталогів Active Directory та їх сервісів, визначення основних понять та сервісів пов'язаних з цією службою, важливість даної служби та загрози. Теоретичні аспекти про локальні комп'ютерні мережі, типи локальних мереж, їх відмінності, переваги та недоліки, методи захисту та завдання, які допомагають вирішити ЛКМ.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 27   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## РОЗДІЛ 2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА БАЗІ СЛУЖБИ КАТАЛОГІВ ACTIVE DIRECTORY ТА ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

### 2.1 Проектування топології мережі

Топологія мережі – це логічне та фізичне розташування пристроїв і з'єднань у мережі. Зазвичай у мережу включають такі пристрої, як комутатори, маршрутизатори, робочі станції та сервери.

#### Важливість топології мережі

Топологія мережі відіграє дуже важливу роль у тому, як функціонує мережа. А саме, топологія безпосередньо впливає на функціональність мережі. Вибір правильної топології може підвищити продуктивність, оскільки правильно обрана топологія мережі підвищує енергоефективність та швидкість передачі даних. Завдяки чітко визначеній і спроектованій топології мережі організації, адміністратору легше знаходити несправності та виправляти проблеми мережі.

#### Типи мережевих топологій

Топології мережі класифікуються як фізична топологія або логічна топологія мережі. Фізична топологія мережі - це фізичне розташування пристроїв і з'єднань. З'єднання вузлів у мережі, здійснюються за допомогою кабелів Ethernet або бездротовим шляхом через Wi-Fi маршрутизатори або точки доступу. Логічна топологія мережі визначає, як налаштована мережа, в тому числі, які вузли підключаються і як, а також шаблон передачі даних.

Поєднати вузли ЛКМ можна такими основними фізичними мережевими схемами:

- Шина;
- Кільце;
- Зірка;
- Повнозв'язана топологія.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 28   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## Топологія “шина”

Це тип топології мережі, де кожен вузол, тобто кожен пристрій мережі, підключений до окремої основної кабельної лінії. Дані передаються одним маршрутом, від однієї точки до іншої. Ми не можемо передавати дані іншими способами.

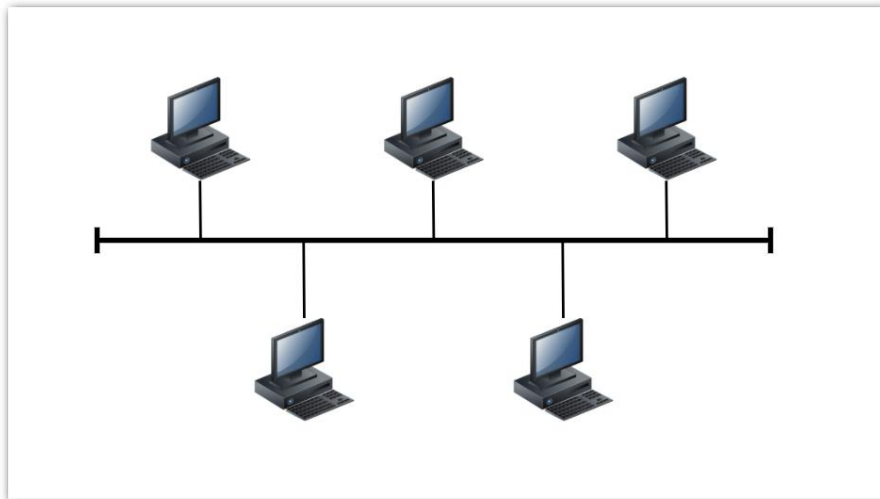


Рисунок 2.1 – Топологія “шина”

### Переваги топології:

- Простота монтажу та конфігурування ЛКМ;
- Несправність одного або декількох пристроїв не впливає на роботу локальної мережі в цілому.

### Недоліки топології

- Якщо відбудеться обрив основного провідника, то комп'ютери будуть відрізані один від одного та паралізується робота мережі. У цьому дуже складно оперативно локалізувати несправність;
- Зі збільшенням мережевих вузлів падає продуктивність ЛКМ.

## Топологія “кільце”

При такому з'єднанні всі комп'ютери підключені один до одного і сигнали передаються по кільцю від одного пристрою до іншого, доки не дійде до необхі-

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 29   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

дного вузла. Кільцева топологія через відсутність колізій та центрального пристрою є стійкою до перенавантажень і забезпечує стабільну роботу локальної мережі навіть за інтенсивного обміну даними. Для підвищення відмовостійкості даної топології, протягують другий кабель, утворюючи подвійне кільце, тобто до кожного пристрою під'єднують два кабелі. Завдяки цьому, можна передавати дані у зворотному напрямку або використовувати його як резервну лінію зв'язку.

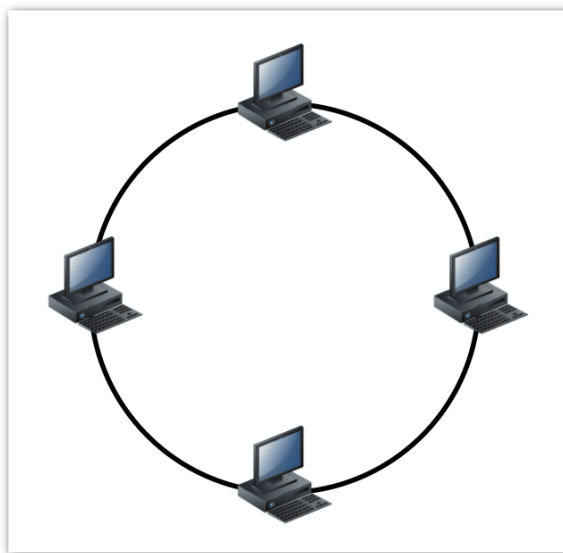


Рисунок 2.2 – Топологія “кільце”

До переваг цієї топології можна віднести відсутність додаткового обладнання та стабільну роботу ЛКМ при інтенсивному обміні даними.

Недоліками є складність пошуку несправностей для їх усунення, вихід з ладу одного вузла мережі або обрив кабелю впливає на працездатність всієї мережі, складна комутація.

#### Топологія “зірка”

В мережі є центральний пристрій, зазвичай це комутатор, з яким з'єднуються хости локальної мережі. Така схема вважається однією з найпоширеніших і застосовується для побудови корпоративних ЛКМ.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 30   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

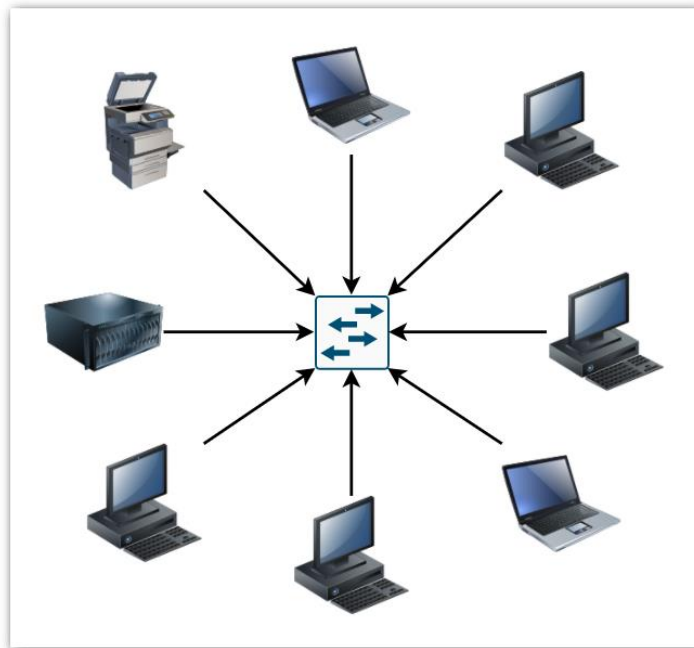


Рисунок 2.3 – Топологія “зірка”

Переваги топології:

- Розрив кабелю або вихід з ладу будь-якого пристрою, окрім центрального, не впливає на роботу всієї ЛКМ;
- Легко локалізувати несправності;
- Висока швидкість передачі даних між пристроями ЛКМ;
- Можливість побудови масштабних ЛКМ.

Недоліки топології:

- Висока вартість при впровадженні;
- Вихід з ладу центрального пристрою зробить ЛКМ недоступною.

Повнозв'язана топологія

Схема мережі передачі даних, де всі пристрої мають зв'язок один з одним. Завдяки цьому завжди є альтернативні шляхи зв'язку. Така схема використовується вкрай рідко, так як при зростанні мережевих пристроїв, збільшується кількість з'єднань, у результаті чого підтримувати цю топологію стає дуже накладно.

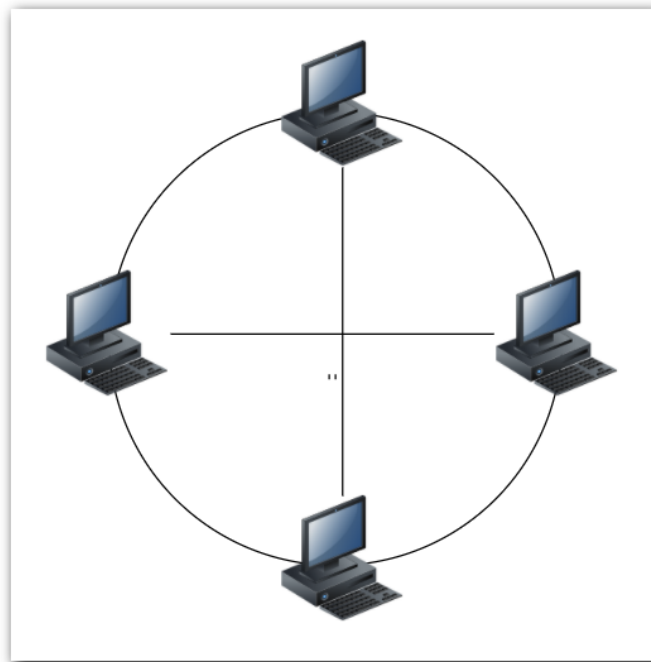


Рисунок 2.3 – Повнозв’язана топологія

Проаналізувавши основні типи топологій, їх переваги та недоліки, було прийнято рішення використати топологію зірка. [8]

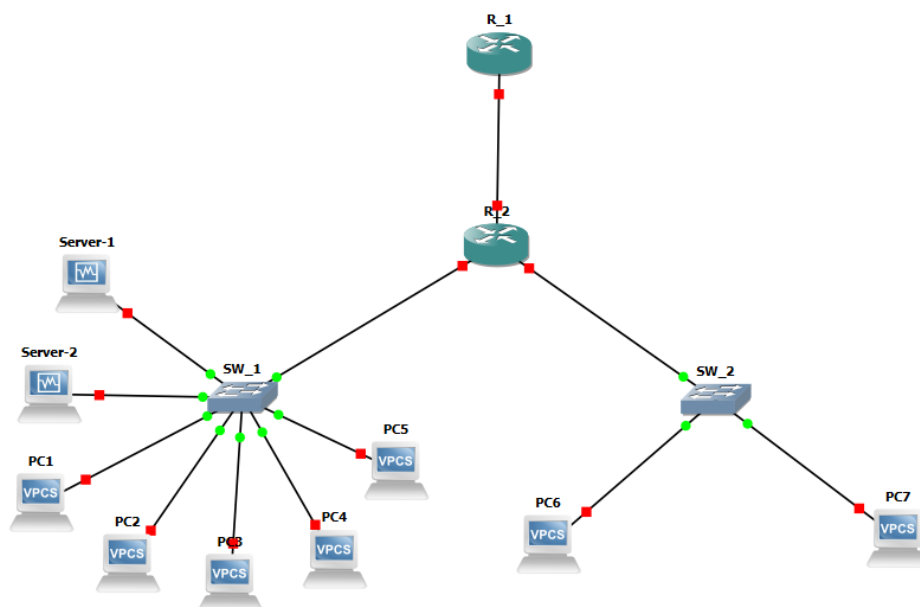


Рисунок 2.4 – Схема мережі

Мережа містить 2 основні підмережі N1 та N2. Перша з яких використовується працівниками організації, яка містить 2 сервери з встановленим Active Directory, робочі станції працівників та пристрої для спільного використання такі

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 32   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

як принтери, факси. Друга мережа призначена для відвідувачів організації, в якій налаштована точка доступу для безпроводного підключення і доступу в інтернет. На жаль емулятор мережі GNS3 не має можливості додати бездротове обладнання, таке як точка доступу чи Wi-Fi маршрутизатор та емулювати бездротове з'єднання. Але у моделі передбачимо також можливість підключення і цих пристроїв.

Загалом в мережі використовується 2 маршрутизатори та 2 комутатори, 1 точка доступу, кількість підмереж – 3.

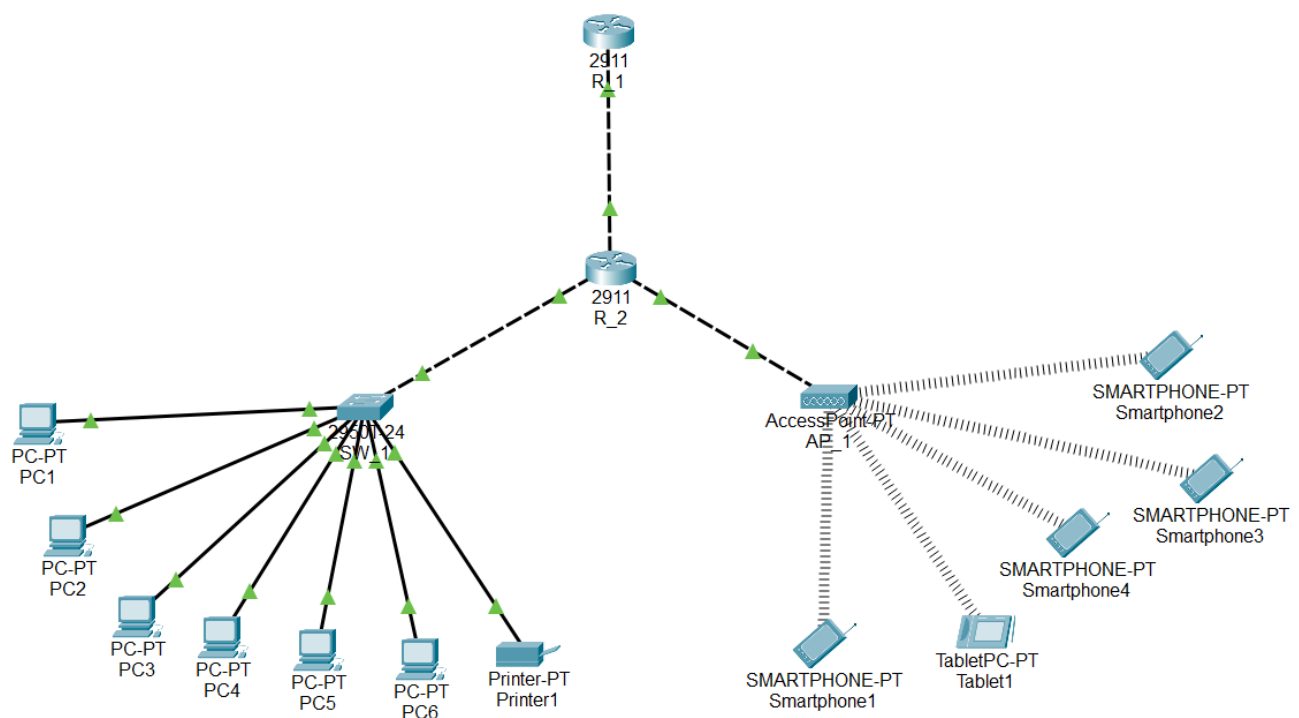


Рисунок 2.5 – Схема мережі в Cisco Packet Tracer

## 2.2 Розробка схеми адресації мережі для протоколів IPv4 та IPv6

Почати слід з розподілу адрес мережам(табл. 2.1).

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          |      |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          | 33   |

Таблиця 2.1 – Адреса мереж IPv4

| Назва мережі | Адреса мережі | Маска           | Префікс |
|--------------|---------------|-----------------|---------|
| A            | 200.4.20.0    | 255.255.255.252 | /30     |
| N1           | 201.4.20.0    | 255.255.255.128 | /25     |
| N2           | 202.4.20.0    | 255.255.255.128 | /25     |

Тепер можна розподілити адреса пристроям(табл. 2.2).

Таблиця 2.2 – Адреси пристроїв IPv4

| Назва пристрою | Інтерфейс | Мережа | Адреса     | Маска           | Префікс |
|----------------|-----------|--------|------------|-----------------|---------|
| R_1            | Gig0/0    | A      | 200.4.20.1 | 255.255.255.252 | /30     |
| R_2            | Gig0/0    | A      | 200.4.20.2 | 255.255.255.252 | /30     |
|                | Fa1/0     | N1     | 201.4.20.1 | 255.255.255.128 | /25     |
|                | Fa1/1     | N2     | 202.4.20.1 | 255.255.255.128 | /25     |
| Server_1       | Fa0       | N1     | 201.4.20.2 | 255.255.255.128 | /25     |
| Server_2       | Fa0       | N1     | 201.4.20.3 | 255.255.255.128 | /25     |
| PC1            | Fa0       | N1     | DHCP       |                 |         |
| PC2            | Fa0       | N1     |            |                 |         |
| PC3            | Fa0       | N1     |            |                 |         |
| PC4            | Fa0       | N1     |            |                 |         |
| PC5            | Fa0       | N1     |            |                 |         |
| PC6            | Fa0       | N1     |            |                 |         |
| PC7            | Fa0       | N2     |            |                 |         |
| PC8            | Fa0       | N2     |            |                 |         |

Також була розроблена таблиця IPv6 адресації, але в дипломному проекті буде використовуватися тільки IPv4. За потреби можна модифікувати мережу у майбутньому.

Таблиця 2.3 – Адреса мереж IPv6

| Назва мережі | Адреса мережі            | Маска |
|--------------|--------------------------|-------|
| A            | 2002:c804:1400:0:0:0:0:0 | 126   |
| N1           | 2002:c904:1400:0:0:0:0:0 | 121   |
| N2           | 2002:ca04:1400:0:0:0:0:0 | 121   |

Таблиця 2.4 – Адреси пристроїв IPv6

| Назва пристрою | Інтерфейс | Мережа | Адреса                   | Маска |
|----------------|-----------|--------|--------------------------|-------|
| R_1            | Gig0/0    | A      | 2002:c804:1401:0:0:0:0:0 | 126   |
| R_2            | Gig0/0    | A      | 2002:c804:1402:0:0:0:0:0 | 126   |
|                | Fa1/0     | N1     | 2002:c904:1401:0:0:0:0:0 | 121   |
|                | Fa1/1     | N2     | 2002:c904:1402:0:0:0:0:0 | 121   |
| Server_1       | Fa0       | N1     | 2002:c904:1402:0:0:0:0:0 | 121   |
| Server_2       | Fa0       | N1     | 2002:c904:1403:0:0:0:0:0 | 121   |
| PC1            | Fa0       | N1     | DHCP                     |       |
| PC2            | Fa0       | N1     |                          |       |
| PC3            | Fa0       | N1     |                          |       |
| PC4            | Fa0       | N1     |                          |       |
| PC5            | Fa0       | N1     |                          |       |
| PC6            | Fa0       | N1     |                          |       |
| PC7            | Fa0       | N2     |                          |       |
| PC8            | Fa0       | N2     |                          |       |

## 2.3 Створення структури домену в Active Directory

У цьому підрозділі буде розглянуто створення моделі організаційної одиниці (OU) для домену. OU застосовуються для створення ієрархічної структури в межах домену. Ця ієрархія може використовуватися для делегування адміністративних завдань або застосування групових політик до сукупності об'єктів.

При проектуванні OU, здійснюється групування об'єктів разом з метою єдиного управління цією групою. Наприклад, можна встановити спільний набір програм для всіх користувачів у певному відділі. Групуючи всіх користувачів в OU, можна задати групову політику (Group Policy), яка автоматично встановить необхідне програмне забезпечення. Можна згрупувати об'єкти для призначення одного адміністратора цієї групи. Якщо є віддалений офіс з місцевим адміністратором, можна створити OU, помістити всіх користувачів та комп'ютери віддаленого офісу в цей підрозділ, а потім делегувати адміністрування цієї OU місцевому адміністратору. [7]

При створенні OU бажано дотримуватися деяких правил, а саме:

- Використовувати єдиний шаблон щодо іменування OU у межах домену;
- Після створення облікових записів користувачів, не залишати їх в групах по замовчуванню, а розподіляти по відповідним OU;
- При створенні OU, встановлювати прапорець на захист від випадкового видалення;
- Розглянути можливість створення окремої OU для серверів;
- Відокремлювати облікові записи адміністраторів від облікових записів простих користувачів;
- Не додавати користувачів до адміністративних груп без потреби

Перейдемо до структури домену, яка показана у вигляді діаграми на рис.

2.6.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 36   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

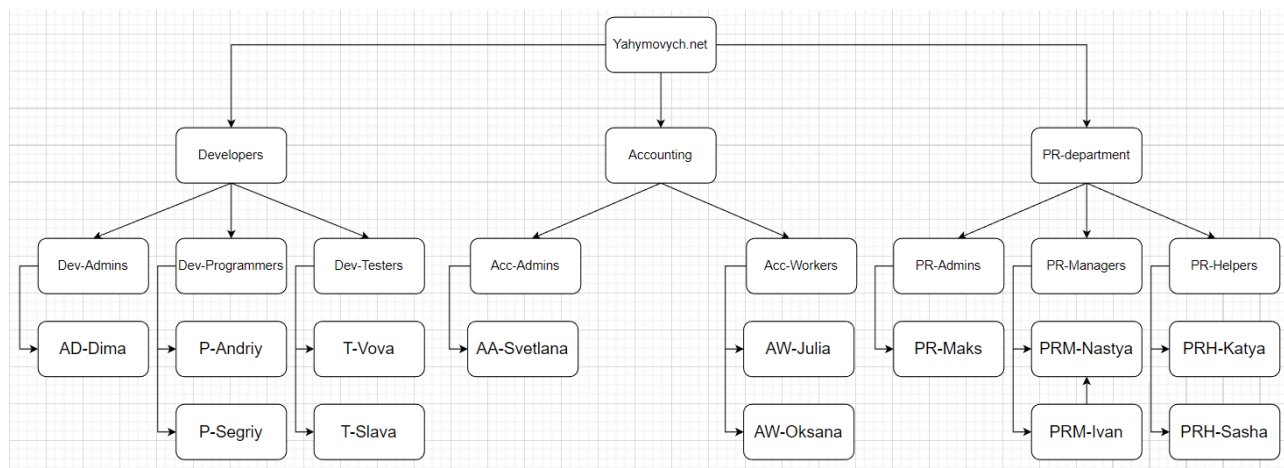


Рисунок 2.6 – Структурна діаграма домену

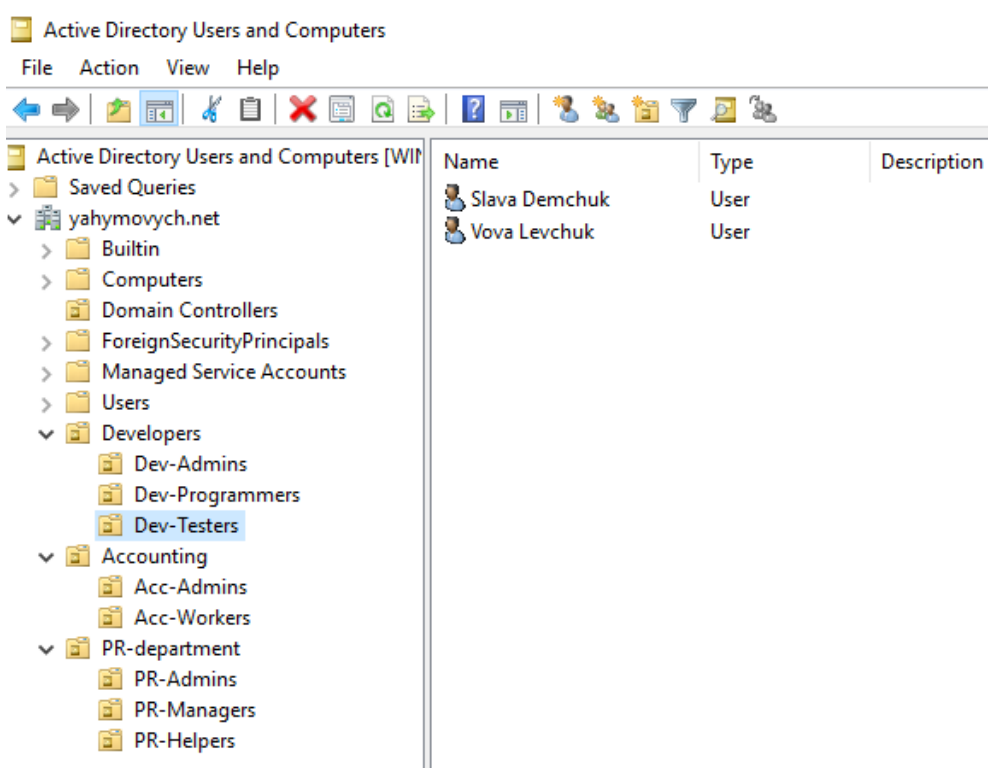


Рисунок 2.6 – Структура на контролері

Користувачам домену було надано спільні папки, через які вони можуть обмінюватися важливими даними. Окрім спільної папки, у кожного користувача є своя персональна папка, завдяки якій можна зберегти важливі документи, при виходу з ладу робочої станції. Також були налаштовані дискові квоти, які дозволяють адміністраторам Windows контролювати скільки місця використову-

ють користувачі на файловій системі серверів. Обмеження дискових квот, зму-  
сять користувачі раціонально розподіляти своє місце на файловій системі сер-  
вера, яке їм було виділено та не засмічувати його непотрібними даними.

## 2.4 Вибір обладнання та програмного забезпечення

Вибір обладнання потрібно робити з врахуванням необхідних параметрів і  
задач які необхідно виконати. Достатня кількість портів, підтримка необхідних  
технологій та протоколів які не обхідні для побудови мережі.



Рисунок 2.7 – Маршрутизатор Cisco 2911/K9

Даний маршрутизатор один із 2900 серії маршрутизаторів, дана модель  
була розроблена для малих та середніх підприємств, які вимагають сучасні тех-  
нологічні рішення, забезпечуючи надійне високопродуктивне підключення до  
мережі. Має можливість розширення кількості портів за рахунок модулів.



Рисунок 2.8 – Комутатор Cisco WS-C2960-24TT-L

Комутатор з великою кількістю портів технології Fast Ethernet та декіль-  
кома портами технології Gigabit Ethernet для під'єднання до маршрутизатора чи  
підключення ще одного комутатора. Підходить для цього комутатор Cisco WS-  
C2960-24TT-L (рисунок 3.2). Даний комутатор має 24 порти технології

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 38   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

FastEthernet та 2 порти технології GigabitEthernet, що повністю задовольняє задані параметри.



Рисунок 2.9 – Точка доступу MikroTik RBCAPGI-5ACD2ND

Дана точка доступу MikroTik, працює одночасно в діапазонах 2,4 ГГц і 5 ГГц. Пропускна здатність пристрою в діапазоні 2,4 ГГц становить до 300 Мб/с, а в 5 ГГц - до 866 Мб/с. Має продуктивний 4-ядерний процесор IPQ-4018 з тактовою частотою 716 МГц і 128 МБ оперативної пам'яті. Додатковою перевагою є 2 порти Gigabit Ethernet. Другий порт має пасивний вихід PoE, що дозволяє легко розширювати мережу. MikroTik можливо не найкращий виробник у світі, але якщо вам потрібна низка можливих конфігурацій, просте налаштування, відношення ціна/якість, то це безумовно хороший вибір.

#### Програмне забезпечення

На всіх робочих станціях мережі встановлена ОС Windows 10, сервера працюють також під управлінням ОС від компанії Microsoft – Windows Server 2019. Active Directory має високий рівень сумісності саме з ОС Windows, оскільки розроблялася передусім для неї. Пристрої на яких встановлена ця ОС, отримують

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          |      |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          | 39   |

регулярні оновлення через служби Windows Update протягом усього терміну підтримки безкоштовно.

**Безпека.** В системі є вбудований антивірус, який захищає систему від шкідливих програм будь-якої складності, тому немає потреби міняти його на інший, які пропонують сторонні компанії. Технологія Windows Hello дозволяє використовувати поряд із PIN біометричні дані. Є рішення для запобігання витоку, що розділяє особисті та робочі дані користувача, зберігає дані в зашифрованому вигляді, контролює та запобігає спробам випадкової або усвідомленої передачі файлів. Корпоративна технологія Credential Guard захищає систему автентифікації Windows та облікові дані користувачів.

**Продуктивність.** ОС легко працює з вікнами програм, віртуальними робочими столами та кількома моніторами. Новий центр повідомлень відкрив доступ до перегляду повідомлень та швидкого перемикання налаштувань.

**Програми та пристрої.** ОС підтримує багато класичних програм та універсальних програм. Користувачі мають доступ до магазину Windows, який забезпечує зручне та безпечне отримання програм. Корпоративні замовники можуть повністю керувати закупівлею та розповсюдженням програм за допомогою Магазину Windows для бізнесу. [16]

Windows Server 2019 – передостання версія (станом на 2022 рік) ОС Windows Server. Випущена наприкінці 2018 року, Windows Server 2019 містить різноманітні нововведення в платформі додатків і безпеці, а також покращену підтримку гібридної хмари. Підтримка Microsoft для цієї серверної ОС триватиме до січня 2024 року, а розширена підтримка триватиме ще п'ять років. І Windows, і Windows Server побудовані на одній кодовій базі. Ось чому вони виглядають майже однаково і виконують багато однакових функцій. Однак Windows Server відрізняється кількома важливими аспектами.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 40   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

По-перше, Windows Server має можливості керування підприємством. Ви можете встановити кілька вбудованих ролей сервера в Windows Server, включаючи протокол динамічної конфігурації хосту (DHCP), Active Directory, служби друку, файли та сховища. Windows Server також не має апаратних обмежень, властивих Windows. Наприклад, Windows Server 2019 може обробляти до 24 ТБ оперативної пам'яті та дозволяє використовувати до 64 роз'ємів процесора, що набагато більше, ніж 2 ТБ оперативної пам'яті та два роз'єми ЦП, дозволені в Windows 10 Pro. Крім того, Windows Server не володіє багатьма функціями, які роблять Windows зручною для звичайних користувачів. Windows Server має іншу модель ціноутворення, ніж Windows – вона, як правило, дорожча. Це не дивно, враховуючи, що Windows Server орієнтована на корпоративне використання. Вам також потрібно сплачувати ліцензії клієнтського доступу (CAL) для користувачів, які мають доступ до комп'ютера Windows Server. [13]

#### Висновки розділу

В другому розділі було створено та показано схему мережі, розписано важливість вибору топології спроектованої мережі, сформовано таблиці IP-адресації для протоколів IPv4 та IPv6, показано структуру домену в Active Directory. Також було обране програмне та апаратне забезпечення, наведені основні характеристики та обґрунтовано вибір тих чи інших компонентів.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 41   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

### 3.1 Базове налагодження обладнання та програмного забезпечення мережі

Мережа була спроектована в програмі GNS3 з використанням VirtualBox. GNS3 – це графічний симулятор мережі, який дозволяє створювати віртуальну мережу. Ця програма надає можливість навчитись налаштовувати обладнання, для проектування мережі є багато різноманітного віртуального обладнання, яке можна встановити і використовувати в своїх проектах.

VirtualBox – це спеціальне програмне забезпечення для віртуалізації, що дозволяє запускати операційну систему всередині іншої. За допомогою VirtualBox ми не тільки можемо запускати ОС, але можемо і налаштовувати мережі, обмінюватися файлами і багато іншого.

Почати слід з налагодження маршрутизаторів мережі.

```
R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#int gig0/0
R_1(config-if)#ip address 200.4.20.1 255.255.255.252
R_1(config-if)#no sh
R_1(config-if)#exit
R_1(config)#ip route 201.4.20.0 255.255.255.128 200.4.20.2
R_1(config)#ip route 202.4.20.0 255.255.255.128 200.4.20.2
R_1(config)#e
*Jun 20 16:18:17.351: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 20 16:18:18.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R_1(config)#exit
R_1#
*Jun 20 16:18:21.027: %SYS-5-CONFIG_I: Configured from console by console
R_1#copy run start
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R_1#
```

Рисунок 3.1 – Налаштування маршрутизатора R\_1

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 42   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

```

R_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_2(config)#int fa1/0
R_2(config-if)#ip address 201.4.20.1 255.255.255.128
R_2(config-if)#no sh
R_2(config-if)#exit
R_2(config)#int fa1/1
R_2(config-if)#ip address 202.4.20.1 255.255.255.128
R_2(config-if)#no sh
R_2(config-if)#ip helper-address 201.4.20.2
R_2(config-if)#exit
R_2(config)#
*Jun 20 16:12:56.547: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Jun 20 16:12:56.659: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Jun 20 16:12:57.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R_2(config)#
*Jun 20 16:12:57.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
R_2(config)#exit
R_2#
*Jun 20 16:13:03.863: %SYS-5-CONFIG_I: Configured from console by console
R_2#copy run start
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_2(config)#int gig0/0
R_2(config-if)#ip address 200.4.20.2 255.255.255.252
R_2(config-if)#no sh
R_2(config-if)#exit
R_2(config)#co
*Jun 20 16:17:02.039: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 20 16:17:03.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R_2(config)#exit
R_2#
*Jun 20 16:17:17.843: %SYS-5-CONFIG_I: Configured from console by console
R_2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R_2#

```

Рисунок 3.2 – Налаштування маршрутизатора R\_2

На рисунку з налаштуванням маршрутизатора R\_2 можна побачити, як налаштовується DHCP relay agent. На порті маршрутизатора сусідньої підмережі вказується IP-адреса контролеру домену, який в мережі виступає також в ролі DHCP-сервера.

Далі буде показано встановлення ОС Windows Server 2019 для серверів, та ОС Windows 10 для клієнтів мережі.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 43   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

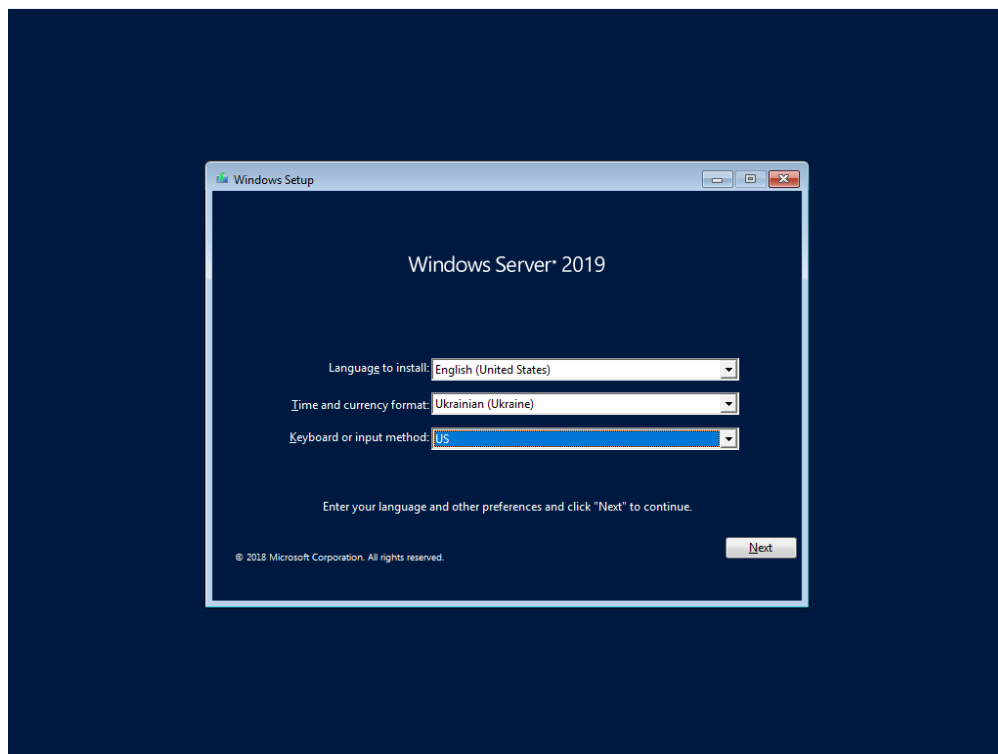


Рисунок 3.3 – Вибір мови, часового поясу та розкладки клавіатури

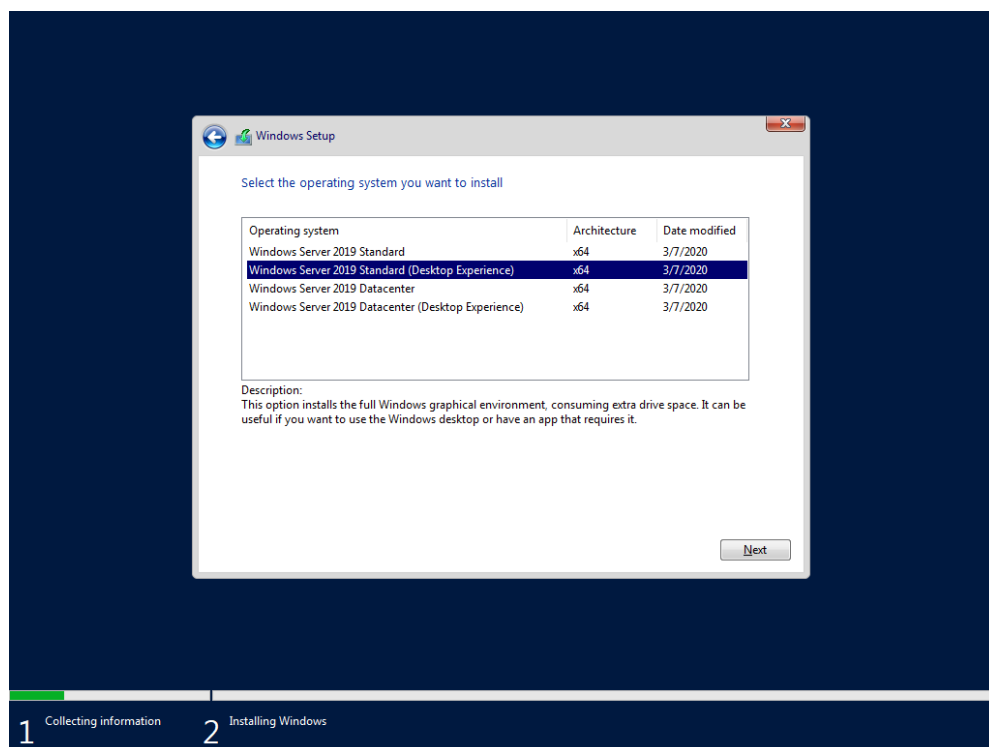


Рисунок 3.4 – Вибір версії ОС

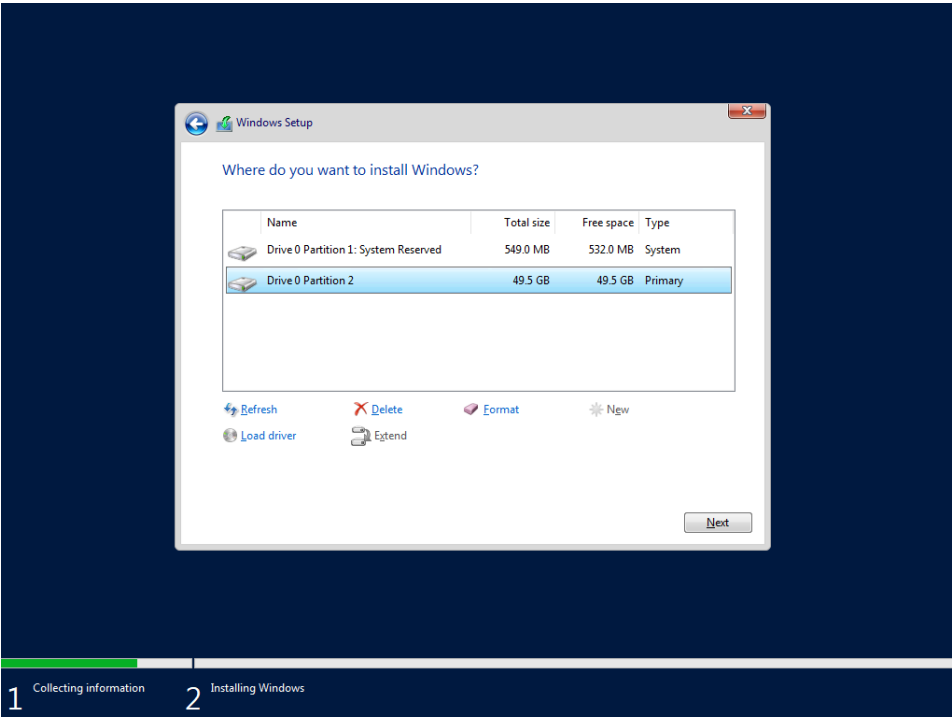


Рисунок 3.5 – Розподілення дискового простору

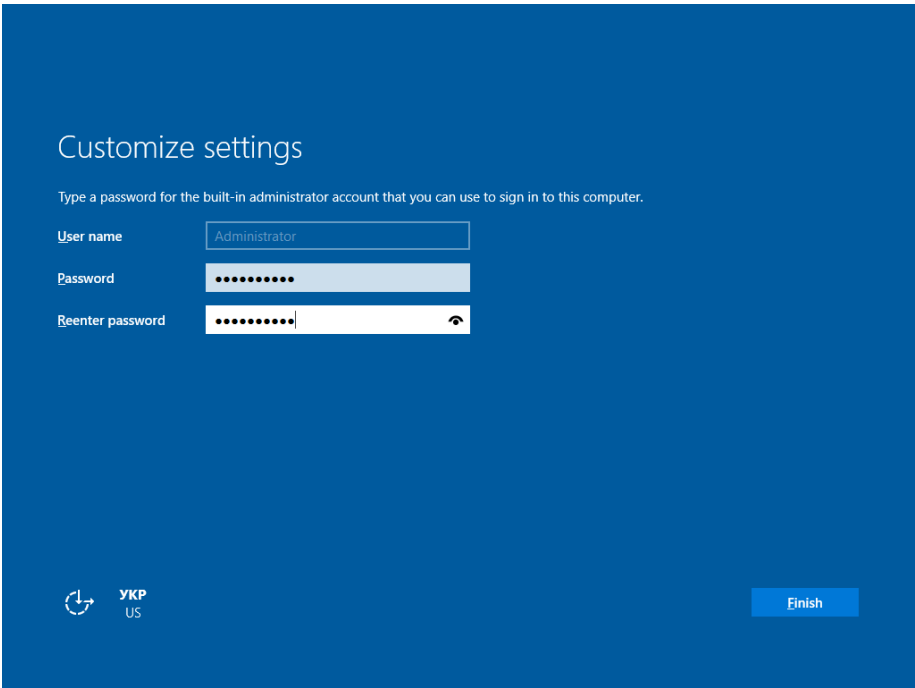


Рисунок 3.6 – Встановлення паролю облікового запису

Пароль повинен бути не менше 8 символів та має містити хоча б 1 велику літеру.

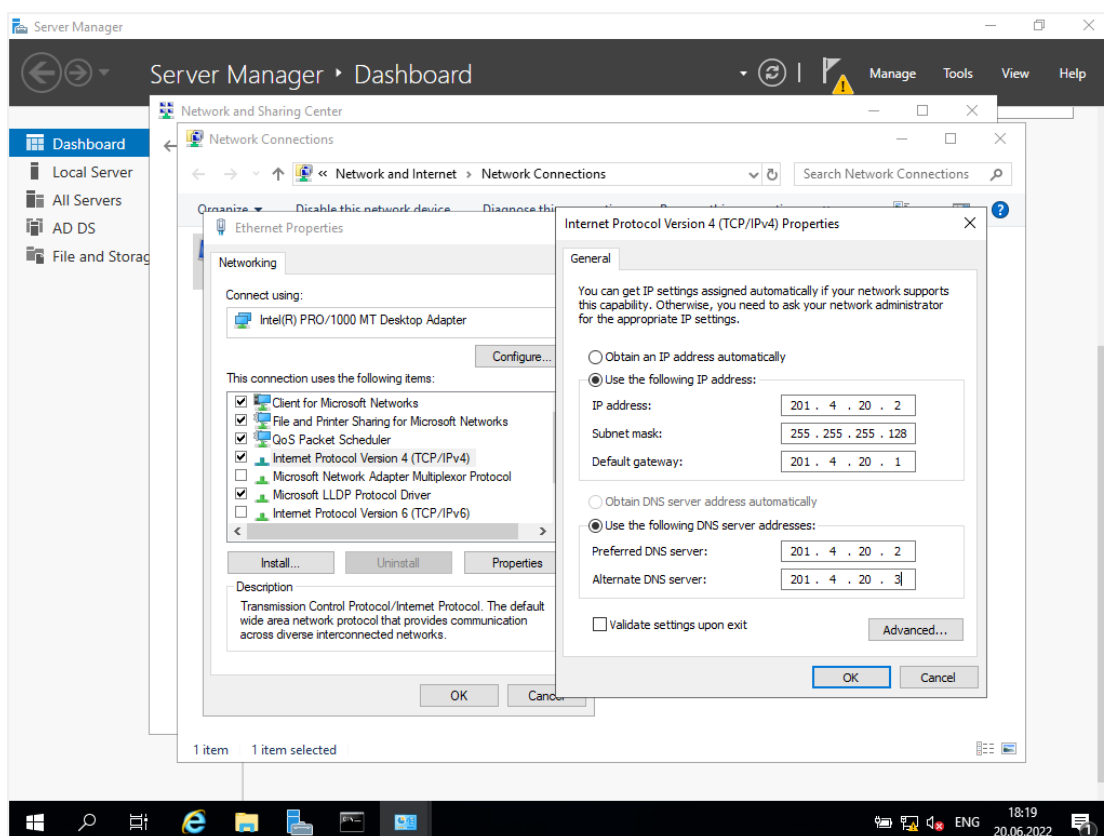


Рисунок 3.7 – Налаштування IP-адреси Server\_1

### 3.2 Налаштування сервісів локальної комп'ютерної мережі

Першим сервісом, який буде встановлений та налаштований на сервері це доменні служби Active Directory, створений домен мережі та доданий основний та додатковий сервер в ролі контролера домену.

Натискаю Додати роль і функції на інформаційній панелі. Відкриється майстер додавання ролей та функцій. У списку ролей вибираю служби Active Directory Directory, та очікую встановлення (рис. 3.8).

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 46   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

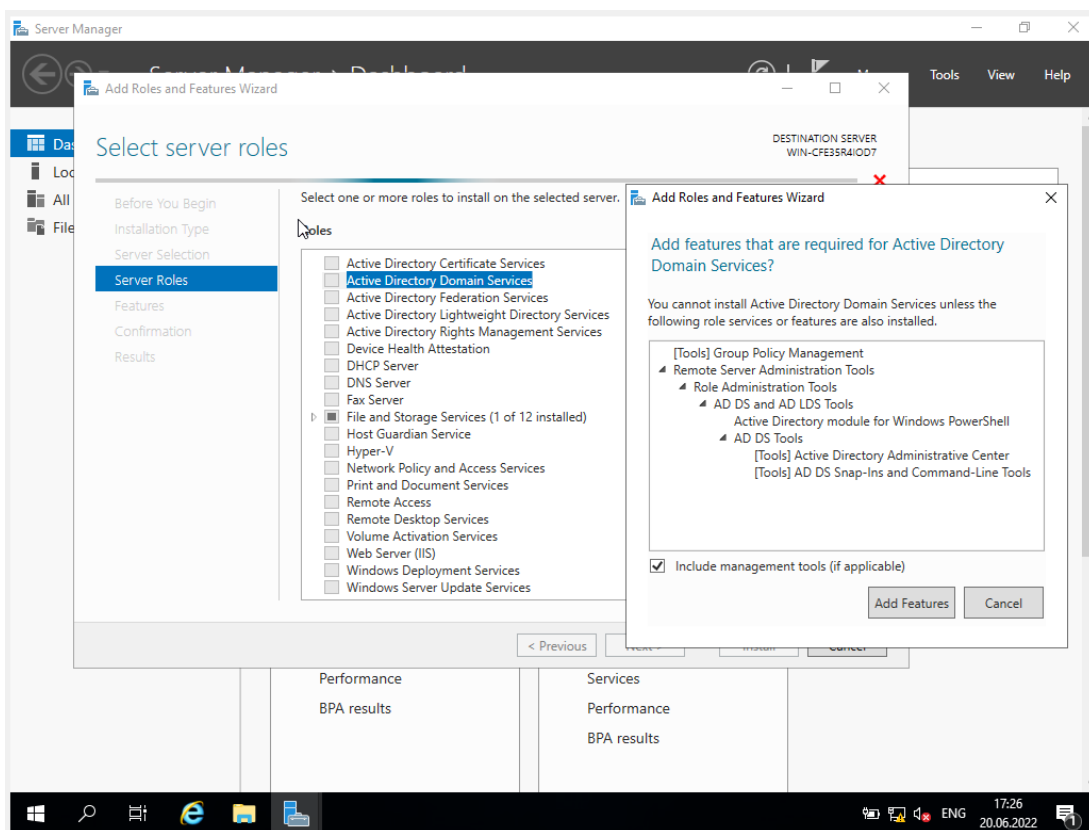


Рисунок 3.8 – Вибір ролей

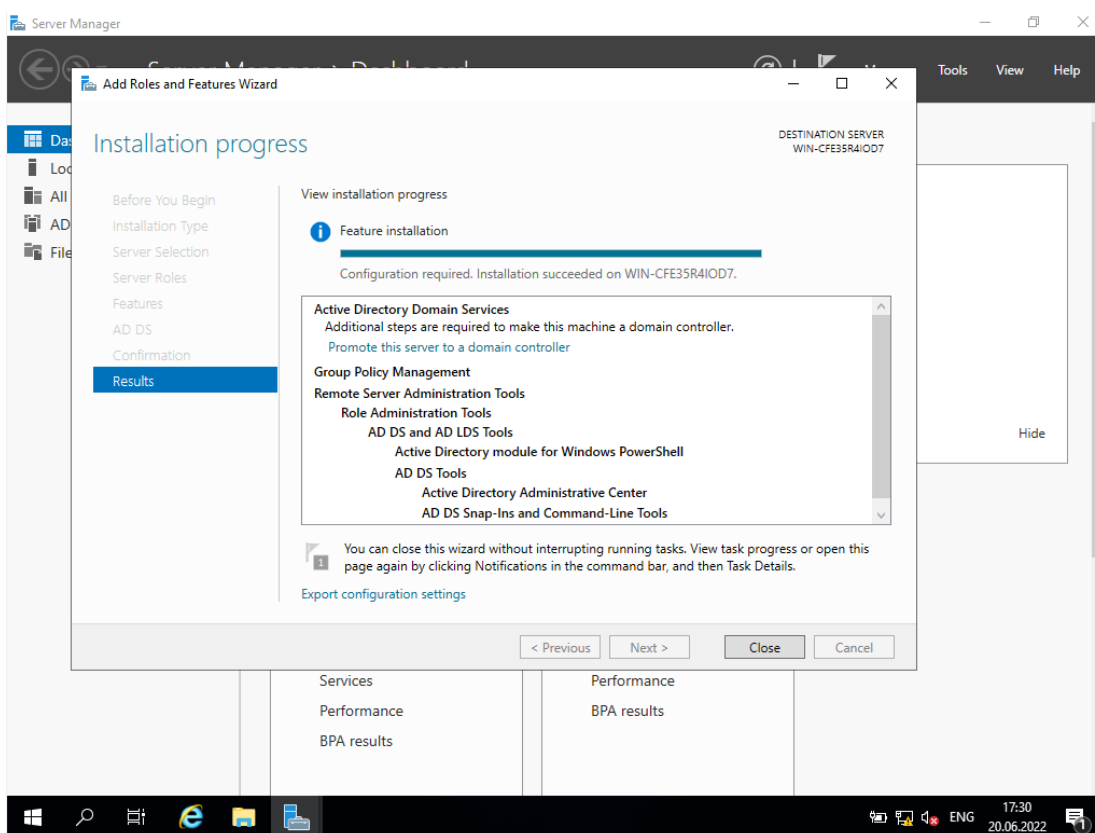


Рисунок 3.9 – Успішне встановлення

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 47   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Створюю домен та підвищую сервер до контролера домену (рис. 3.10).

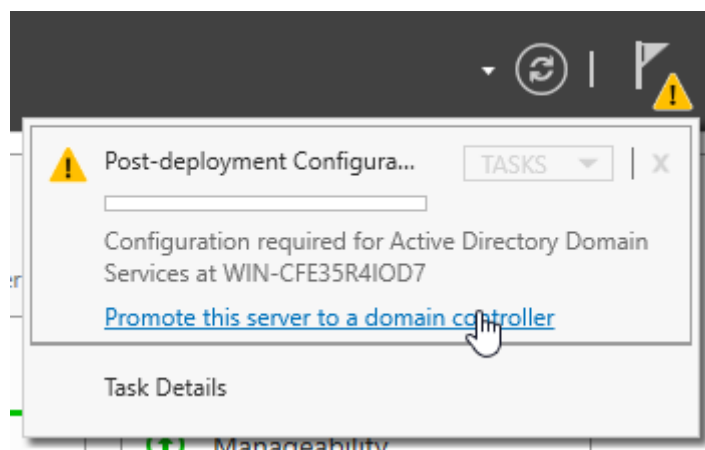


Рисунок 3.10 – Перехід до налаштувань AD DS

Створюю новий ліс та ввожу назву нового домену (3.11).

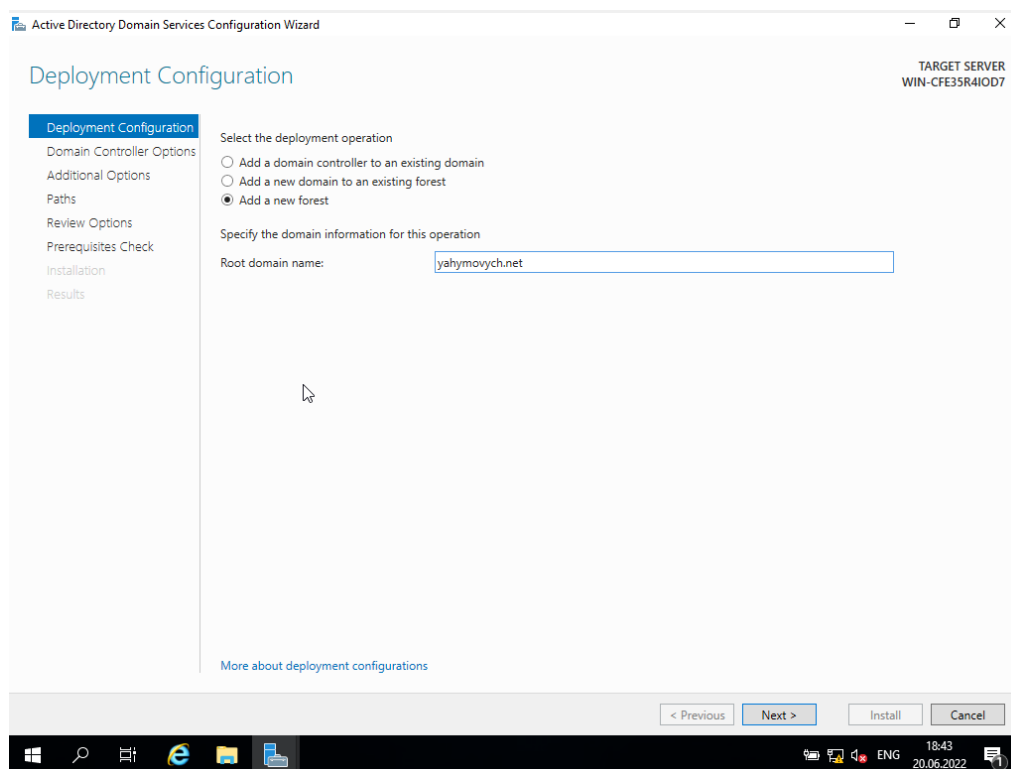


Рисунок 3.11 – Створення домену

Задаю пароль, який потребується для інсталяції (рис. 3.12)

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 48   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

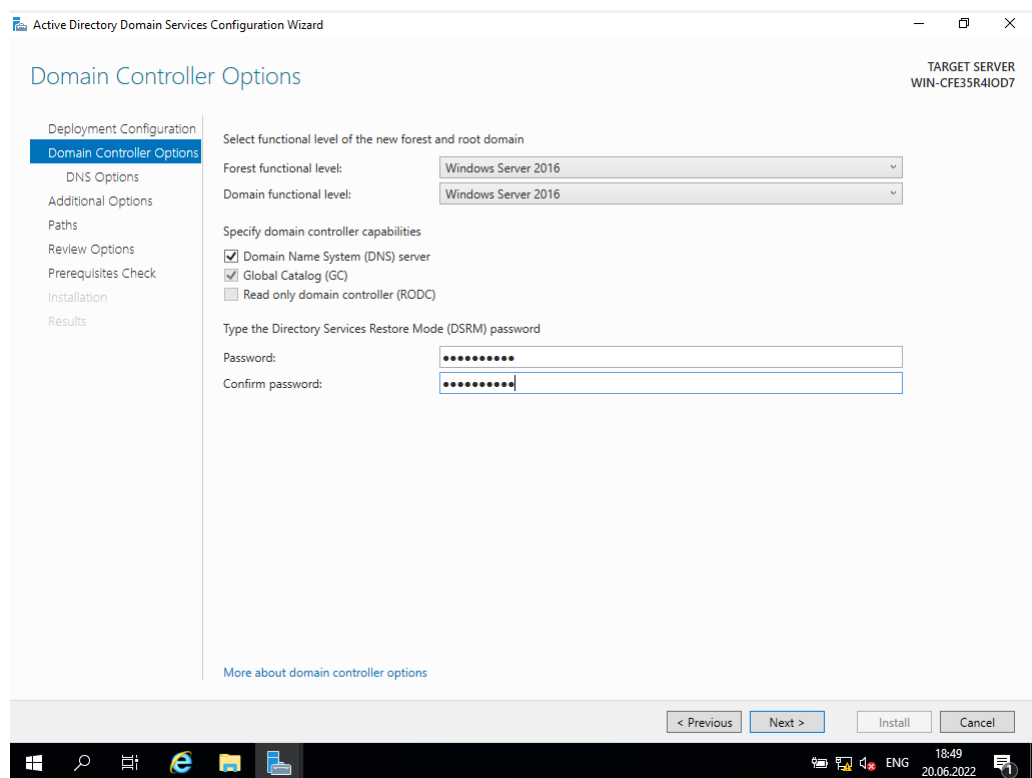


Рисунок 3.12 – Пароль

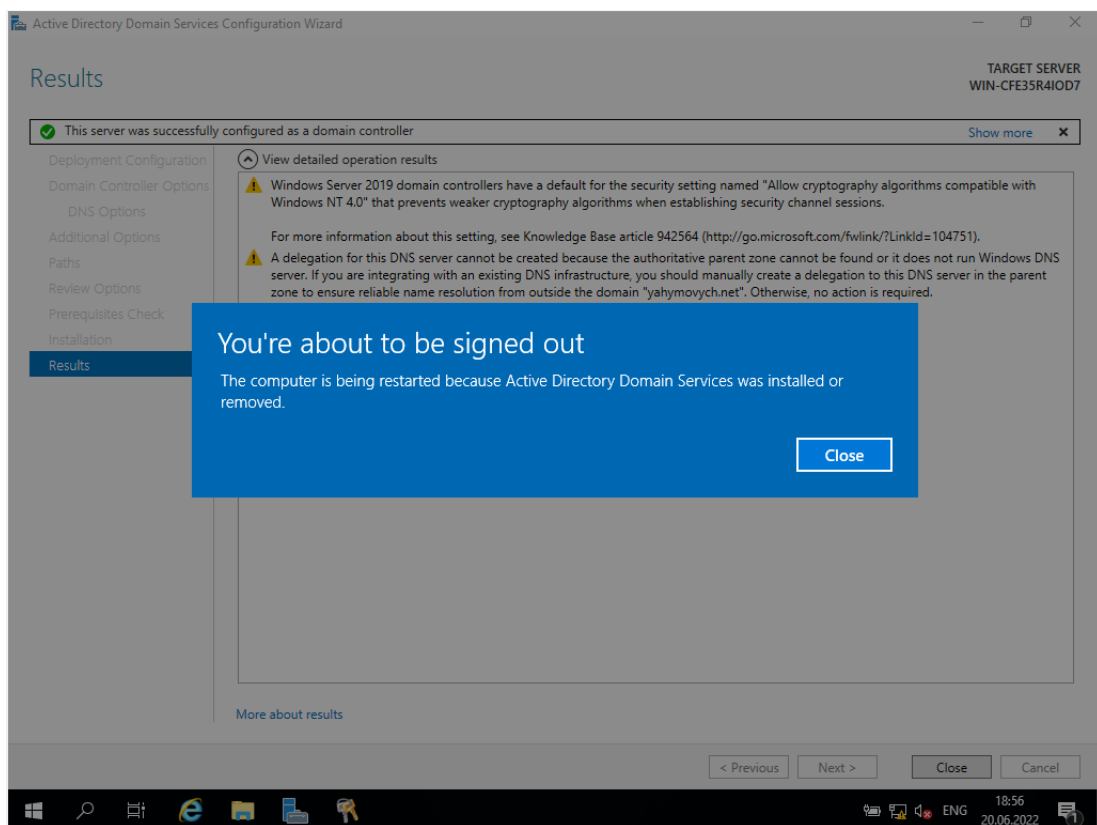


Рисунок 3.13 – Завершення встановлення та перевантаження

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 49   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Додаю другий контролер в створений домен (рис. 3.14)

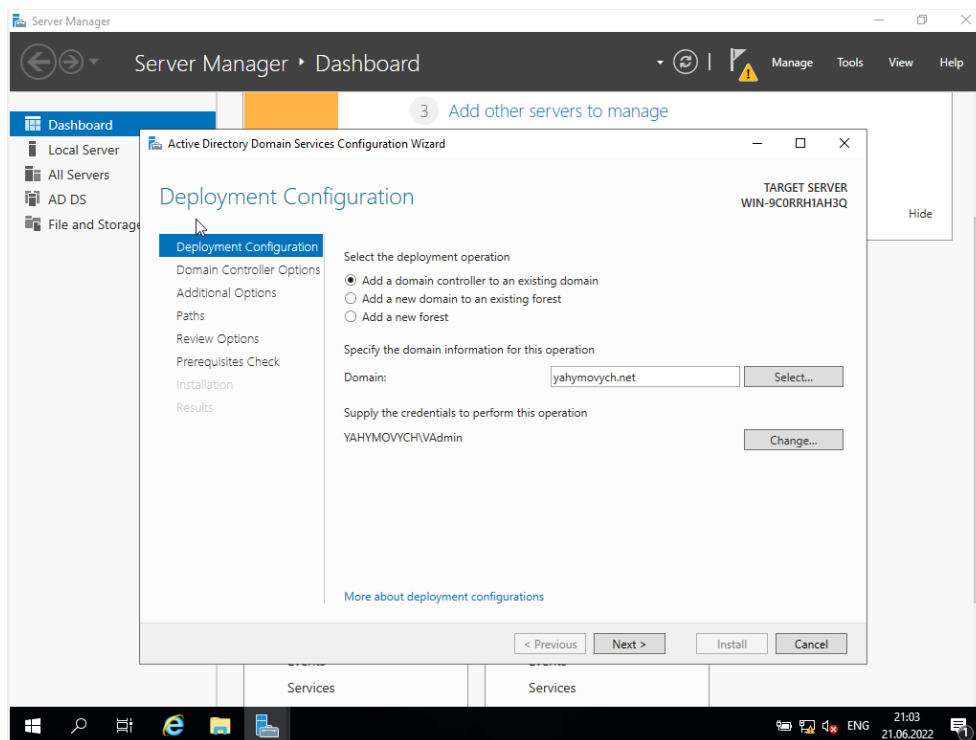


Рисунок 3.14 – Додавання другого контролера домену

Перевіряю наявність контролерів у відповідному оснащенні (рис. 3.15)

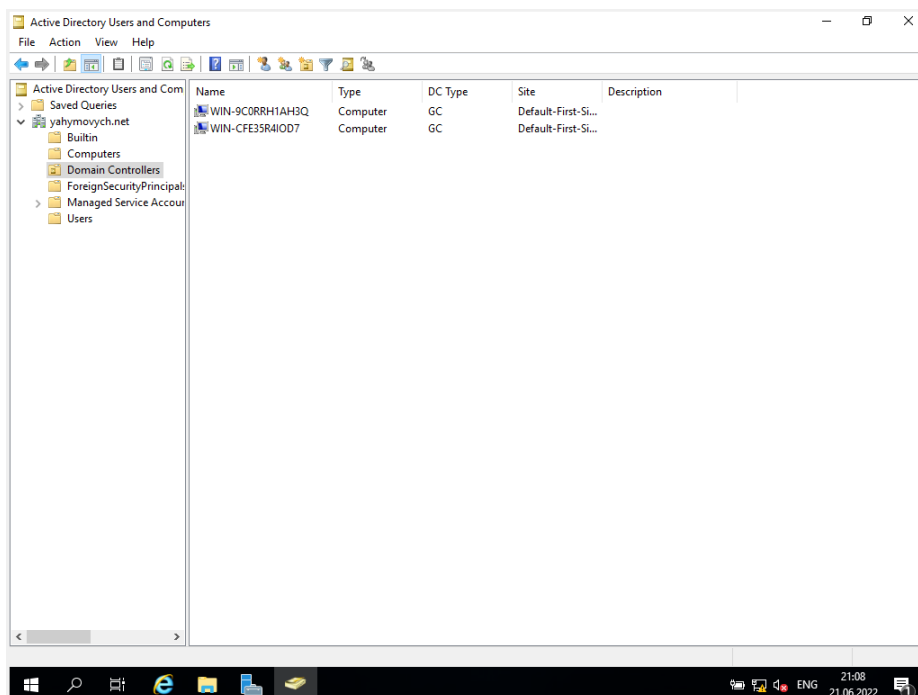


Рисунок 3.15 – Список наявних контролерів домену

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 50   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Встановлюю DNS на контролер домену (рис. 3.16)

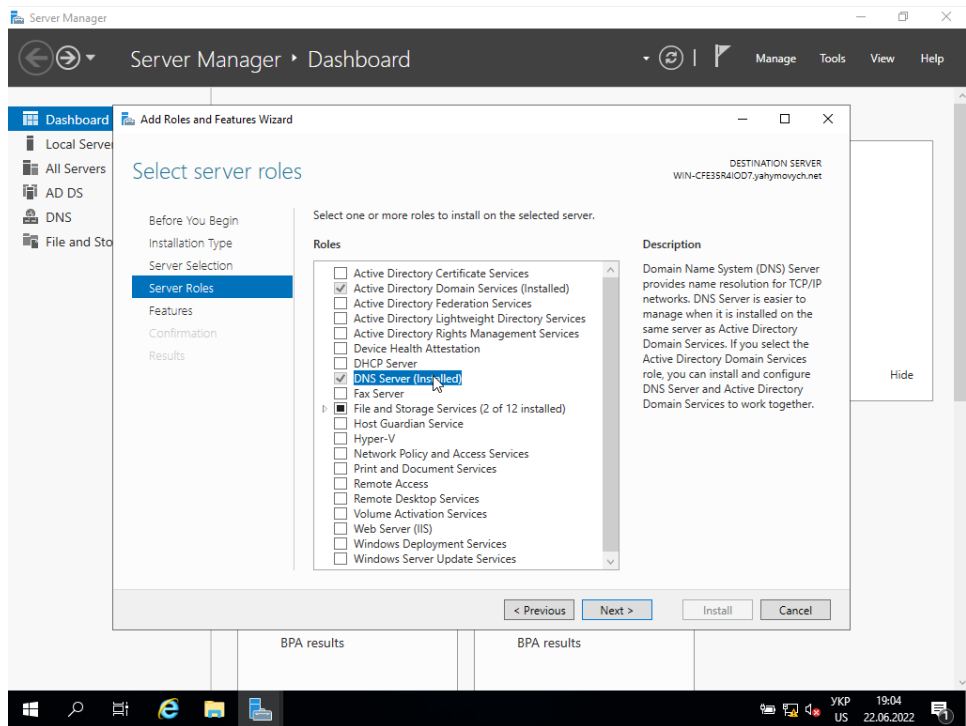


Рисунок 3.16 – Встановлення ролі DNS-сервера

Додаю DNS-запис для порту маршрутизатора (рис. 3.17)

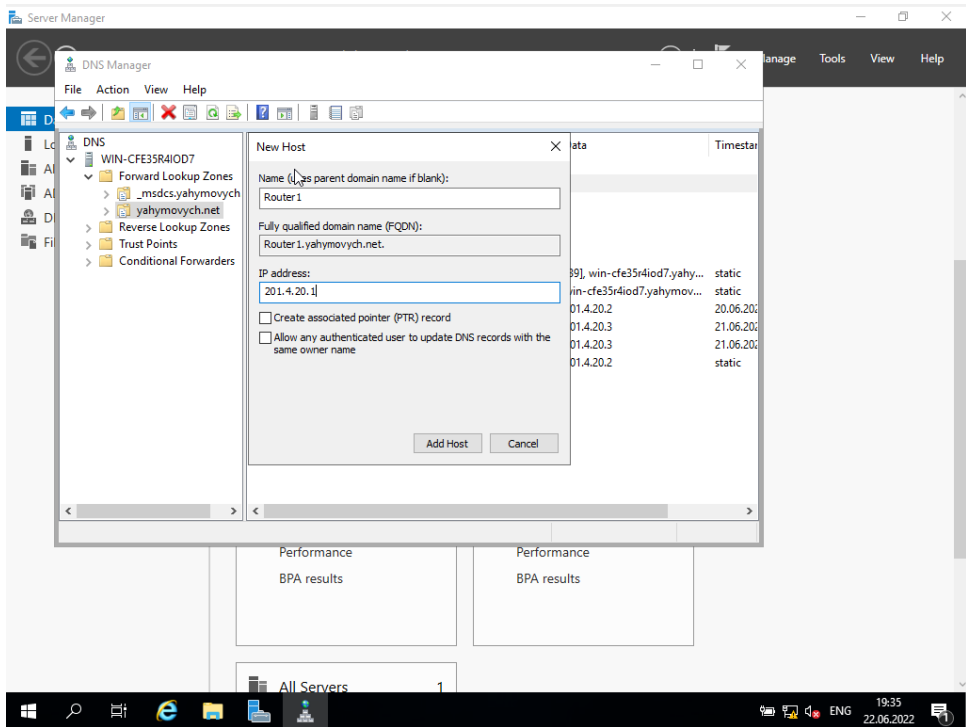


Рисунок 3.17 – Додавання DNS-запису

## Створення зони зворотнього перегляду

Створюю нову зону через оснащення DNS Manager (рис. 3.18)

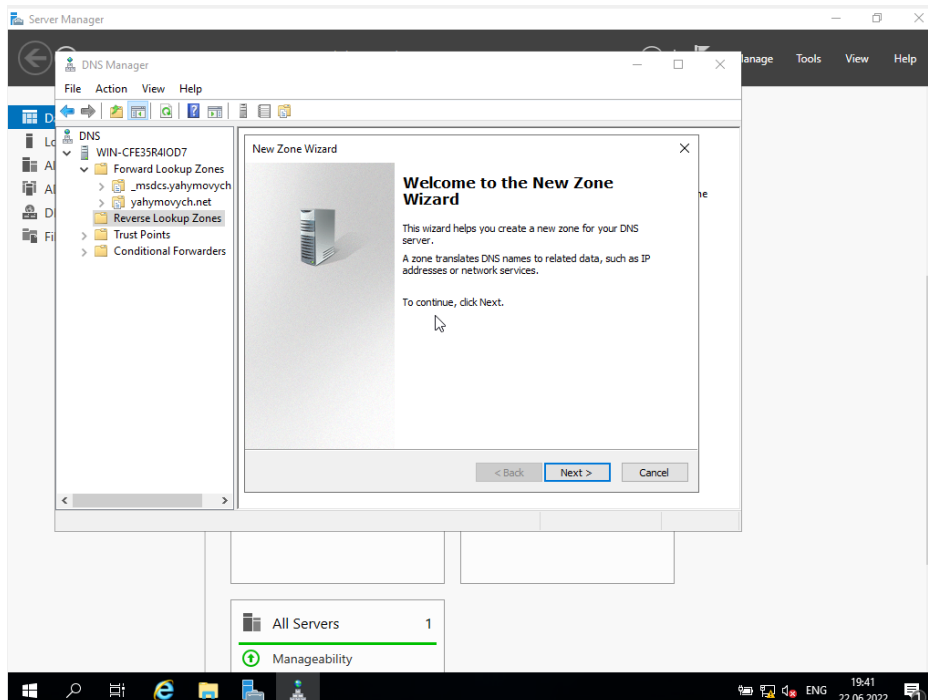


Рисунок 3.18 – Майстер створення зон

Обираю первинну зону (primary zone), щоб майбутню зону зворотного перегляду було створено на поточному сервері (рис. 3.19)

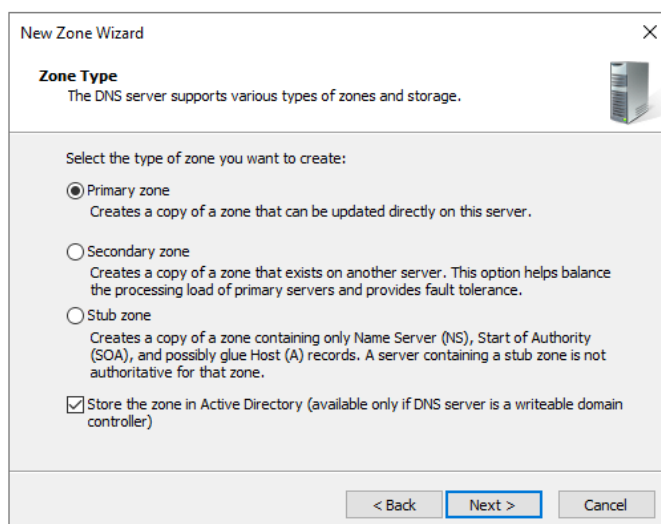


Рисунок 3.19 – Вибір типу зони

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 52   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Обираю зону реплікації для створюваної зони DNS - у даному випадку реплікація даних буде відбуватися з цієї зони DNS на всіх DNS-серверах, організованих на контролерах домену (рис. 3.20)

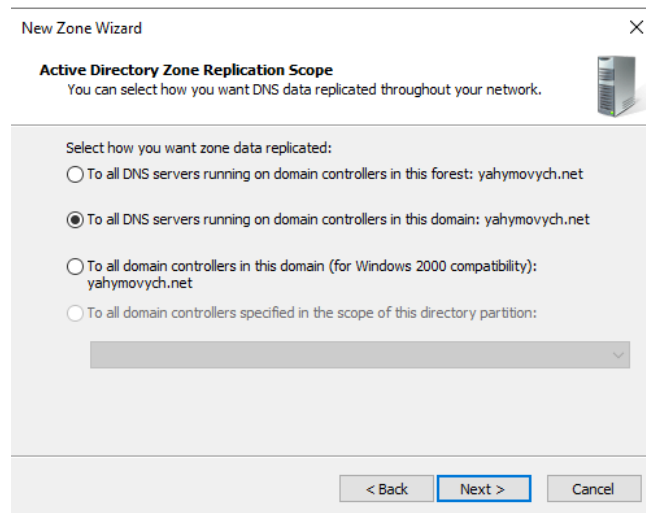


Рисунок 3.20 – Зона реплікації

Вказую, версію IP-протоколу, яка буде використовуватися у створюваній зоні зворотного перегляду (рис. 3.21)

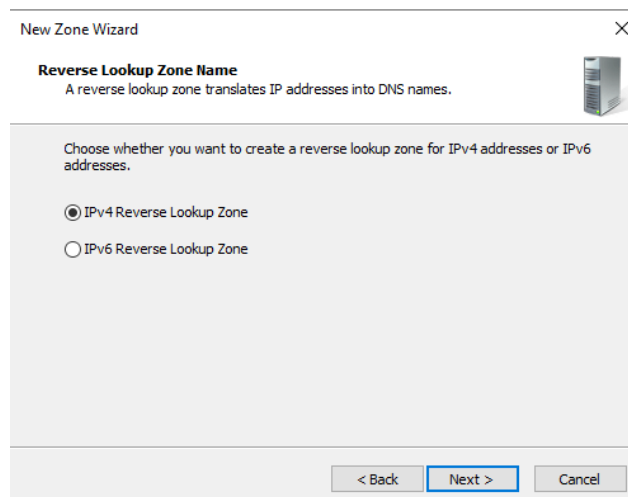


Рисунок 3.21 – Версія протоколу для зони

Вказую ім'я створюваній зоні зворотного перегляду (рис. 3.22)

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 53   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

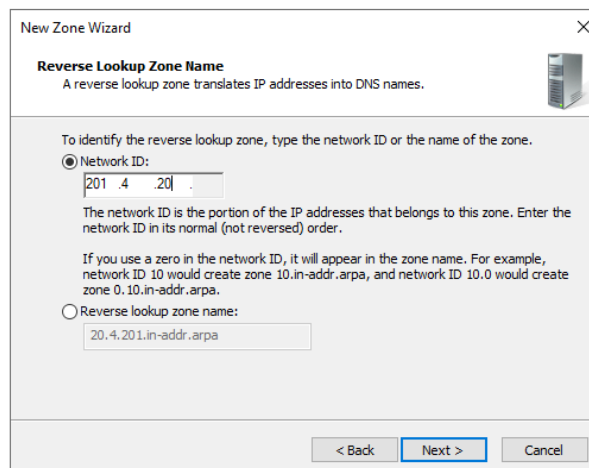


Рисунок 3.22 – Ім'я зони зворотнього перегляду

Налаштовую динамічне оновлення створюваної зони DNS. Такі оновлення будуть відбуватися лише з довірених джерел (рис. 3.23)

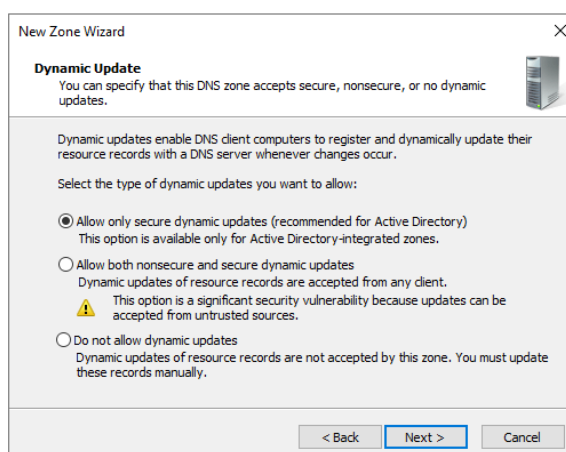


Рисунок 3.23 – Динамічні оновлення

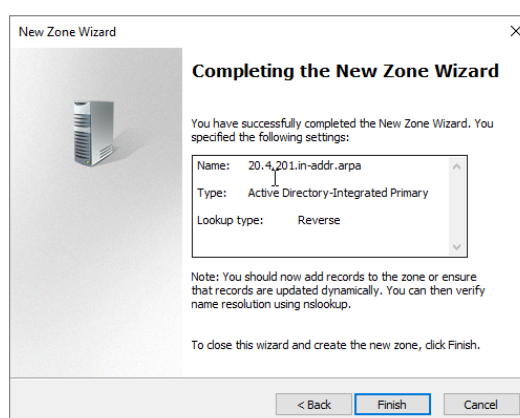


Рисунок 3.24 – Завершення

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 54   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## Налаштування DHCP-сервера

### Встановлення ролі DHCP-сервера (рис 3.25)

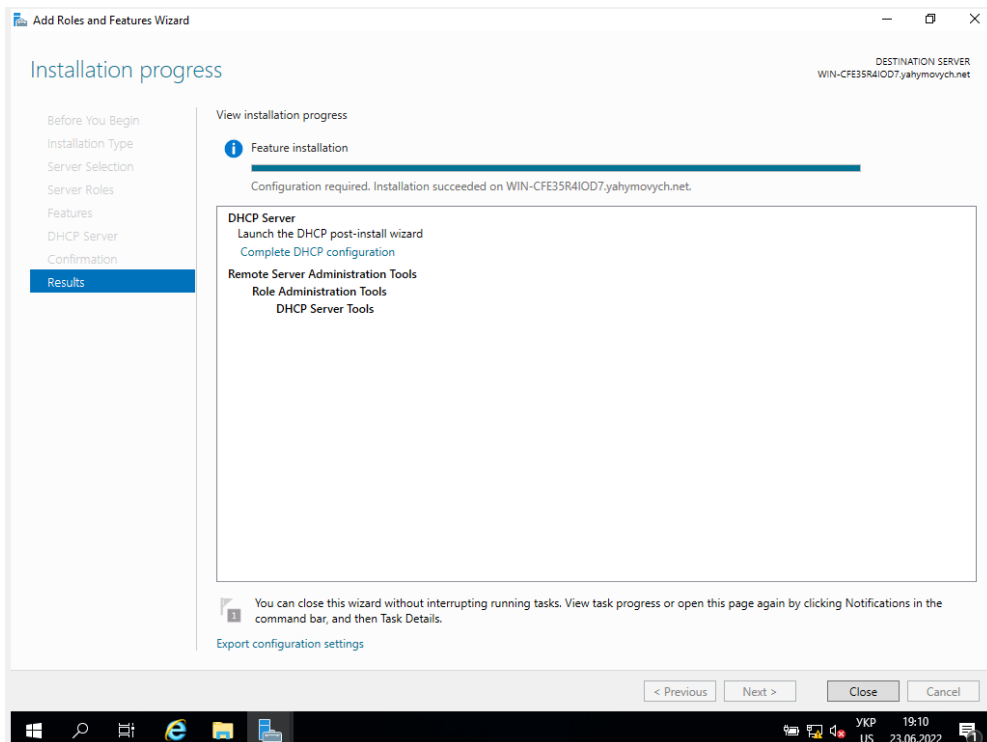


Рисунок 3.25 – Успішне встановлення.

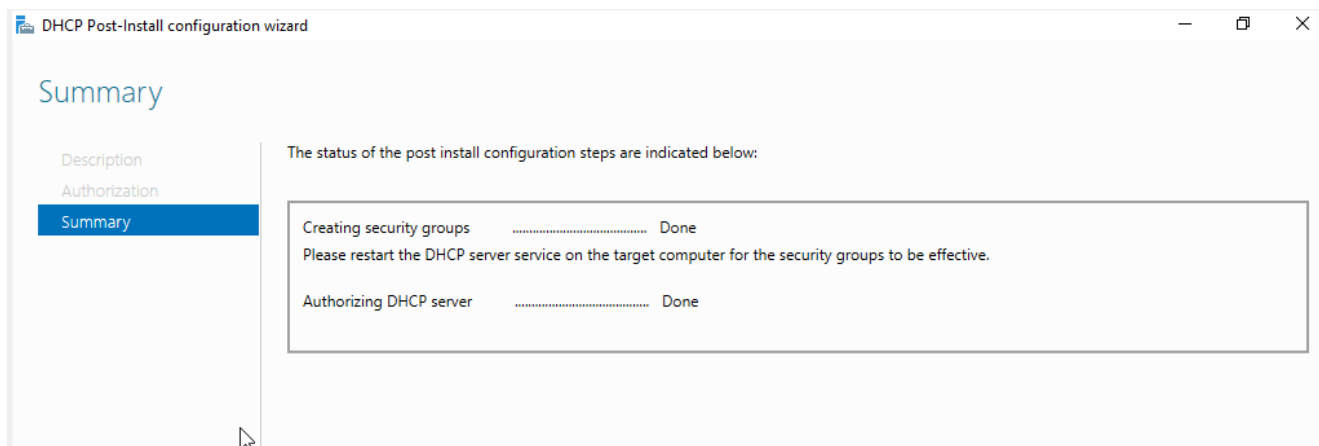


Рисунок 3.26 – Доналаштування

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 55   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

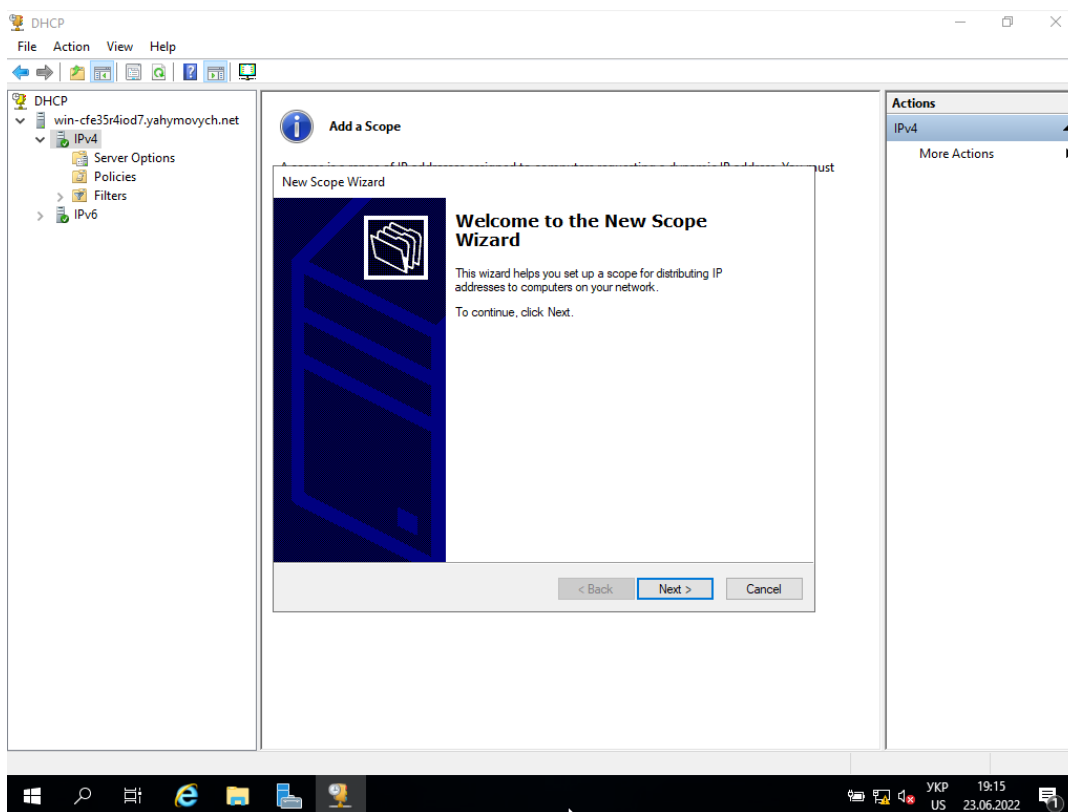


Рисунок 3.27 – Майстер областей

Вказую ім'я та опис для області (рис 3.28)

New Scope Wizard

**Scope Name**  
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back Next > Cancel

Рисунок 3.28 – Ім'я області

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 56   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Вказав початкову та кінцеву IP-адресу підмережі та маску (рис. 3.29)

Рисунок 3.29 – Діапазон адрес

Додаємо діапазон адрес, які не будуть використовуватися для автоматичного присвоєння пристроям мережі, а задані статично для серверів і порту маршрутизатора (рис.3.30)

Рисунок 3.30 – Діапазон виключених IP-адрес



Вибираю другий контролер домену для налаштування (3.33)

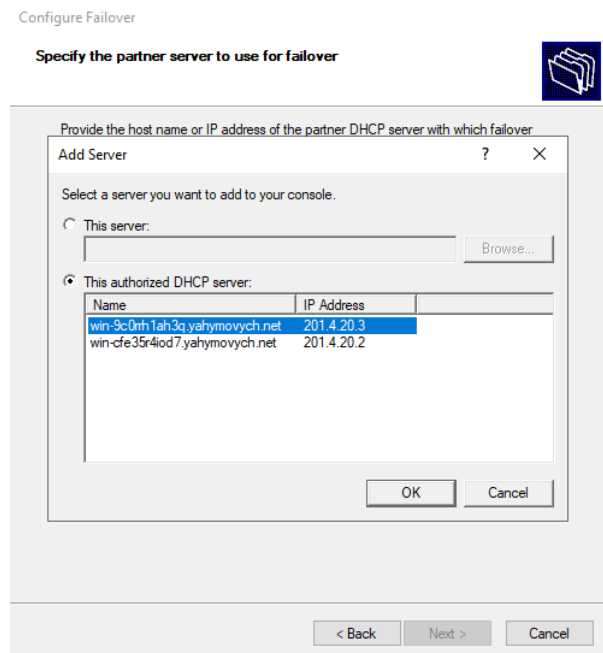


Рисунок 3.33 – Вибір другого контролера

Вибрані налаштування та встановлення. Другий контролер буде працювати в режимі “Гарячої заміни”, тобто у випадку виходу з ладу першого контролеру або запланованого технічного обслуговування, другий візьме на себе всю роботу (рис. 3.34)

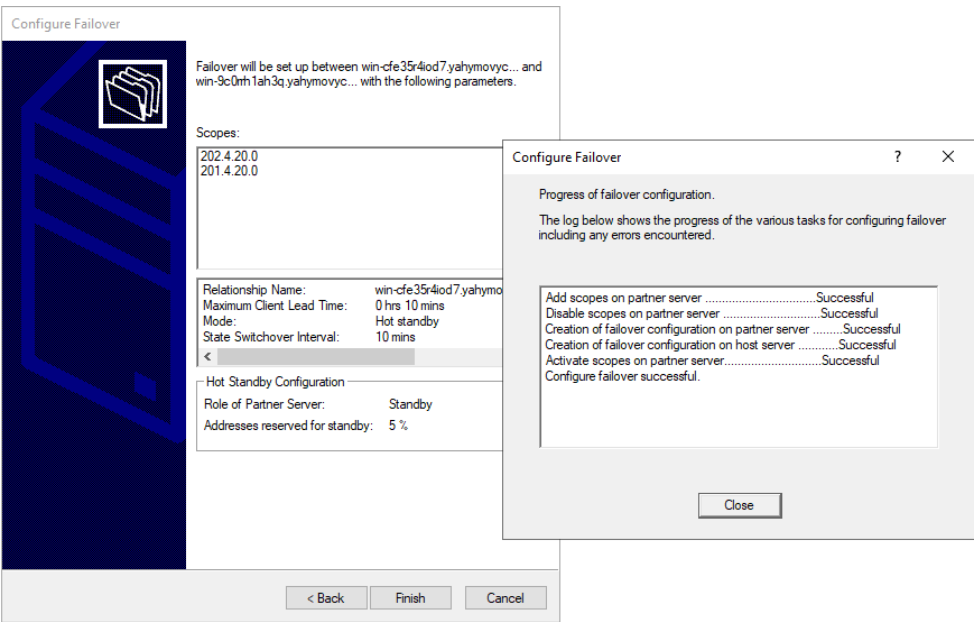


Рисунок 3.34 – Вибрані налаштування та успішне встановлення

Було здійснене налаштування служб віддаленого робочого столу

Встановлюю необхідні служби для роботи (рис. 3.36)

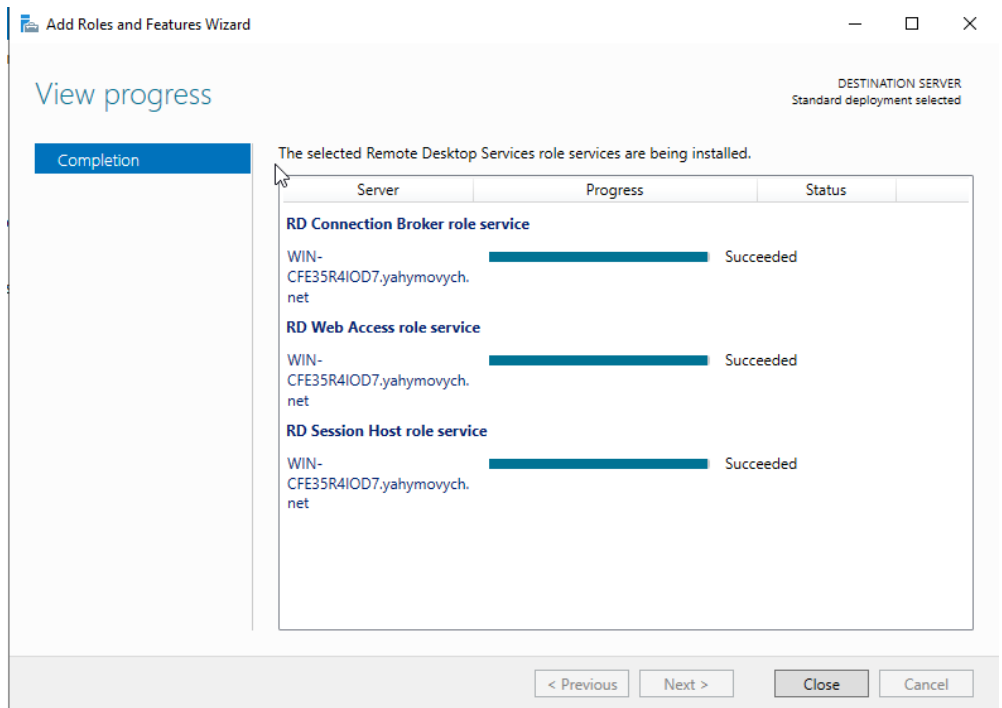


Рисунок 3.36 – Завершення установки

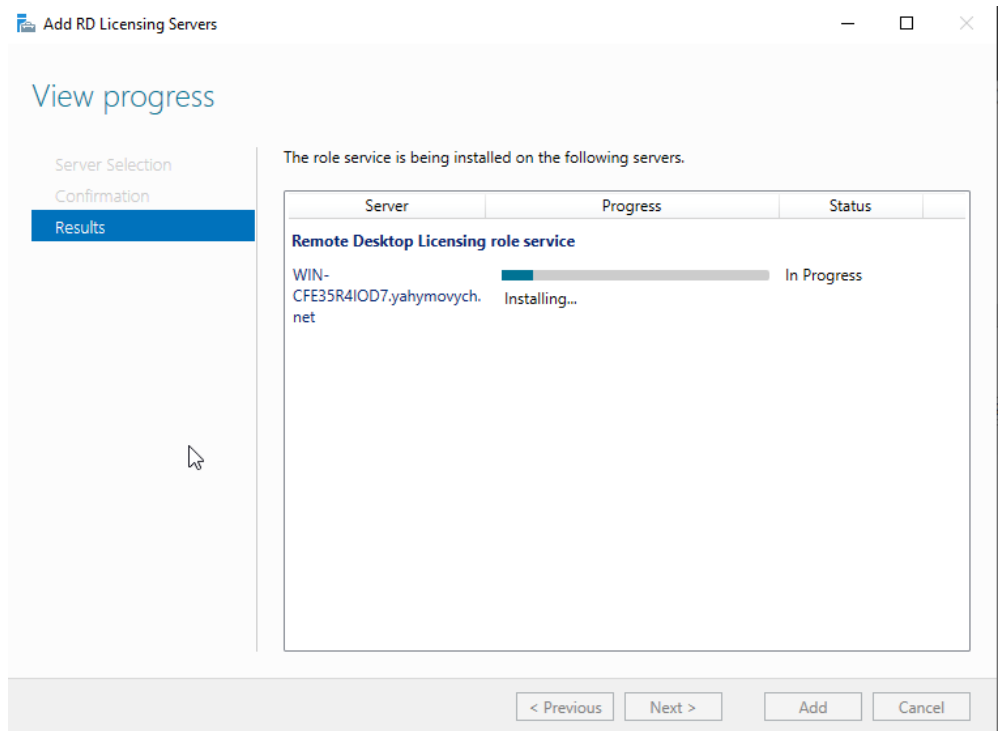


Рисунок 3.37 – Роль сервера ліцензій

У властивостях системи на контролері домену, вказую групу користувачів, яка зможе мати доступ до віддалених сервісів (рис.3.38)

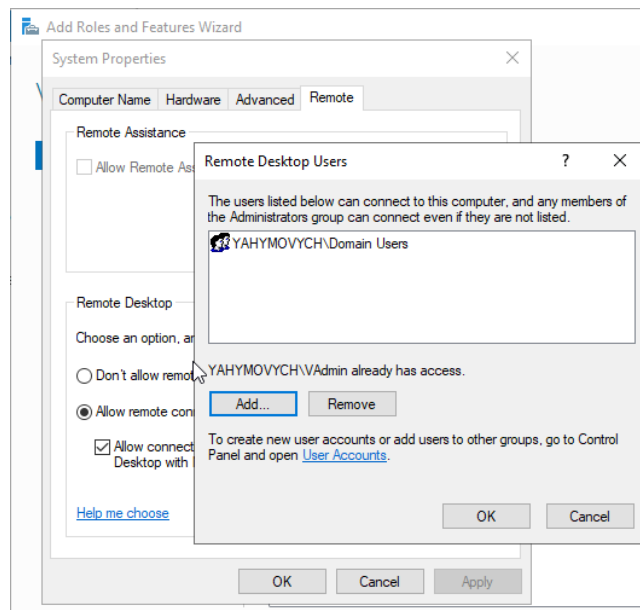


Рисунок 3.38 – Дозвіл на віддалене підключення

Вказую, що ліцензування буде здійснюватися у режимі Per User і переконаюсь, що у ролі серверу ліцензування обрано перший контролер домену (рис. 3.39)

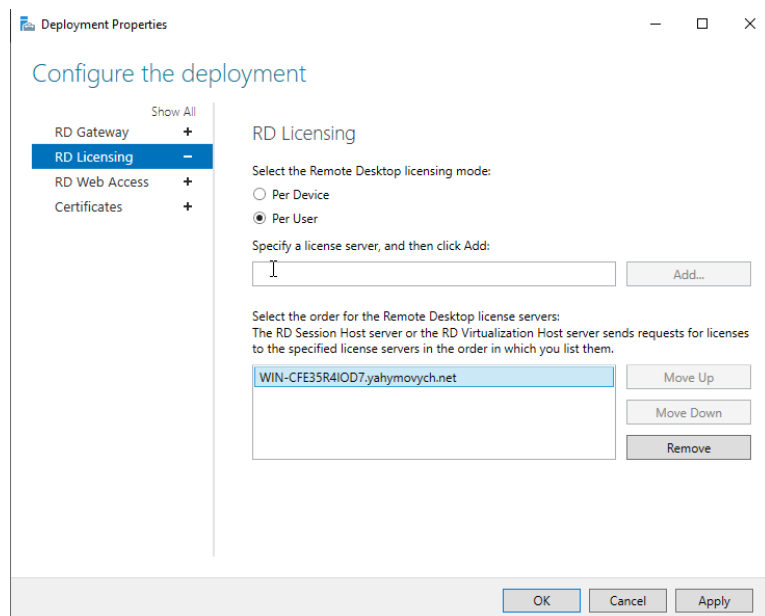


Рисунок 3.39 – Доналаштування RD Licensing

Далі створюю сертифікат, який використовуватиметься для ліцензування, а також задаю пароль (рис. 3.40)

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -dnsname "RDP"

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\my

Thumbprint                               Subject
-----
578863532F7AA29DB19193C12E71E9B9211A8FE9  CN=RDP

PS C:\Windows\system32> $pwd = ConvertTo-SecureString -String "str0ng" -Force -AsPlainText
```

Рисунок 3.40 – Сертифікат і пароль

Додаю інструмент у MMC-консоль (рис. 3.41). MMC (Microsoft Management Console) – це засіб створення, збереження та відкриття адміністративних інструментів, званими консолями (consoles) [17]

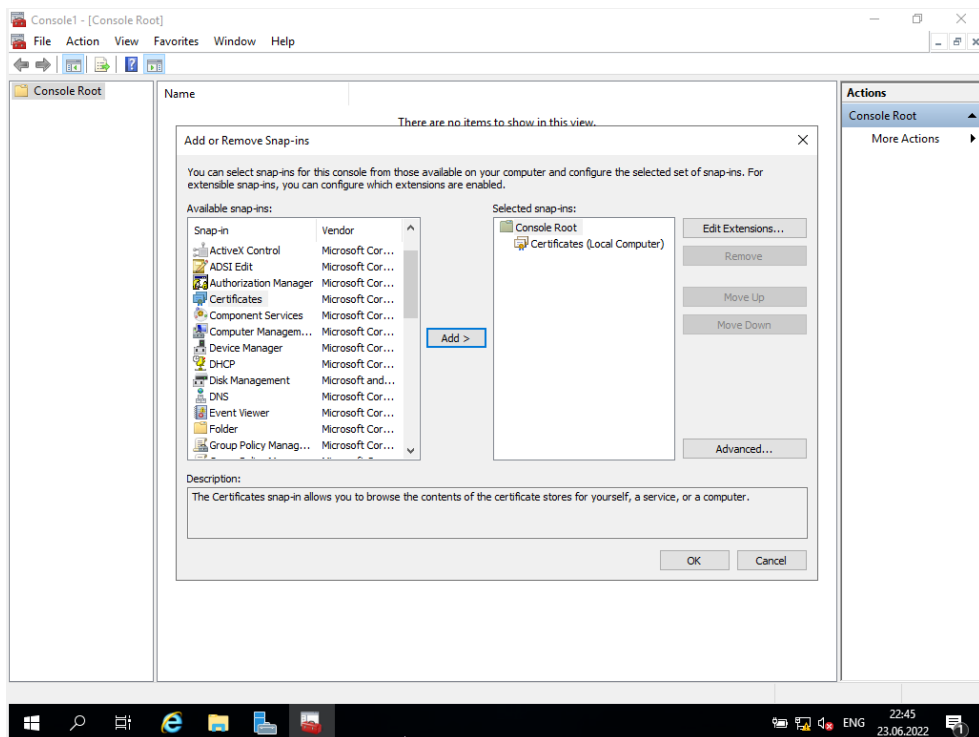


Рисунок 3.41 – Консоль MMC

Виконую експорт необхідного сертифікату (рис. 3.42)

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 62   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

|                                                    |                                       |
|----------------------------------------------------|---------------------------------------|
| File Name                                          | C:\Users\Admin\Desktop\RDP_Certifi    |
| Export Keys                                        | Yes                                   |
| Include all certificates in the certification path | Yes                                   |
| File Format                                        | Personal Information Exchange (*.pfx) |

Finish

Cancel

Рисунок 3.42 – Експорт сертифікату

Провожу ліцензування сервісів за допомогою експортованого сертифікату (рис. 3.43)

## Configure the deployment

- Show All
- RD Gateway +
  - RD Licensing +
  - RD Web Access +
  - Certificates -**

### Manage certificates

A Remote Desktop Services deployment requires certificates for server authentication, single sign-on, and establishing secure connections.

Current deployment certificate level is **Untrusted**

[What is a certificate level?](#)

| Role Service                       | Level     | Status | State   |
|------------------------------------|-----------|--------|---------|
| RD Connection Broker - Enable Sing | Untrusted | OK     | Success |
| RD Connection Broker - Publishing  | Untrusted | OK     | Success |
| RD Web Access                      | Untrusted | OK     | Success |
| RD Gateway                         | Unknown   | --     |         |

Subject name: CN=RDP

[View Details](#)

This certificate is required to enable RemoteApp and Desktop Connection subscription and server authentication for RD Web Access.

You can update this certificate by creating a new certificate or by selecting an existing certificate.

Create new certificate...

Select existing certificate...

OK

Cancel

Apply

Рисунок 3.43 – Ліцензування

|      |      |               |        |      |
|------|------|---------------|--------|------|
|      |      | Яхимович В.С. |        |      |
|      |      | Головня О.С.  |        |      |
| Змн. | Арк. | № докум.      | Підпис | Дата |

КІК.КР.Б – 123 – 20 – ПЗ

Арк.

63

Створення DNS-запису про відповідну віддалену службу (рис 3.44).

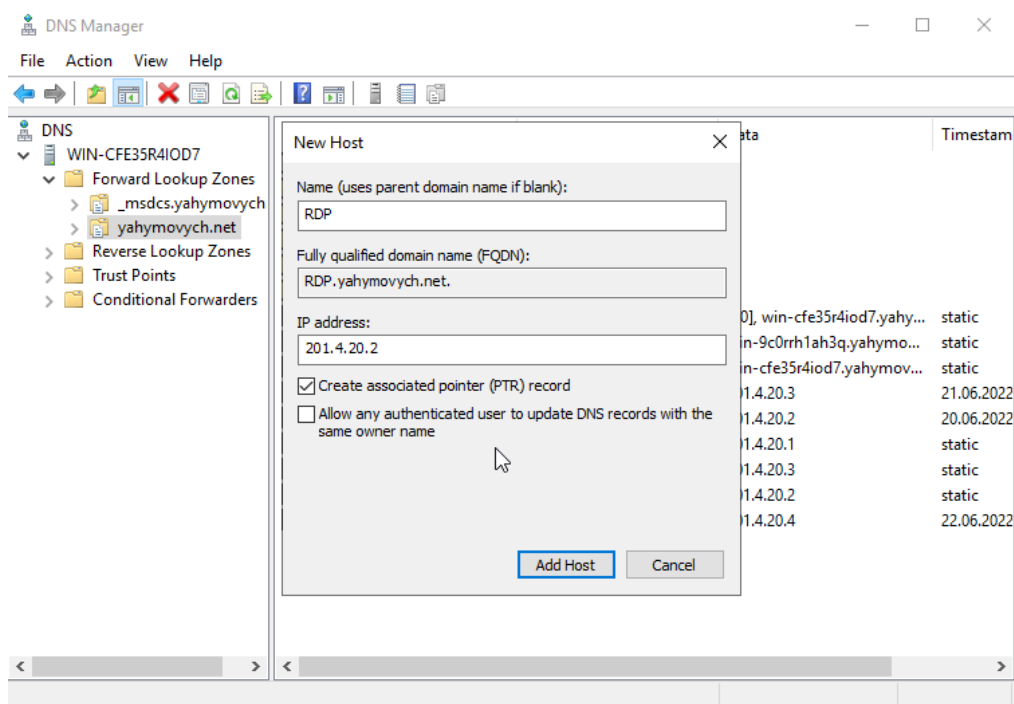


Рисунок 3.44 – Створення DNS-запису

Створення колекції в які будуть додані відповідні програми, для віддаленого доступу (рис. 3.45)

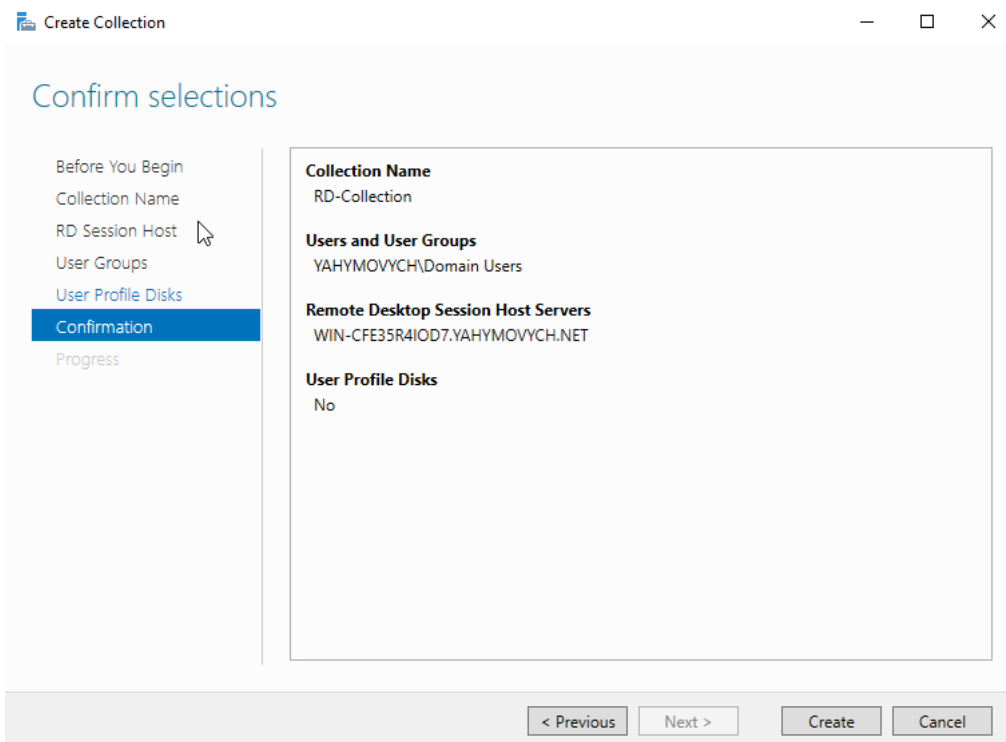


Рисунок 3.45 – Створення колекції

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 64   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

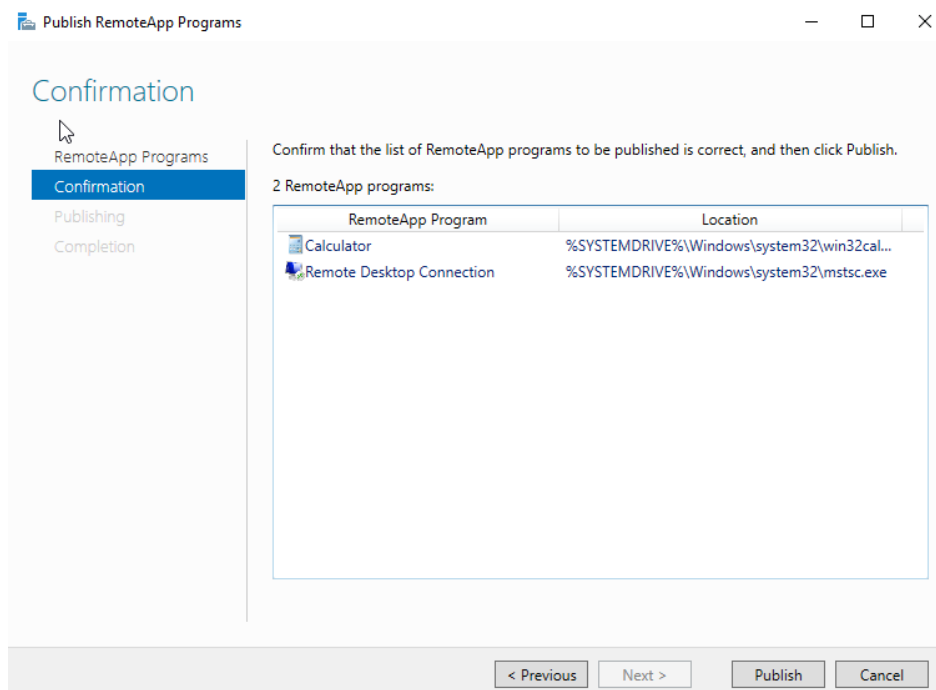


Рисунок 3.46 – Додавання програм в колекцію

Налаштування IIS та запуск сайту

Створюю папку на системному диску для файлів сайту (рис. 3. 47)

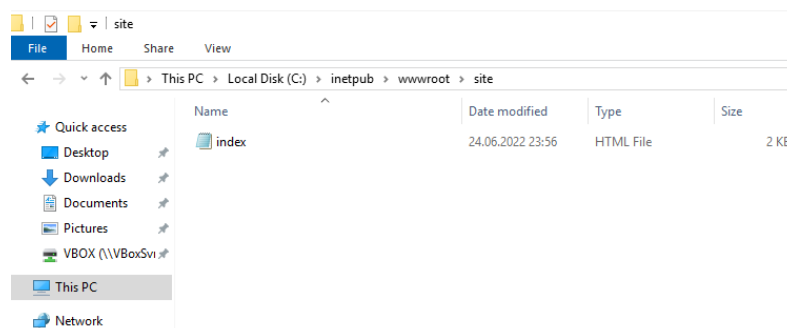


Рисунок 3.47 – Файли сайту

Додаю вебсайт через відповідний менеджер, вказую шлях до папки з файлами сайту, вказую назву сайту (рис. 3.48)

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 65   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

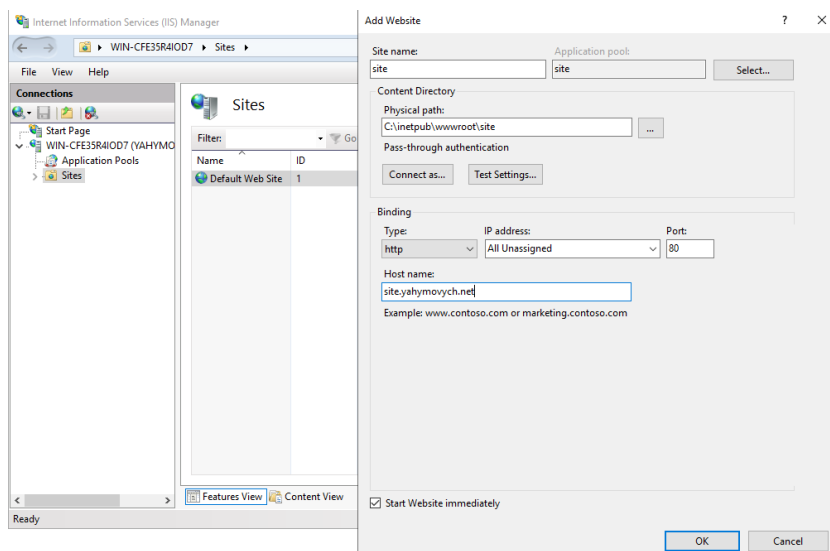


Рисунок 3.48 – Створення нового сайту в IIS Manager

Створення DNS-запису про сайт (рис 3.49)

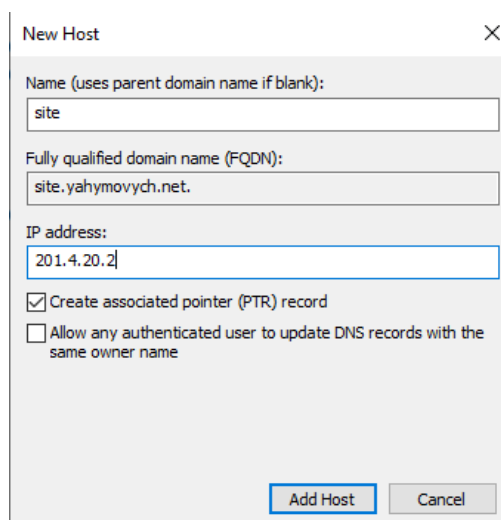


Рисунок 3.49 – Створення DNS запису

Перехожу за відповідною адресою та перевіряю працездатність сайту. Для перевірки роботи була зверстана проста форма реєстрації на html (рис. 3.73).

За допомогою даного веб-серверу OU Programmers можуть запускати локально сайт, а OU Testers переходити на сайт і відповідно проводити тестування розробленого сайту та відправляти відомості про помилки через спільні папки.

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 66   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Налаштування папок для користувачів та квот

Створюю нову групову політку для OU Developers за допомогою консолі ММС та у розділі конфігурацій користувачів призначаю нову спільну папку (рис 3.50)

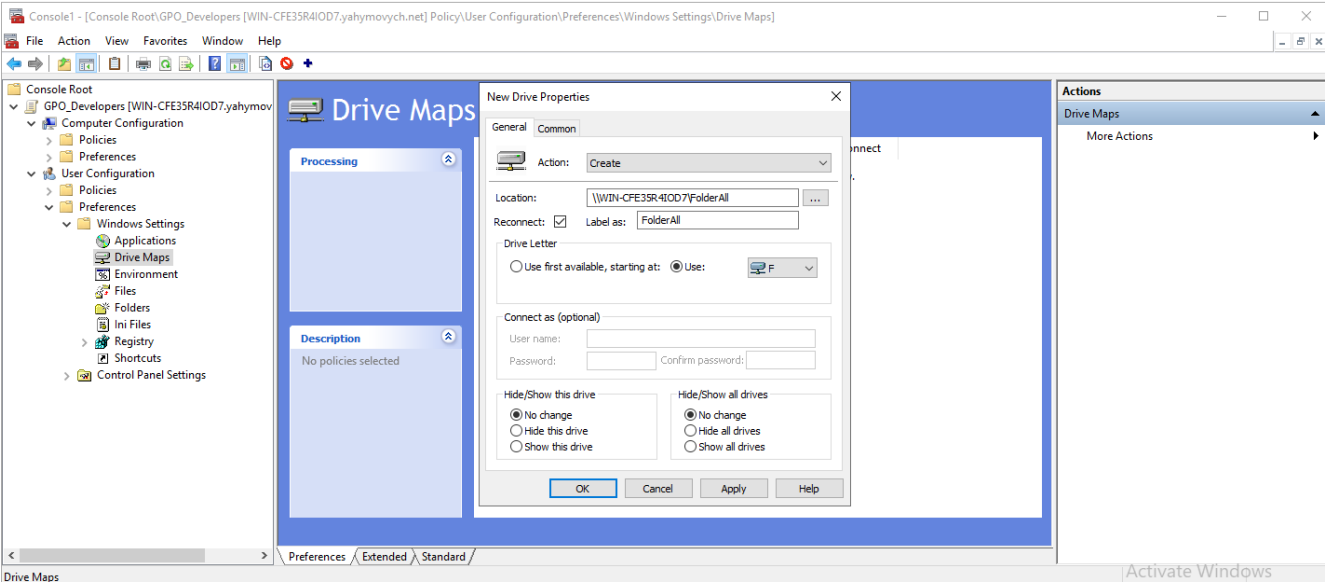


Рисунок 3.50 – Створення спільної папки

Створюю особисті папки для користувачів (рис 3.50)

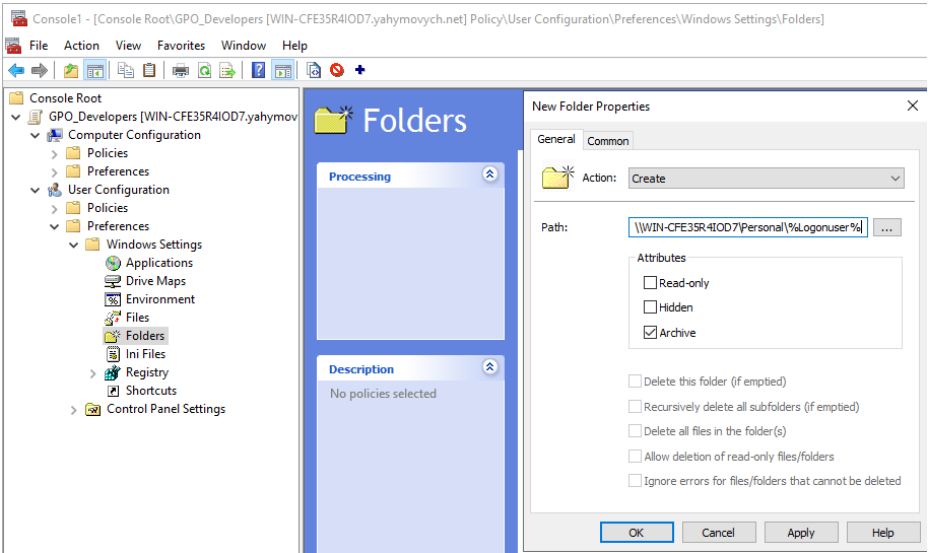


Рисунок 3.51 – Налаштування особистих папок

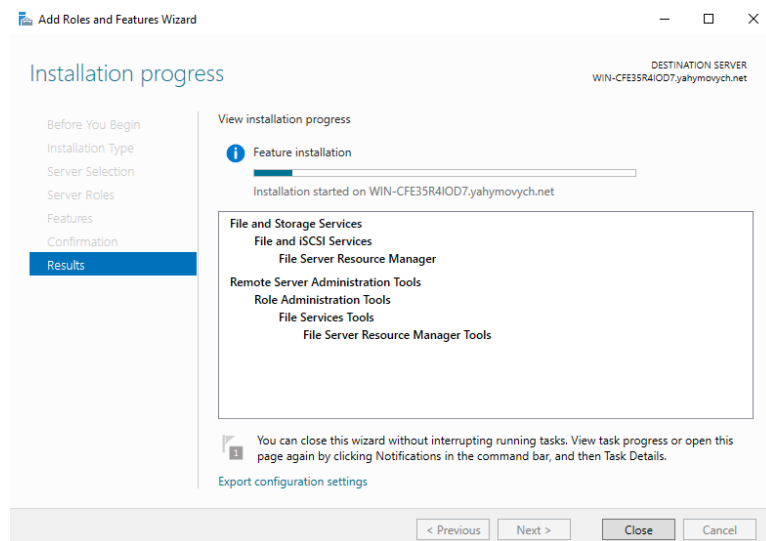


Рисунок 3.52 – Встановлення файлових служб

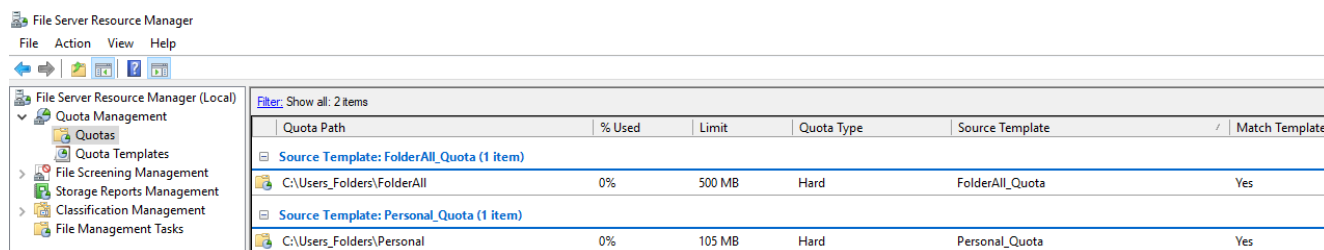


Рисунок 3.53 – Вікно менеджера ресурсів

Через менеджер ресурсів створюю новий шаблон квот для спільних та персональних папок (рис. 3.54)

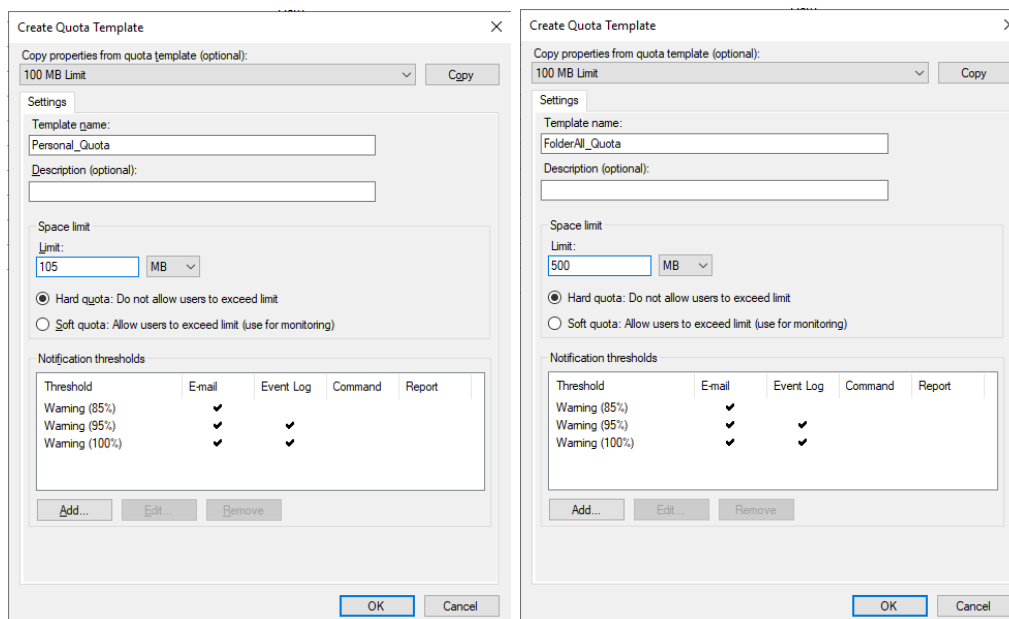


Рисунок 3.54 – Створення шаблону квоти

Через менеджер ресурсів створюю квоти та застосовую попередньо створені шаблони (рис. 3.55)

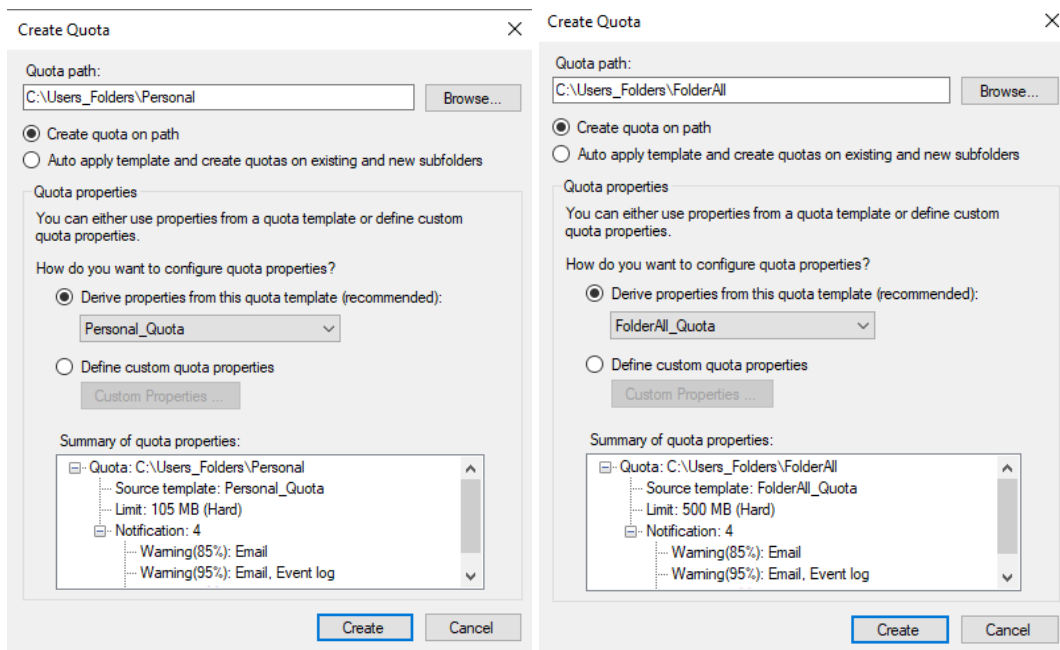


Рисунок 3.55 – Створення самих квот

Налаштування повного резервного копіювання системи за допомогою Windows Server Backup

Встановлення необхідної функції для резервного копіювання (рис. 3.56)

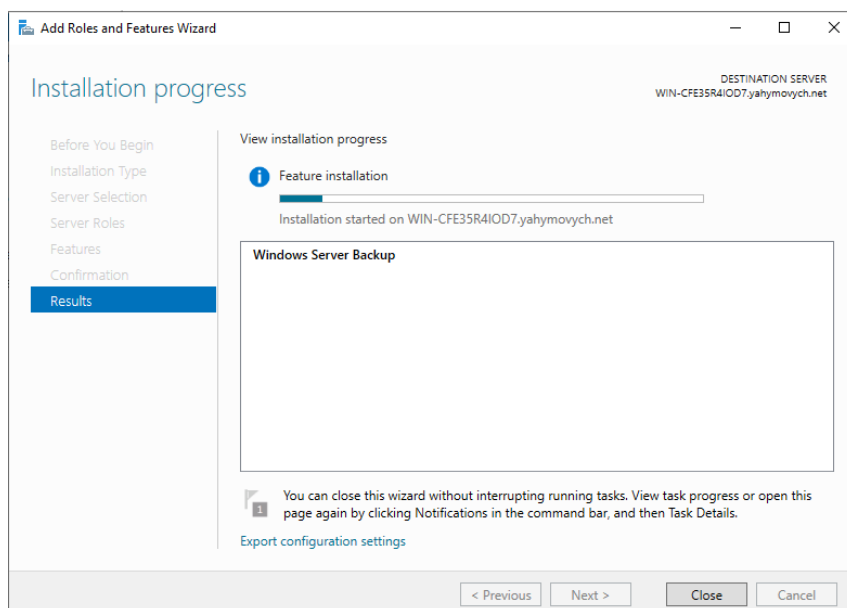


Рисунок 3.56 – Встановлення функції резервного копіювання

Запускаю оснащення для резервного копіювання через меню Пуск (рис. 3.57)

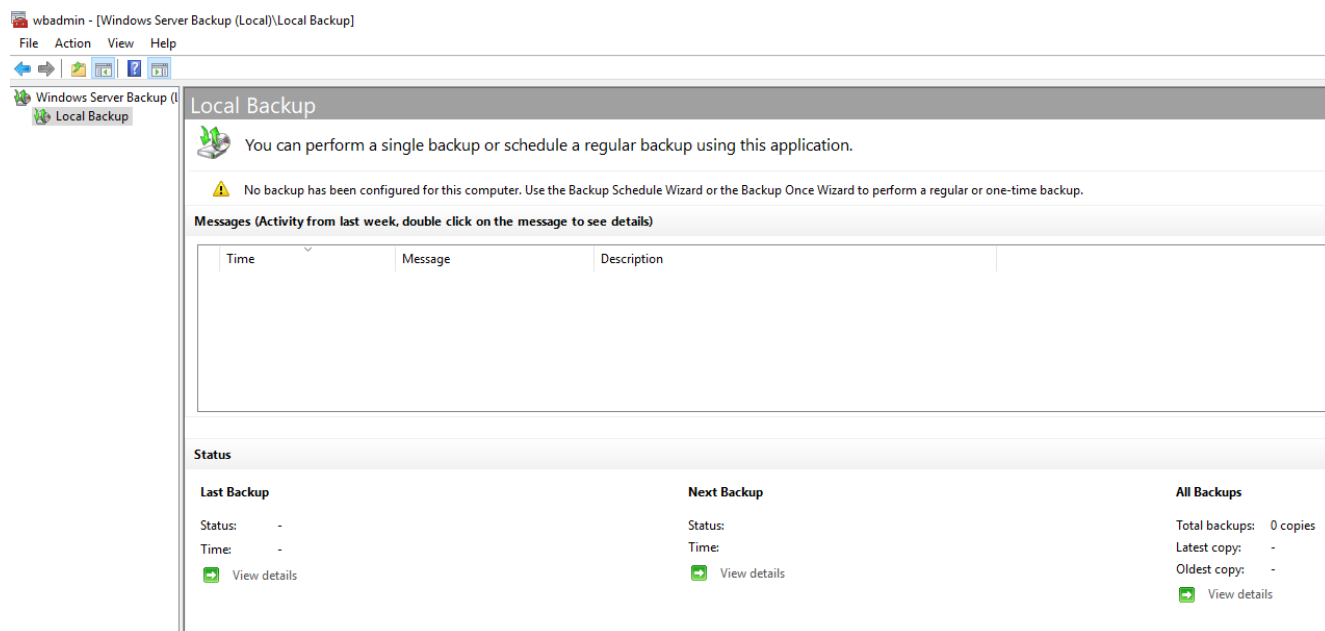


Рисунок 3.57 – Windows Server Backup

Вибираю тип резервного копіювання (рис. 3.58)

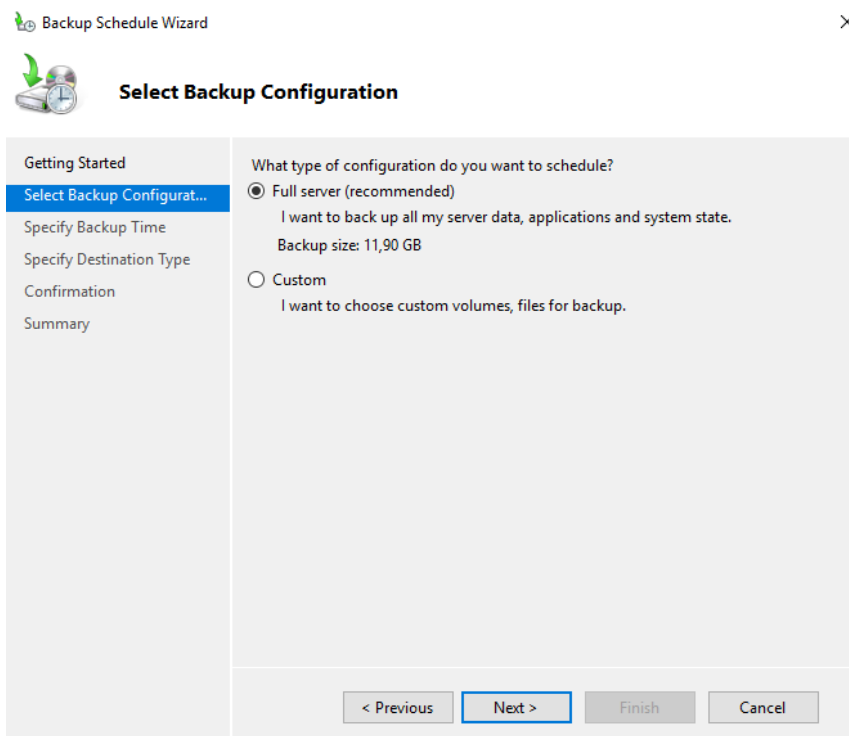


Рисунок 3.58 – Вибір типу резервного копіювання

Задаю час, в якій буде відбуватися резервне копіювання (рис. 3.59)

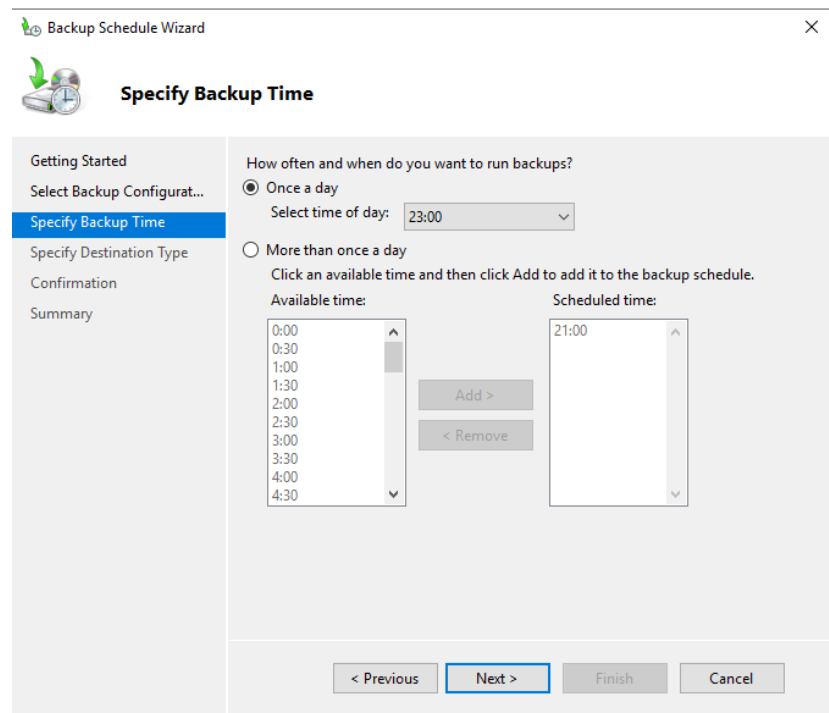


Рисунок 3.59 – Вибір часу для резервного копіювання

Створення організаційних одиниць (Organization unit) домену

Створюю OU для користувачів домену (рис. 3.60)

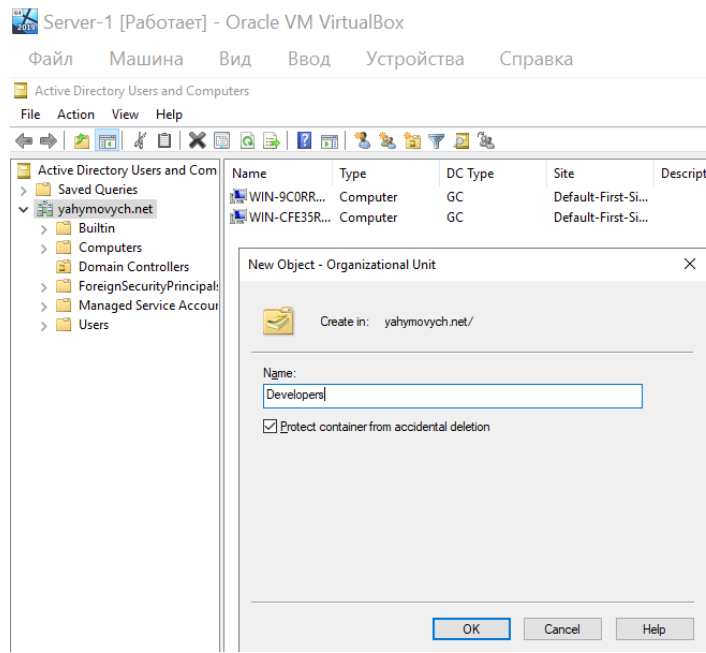


Рисунок 3.60 – Створення першої OU

|      |      |               |        |      |
|------|------|---------------|--------|------|
|      |      | Яхимович В.С. |        |      |
|      |      | Головня О.С.  |        |      |
| Змн. | Арк. | № докум.      | Підпис | Дата |

КІК.КР.Б – 123 – 20 – ПЗ

Арк.

71

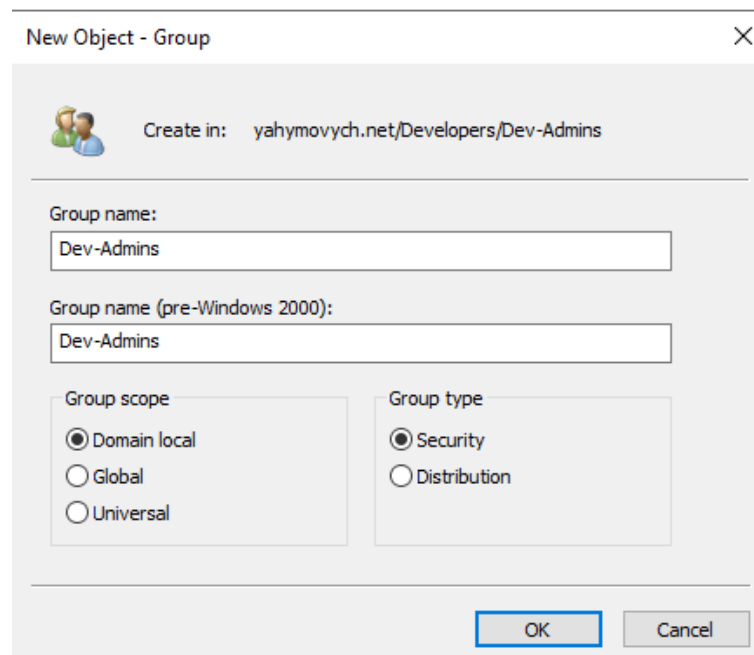


Рисунок 3.61 – Створення групи

Надаю кожній OU адміністраторів контроль над відповідними OU користувачів (рис. 3.62)

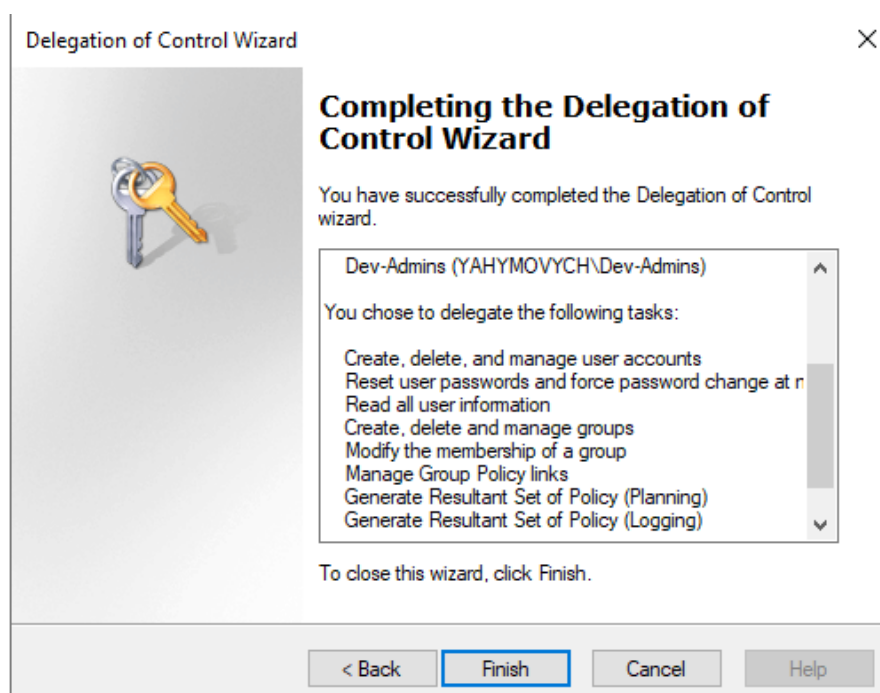


Рисунок 3.62 – Майстер делегування контролю

Адміністраторам кожної OU було делеговано котроль для відповідних OU користувачів. На рис. 3.62 показані всі дії, які можуть застосовувати адміністратори до контрольованих OU, а саме:

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 72   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

- Створення, видалення та управління обліковими записами
- Відновлення або зміна паролів користувачів
- Передивлятися всю інформацію про користувачів
- Створювати, видаляти та управляти групами
- Редагувати учасників груп
- Керувати посиланнями групових політик
- Створити результуючий набір політик

Також були показані налаштування сервісів, зокрема:

- Як приєднатися у домен з нової робочої станції
- Налаштування апаратного забезпечення мережі
- Встановлення ОС на сервери та робочі станції
- Створення домену мережі та додавання основного та додаткового

серверів в ролі контролера домену

- Налаштування DNS
- Налаштування DHCP
- Налаштування відмовостійкості серверів
- Налаштування служб віддаленого доступу
- Налаштування інформаційних служб інтернету (IIS)
- Створення організаційних одиниць
- Створення папок для користувачів та квот
- Налаштування спільних принтерів
- Внутрішньосайтова реплікація
- Налаштування повного резервного копіювання

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 73   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

3.3 Тестування працездатності вузлів та сервісів побудованої локальної комп’ютерної мережі

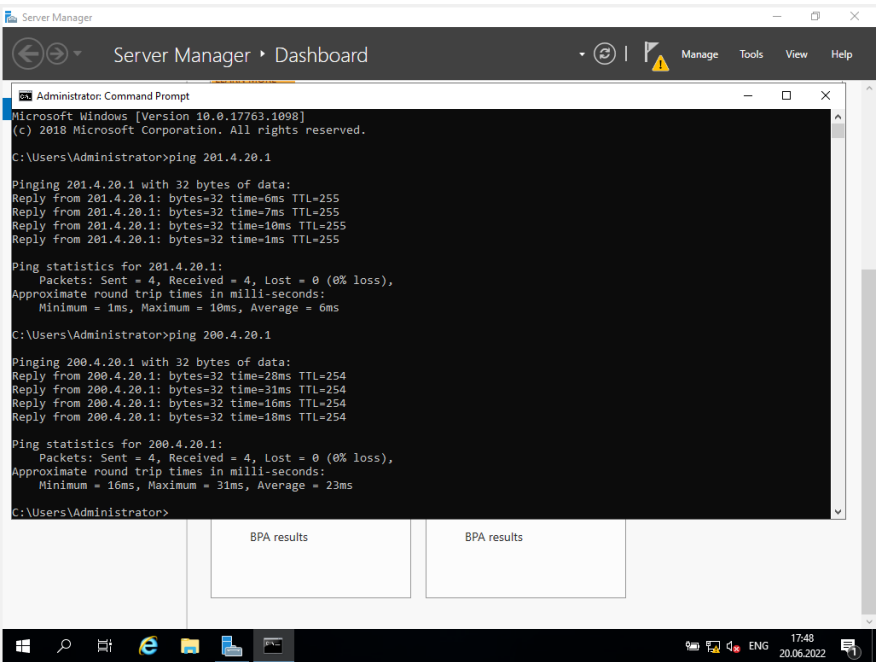


Рисунок 3.63 – Перевірка зв’язку між вузлами мережі

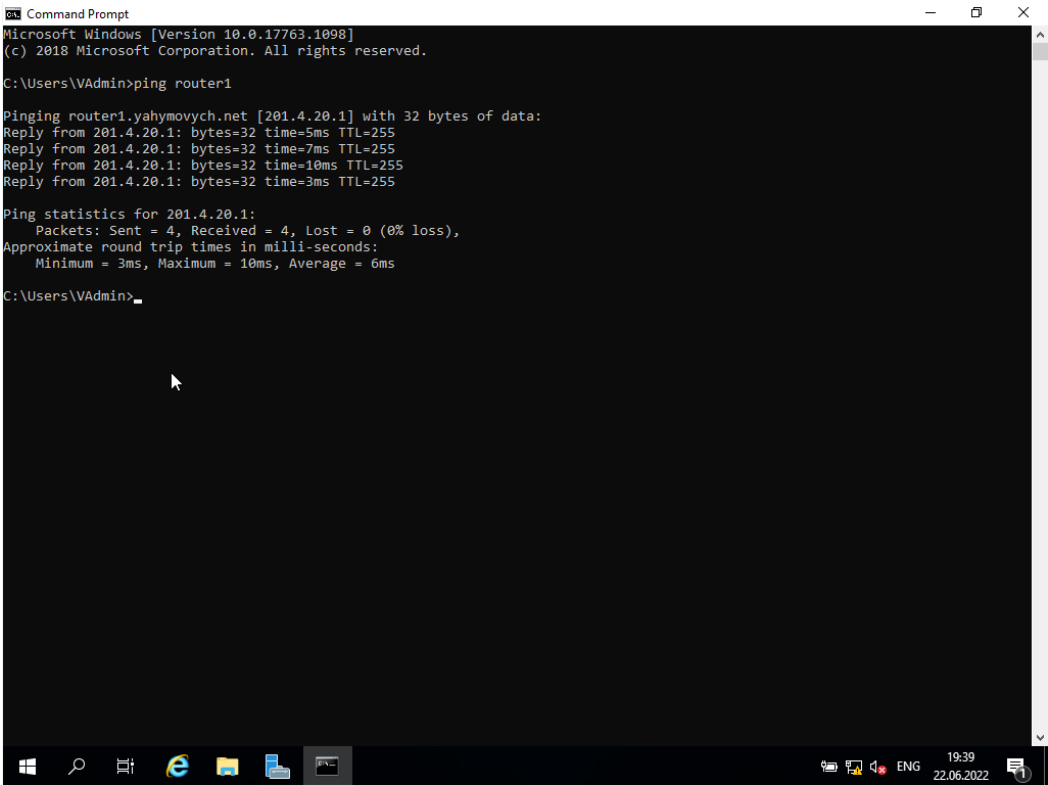


Рисунок 3.64 – Пінгування через доменне ім’я

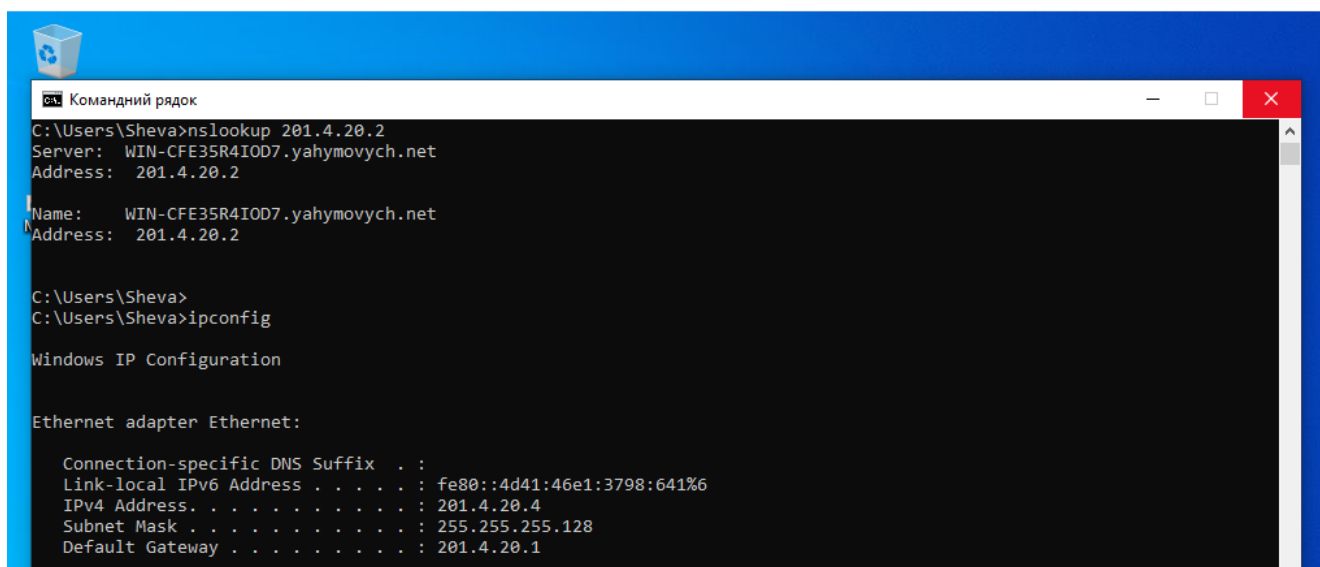


Рисунок 3.65 – Перевірка працездатності зворотніх зон

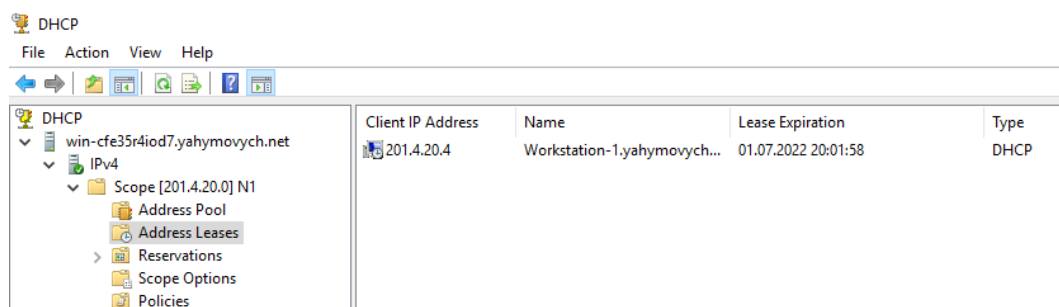
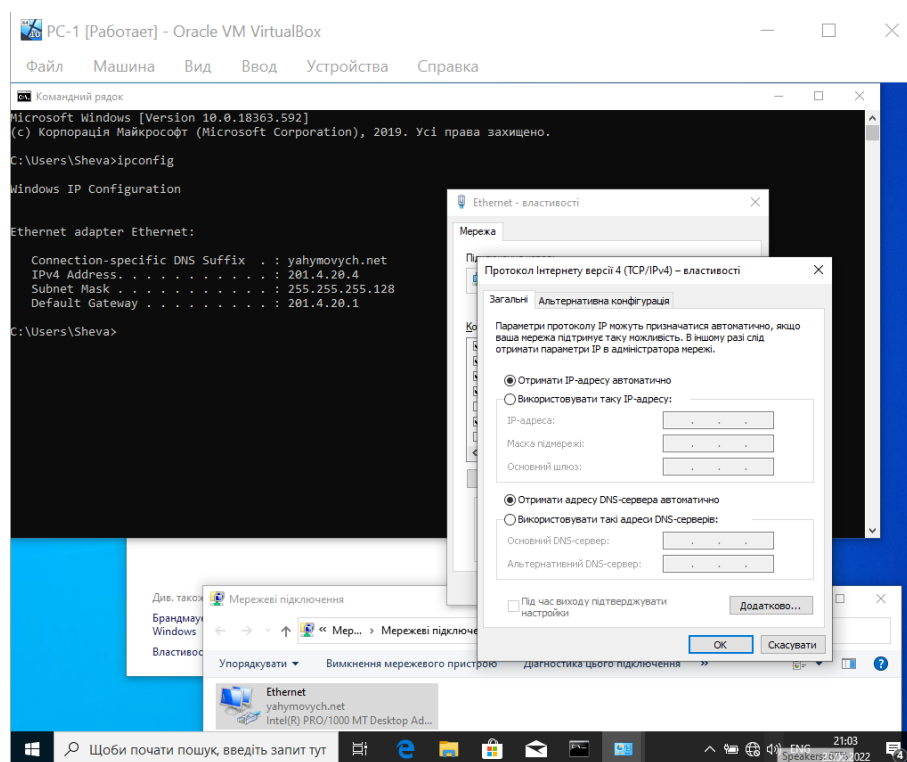


Рисунок 3.66 – робота DHCP-сервера

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арх. |
|      |      | Головня О.С.  |        |      |                          | 75   |
| Змн. | Арх. | № докум.      | Підпис | Дата |                          |      |

```

PC-2 [Роботаєт] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Командний рядок
C:\Users\Student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : yahymovych.net
    IPv4 Address. . . . . : 202.4.20.2
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 202.4.20.1

C:\Users\Student>ping 201.4.20.2

Pinging 201.4.20.2 with 32 bytes of data:
Reply from 201.4.20.2: bytes=32 time=21ms TTL=127
Reply from 201.4.20.2: bytes=32 time=22ms TTL=127
Reply from 201.4.20.2: bytes=32 time=19ms TTL=127
Reply from 201.4.20.2: bytes=32 time=16ms TTL=127

Ping statistics for 201.4.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 22ms, Average = 19ms

C:\Users\Student>ping 201.4.20.1

Pinging 201.4.20.1 with 32 bytes of data:
Reply from 201.4.20.1: bytes=32 time=9ms TTL=255
Reply from 201.4.20.1: bytes=32 time=3ms TTL=255
Reply from 201.4.20.1: bytes=32 time=10ms TTL=255
Reply from 201.4.20.1: bytes=32 time=10ms TTL=255

Ping statistics for 201.4.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 10ms, Average = 8ms

C:\Users\Student>ping 200.4.20.1

Pinging 200.4.20.1 with 32 bytes of data:
Reply from 200.4.20.1: bytes=32 time=22ms TTL=254
Reply from 200.4.20.1: bytes=32 time=27ms TTL=254
Reply from 200.4.20.1: bytes=32 time=32ms TTL=254
  
```

Рисунок 3.67 – Перевірка зв’язку та DHCP у гостьовій мережі

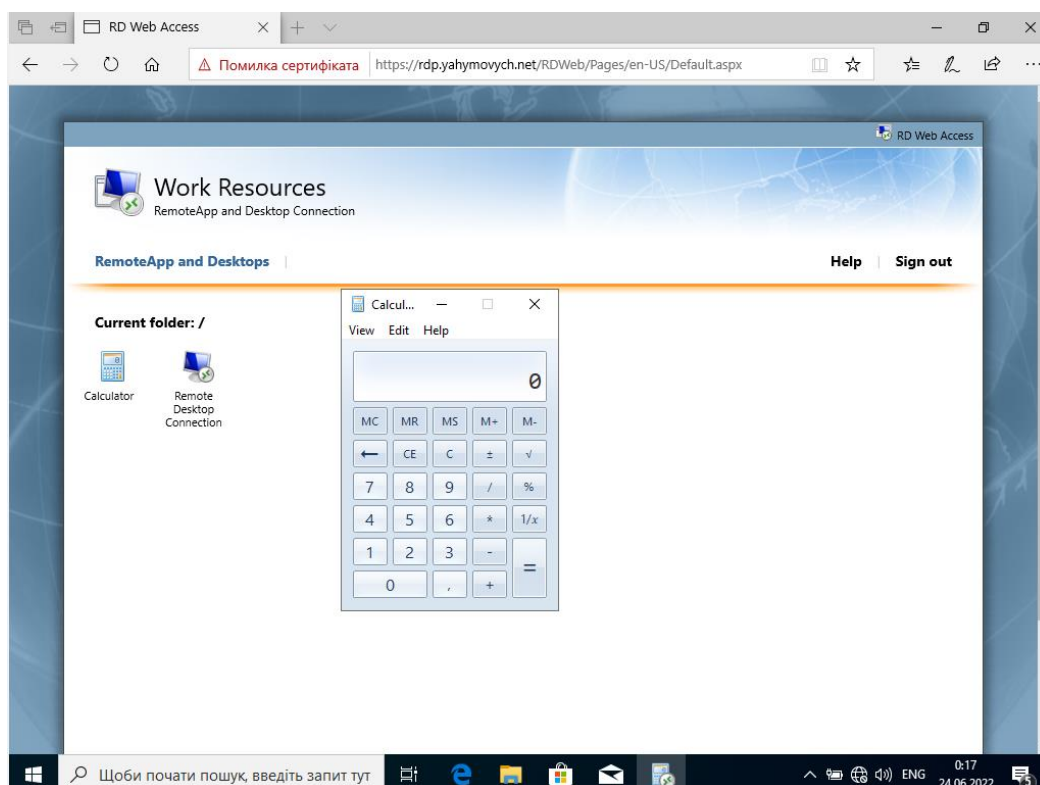


Рисунок 3.68 – Перевірка роботи віддаленого доступу

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 76   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

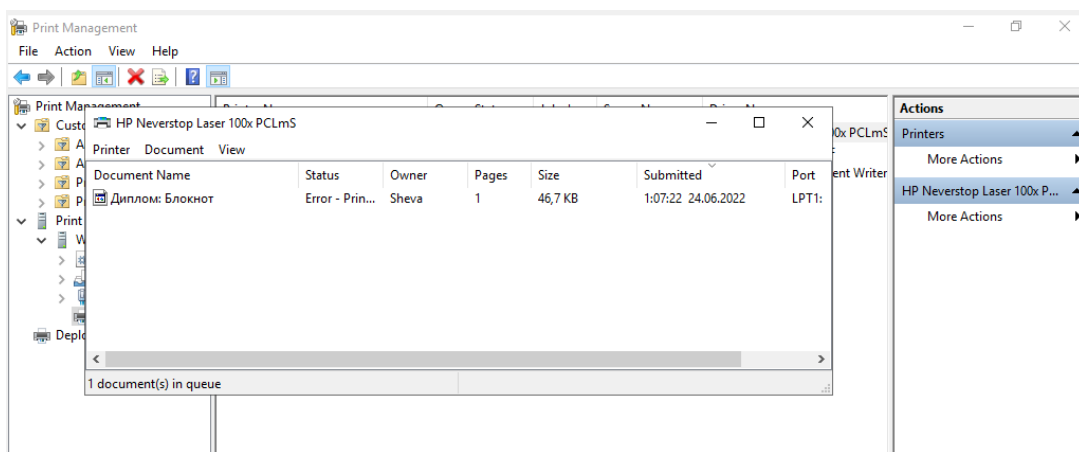


Рисунок 3.69 – Перевірка спільного принтера

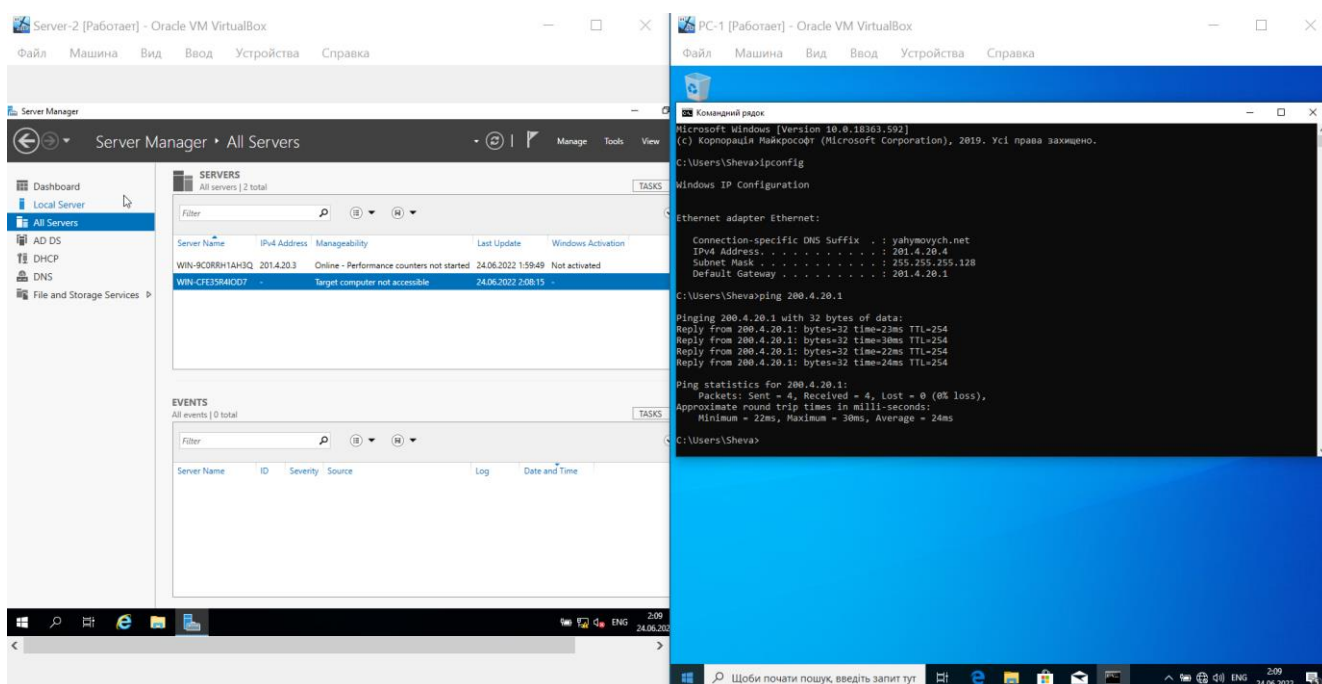


Рисунок 3.70 – Перевірка роботи відмовостійкості

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 77   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

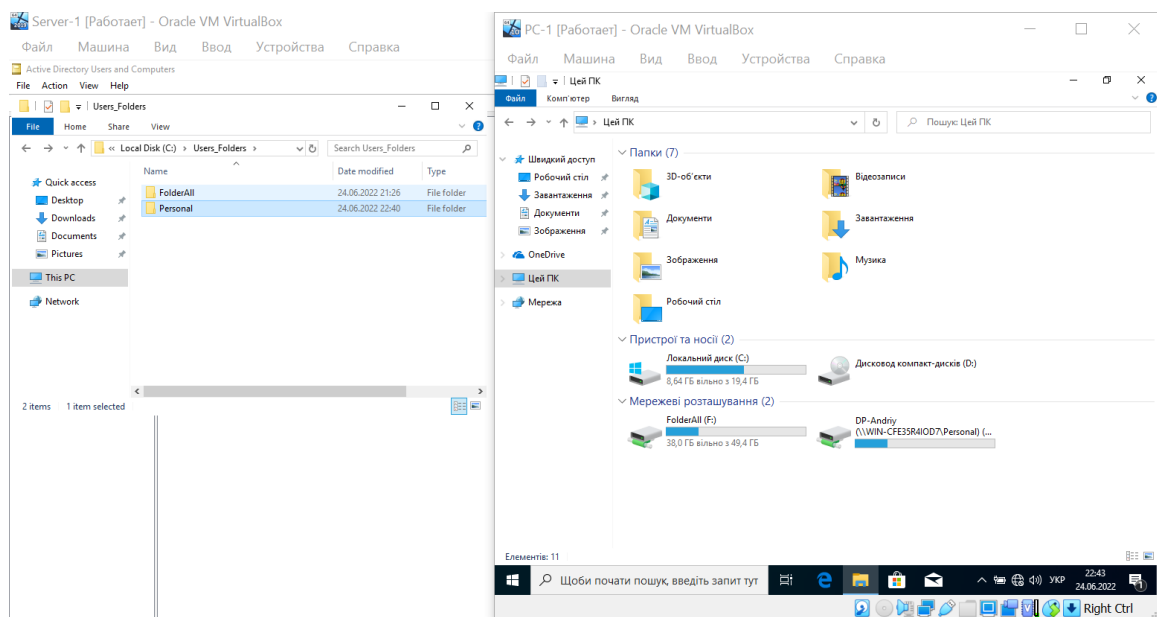


Рисунок 3.71 – Перевірка роботи спільних та особистих папок

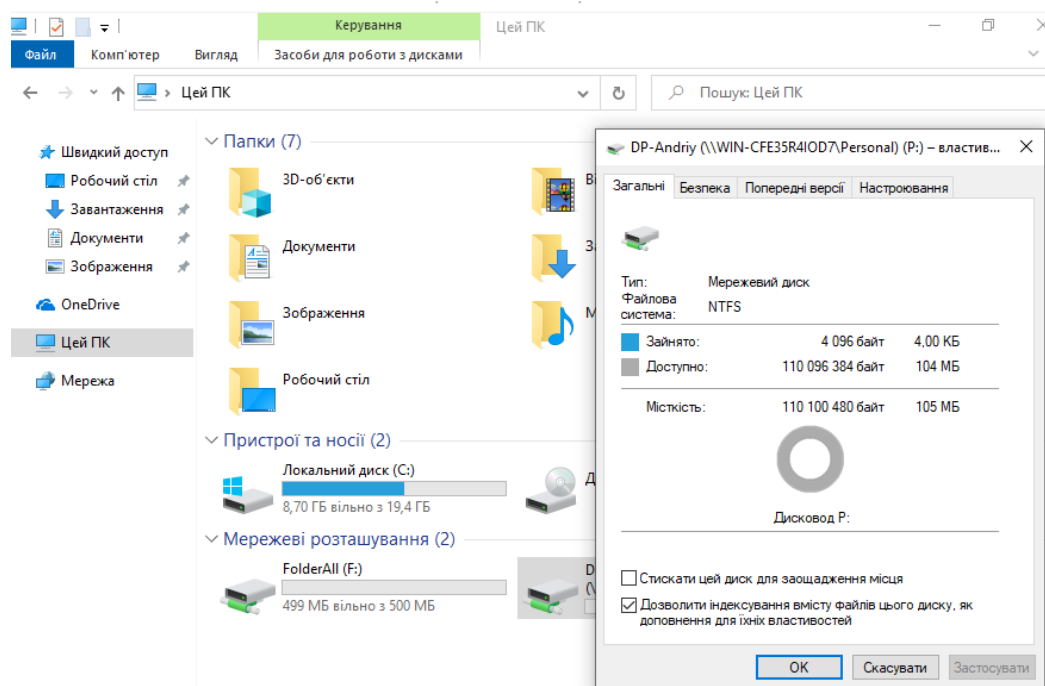


Рисунок 3.72 – Перевірка роботи квот

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 78   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Дипломна робота

—2022—

Логін:

Пароль:

Повторіть пароль:

Стать: Чоловік ☐ Жінка ☒

Вкажіть країну:

Про себе:

Яхимович В.С.

Рисунок 3.73 – Перевірка сайту

## Висновки розділу

В третьому розділі було показано налаштування компонентів локальної комп'ютерної мережі та багатьох сервісів служб каталогів Active Directory з детальними скріншотами, а саме:

- Налагодження апаратного забезпечення мережі
- Встановлення ОС на сервери та робочі станції
- Створення домену мережі та додавання основного та додаткового серверів в ролі контролера домену
- Налаштування DNS
- Налаштування DHCP
- Налаштування відмовостійкості серверів
- Налаштування служб віддаленого доступу
- Налаштування інформаційних служб інтернету (IIS)
- Створення організаційних одиниць
- Створення папок для користувачів та квот
- Налаштування спільних принтерів

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 79   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

- Внутрішньосайтова реплікація
- Налаштування повного резервного копіювання
- Тестування працездатності налаштованої мережі та сервісів

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 80   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## ВИСНОВКИ

Під час виконання дипломного проекту в першому розділі було розглянуто загальні характеристики служби каталогів Active Directory та їх сервісів, визначення основних понять та сервісів пов'язаних з цією службою, важливість даної служби та загрози. Теоретичні аспекти про локальні комп'ютерні мережі, типи локальних мереж, їх відмінності, переваги та недоліки, методи захисту та завдання, які допомагають вирішити локальні комп'ютерні мережі.

В другому розділі було створено та показано схему мережі, розписано важливість вибору топології зпроектованої мережі, сформовано таблиці IP-адресації для протоколів IPv4 та IPv6, показано структуру домену в Active Directory. Також було обране реальне програмне та апаратне забезпечення на основі потреб зпроектованої мережі, наведені основні характеристики та обґрунтовано вибір тих чи інших компонентів.

В третьому розділі було показано налаштування компонентів локальної комп'ютерної мережі та багатьох сервісів служб каталогів Active Directory з детальними скріншотами, а саме:

- Налагодження апаратного забезпечення мережі
- Встановлення ОС на сервери та робочі станції
- Створення домену мережі та додавання основного та додаткового серверів в ролі контролера домену
- Налаштування DNS
- Налаштування DHCP
- Налаштування відмовостійкості серверів
- Налаштування служб віддаленого доступу
- Створення організаційних одиниць
- Створення папок для користувачів та квот
- Налаштування спільних принтерів

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 81   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

- Внутрішньосайтова реплікація
- Налаштування повного резервного копіювання
- Тестування працездатності налаштованої мережі та сервісів

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 82   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. M. Henderson, J. Krause. Windows Server 2019 Cookbookm - Second Edition: Over 100 recipes to effectively configure networks, manage security, and administer workloads.
2. S. Clines, M. Loughry. Active Directory For Dummies.
3. K. Kocis. Microsoft Active Server Directory Administration (Sams White Book Series)
4. DHCP in Active Directory. Informit. [URL:https://www.informit.com/articles/article.aspx?p=130843&seqNum=8](https://www.informit.com/articles/article.aspx?p=130843&seqNum=8)
5. D. Stelmach. WSTĘP TEORETYCZNY DO ACTIVE DIRECTORY. Pasja informatyki. URL: <https://pasja-informatyki.pl/sieci-komputerowe/active-directory-wstep/>
6. Wireless Local Area Network (WLAN). Techopedia. URL:<https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan>
7. Active Directory. Adminbook. URL:[http://adminbook.ru/index.php?men3=3\\_1](http://adminbook.ru/index.php?men3=3_1)
8. Alexander S. Gillis. Network topology. Techtarget. URL:<https://www.techtarget.com/searchnetworking/definition/network-topology>
9. Що таке локальна мережа? Briz. URL: <https://www.briz.ua/blog/article/cto-takoe-lokalnaya-set>
10. What Is RDS And What Are The Benefits Of RDS. Acecloudhosting. URL: <https://www.acecloudhosting.com/blog/benefits-of-rds/>
11. Local Area Network. Heavy.ai. URL: <https://www.heavy.ai/technical-glossary/local-area-network>
12. Kindson The Genius. How to Setup Active Directory Domain With VirtualBox and Join Computers. URL: <https://www.kindsonthegenius.com/how-to-setup-active-directory-domain-with-virtualbox-and-join-computers-part-1/>
13. S. Wallei. Windows Server 2019 Vs 2016: What are the Differences? Parallels. URL:<https://www.parallels.com/blogs/ras/windows-server-2019-vs-2016/>

|      |      |               |        |      |                                 |      |
|------|------|---------------|--------|------|---------------------------------|------|
|      |      | Яхимович В.С. |        |      | <i>KIK.KP.B – 123 – 20 – ПЗ</i> | Арк. |
|      |      | Головня О.С.  |        |      |                                 | 83   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                                 |      |

14. DNS and Active Directory. Windows Active Directory.  
URL: <https://www.windows-active-directory.com/dns-and-active-directory.html>

15. IIS Server. Solarwinds. URL: <https://www.solarwinds.com/resources/it-glossary/iis-server>

16. Преимущества Windows 10 для корпоративных клиентов. DC Link Group. URL: <https://dclink.ua/ru/news/news/perevagi-windows-10-dlya-korporativnikh-klientiv/>

17. Настройка консолей управления Microsoft (MMC). Alterego. URL: [https://alterego.ucoz.org/publ/active\\_directory/nastrojka\\_mmc/4-1-0-63](https://alterego.ucoz.org/publ/active_directory/nastrojka_mmc/4-1-0-63)

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 84   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

# ДОДАТКИ

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 85   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Приєднання робочої станції у домен

Переходимо у властивості системи (рис. 3.61)

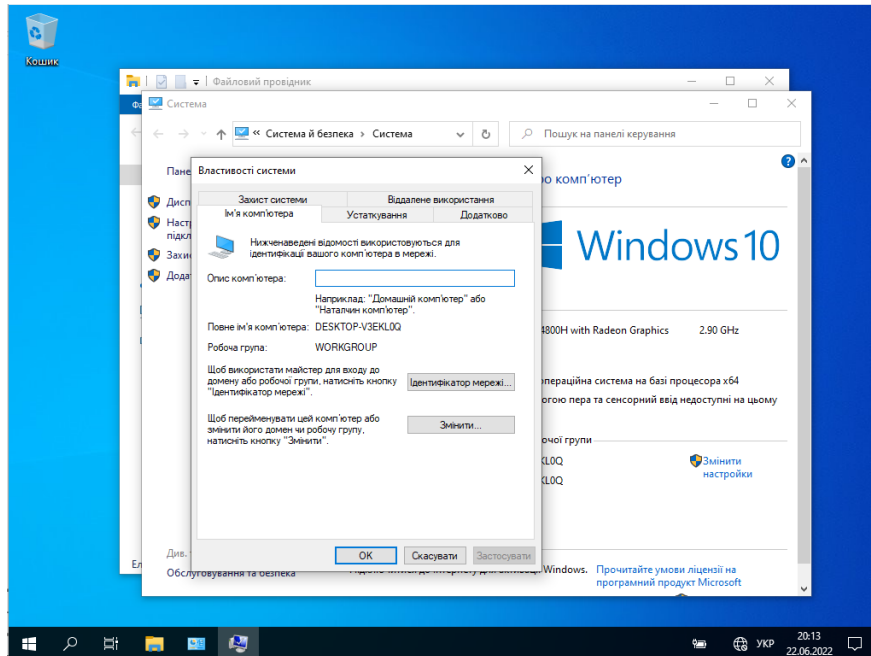


Рисунок 3.74 – Властивості системи

Натискаємо кнопку “Змінити”.

Вказуємо ім’я домену та по бажанню можемо змінити ім’я комп’ютера, яке буде відображатися на сервері AD.

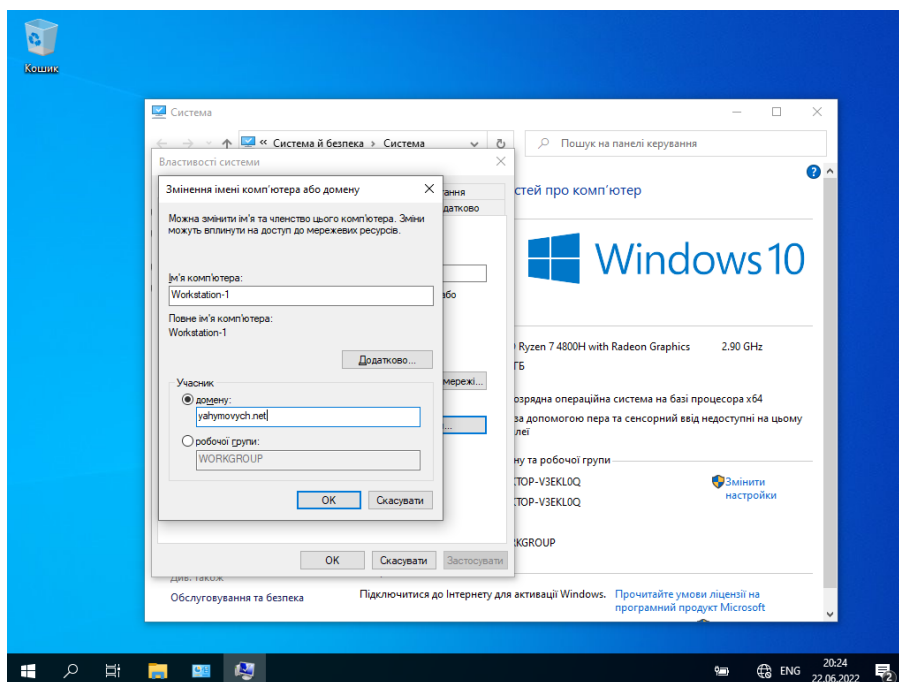


Рисунок 3.75 – Зміна імені та домену

Далі система запросить дані облікового запису, який був раніше створений на контролері домену. Вводимо і натискаємо ОК.

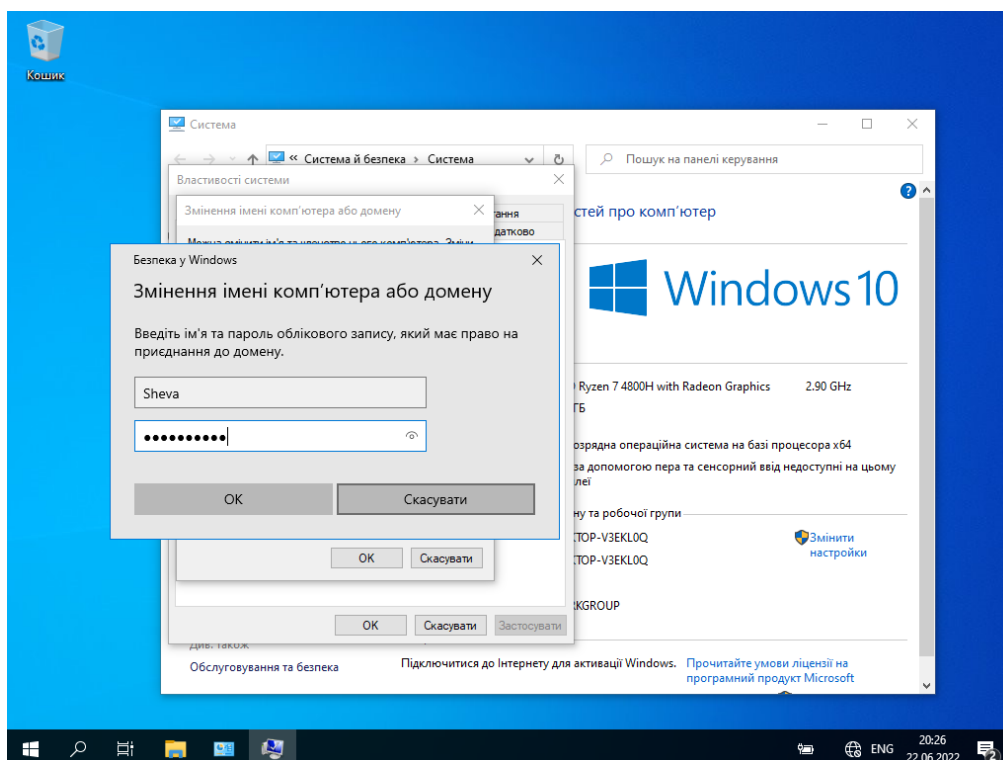


Рисунок 3.76 – Обліковий запис

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | KIK.KP.B – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 87   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

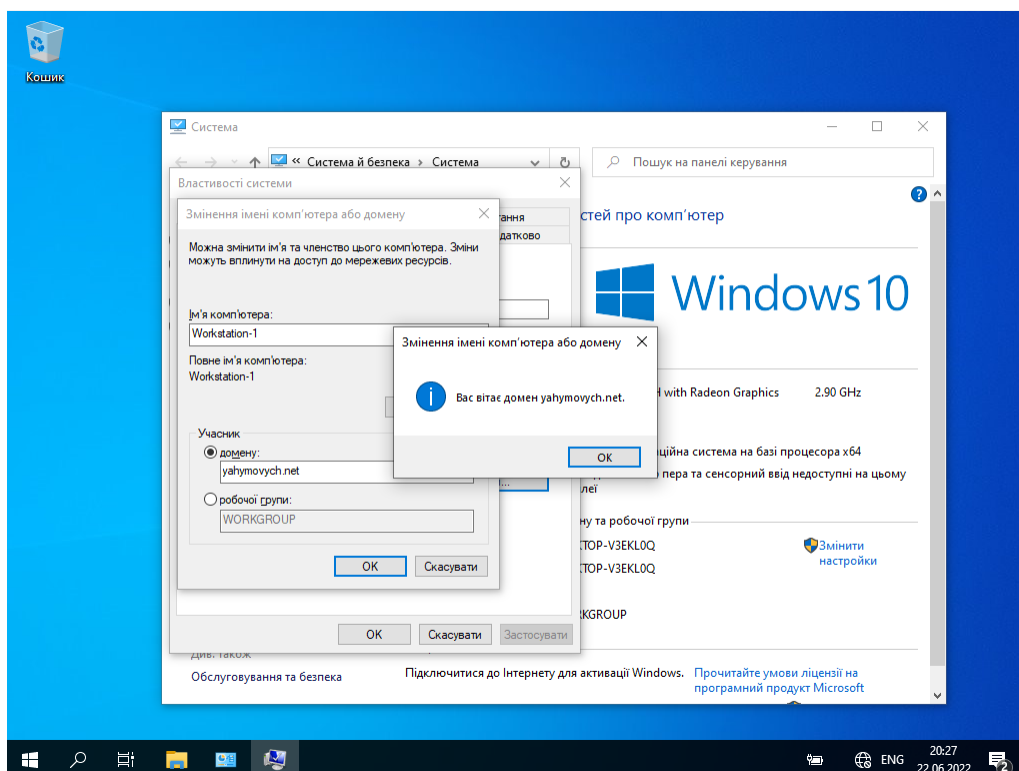


Рисунок 3.77 – Успішний вхід.

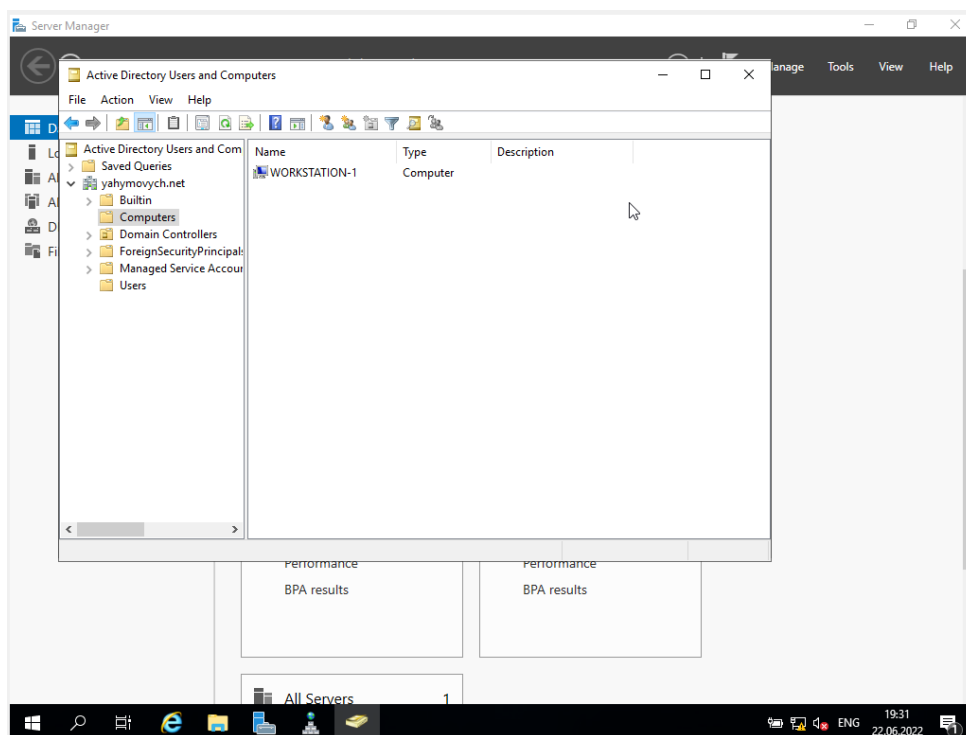


Рисунок 3.78 – Комп'ютер на сервері

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 88   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

## Додавання нових користувачів та надання прав

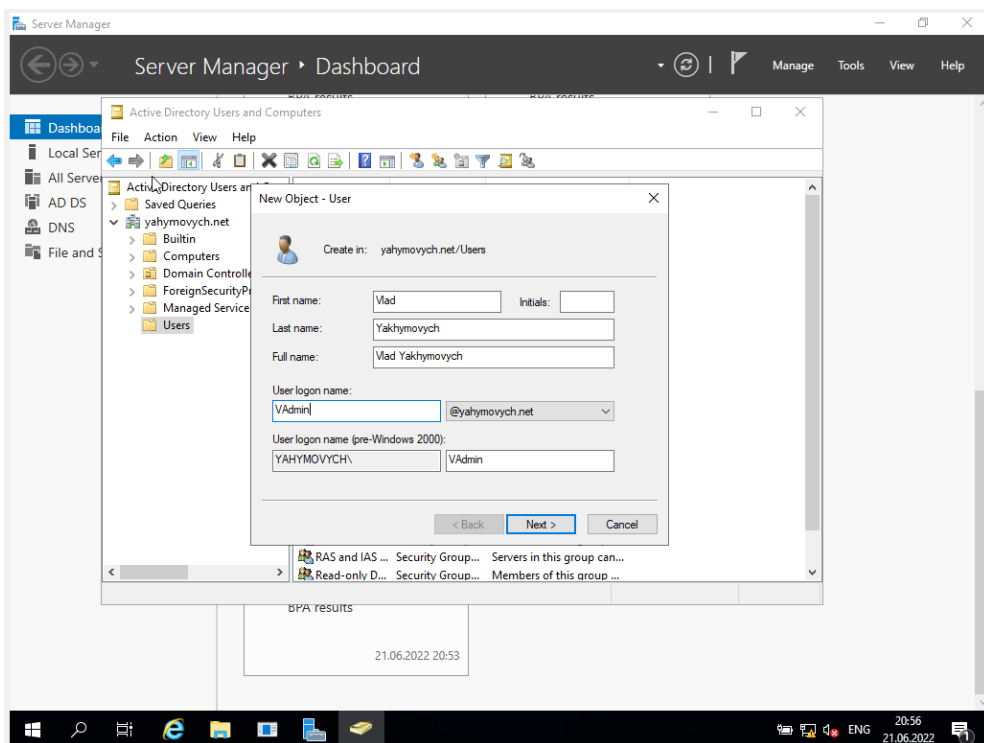


Рисунок 3.79 – Створення нового користувача

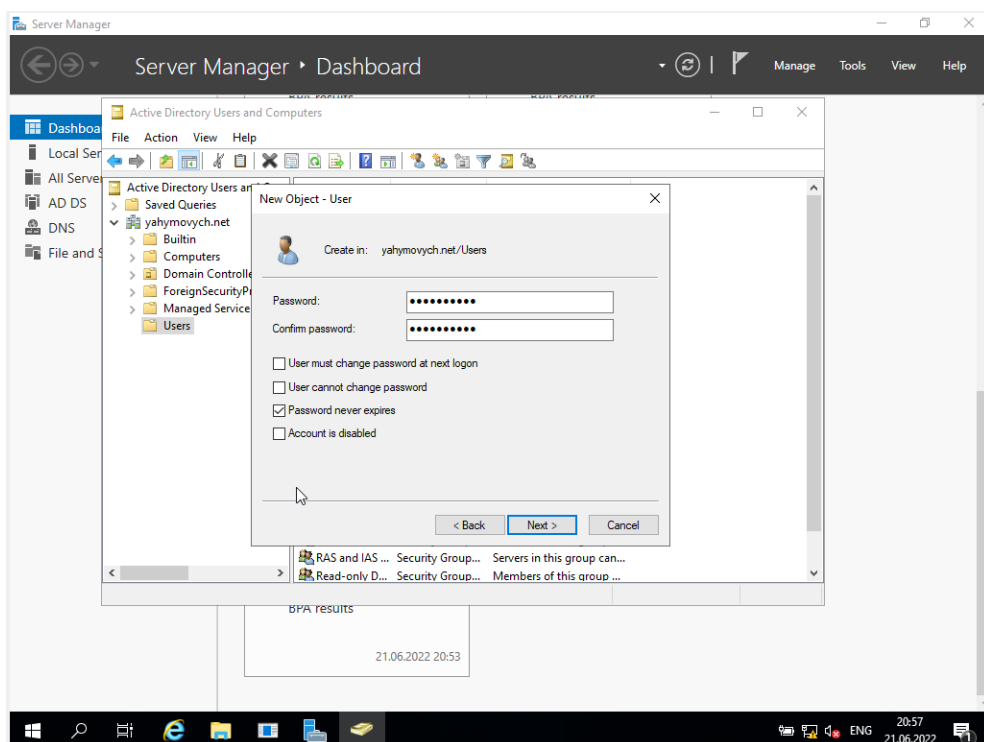


Рисунок 3.80 – Задання паролю для облікового запису

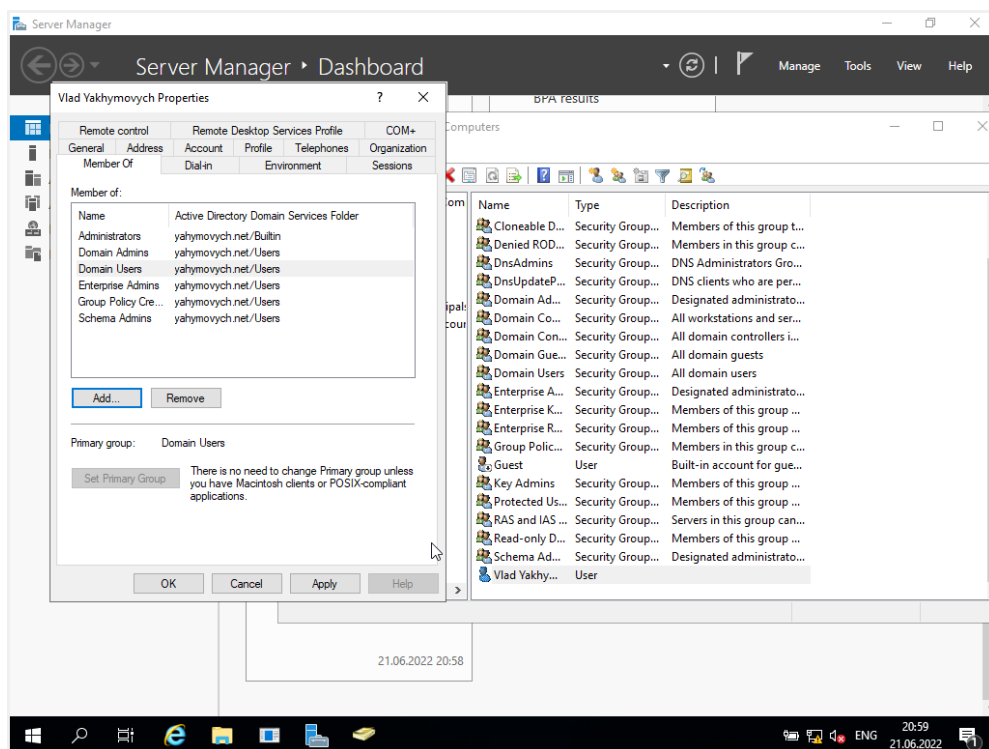


Рисунок 3.81 – Надання повних адміністративних прав

## Внутрішньосайтова реплікація

Цей вид реплікації здійснюється автоматично, при наявності двох і більше контролерів домену в мережі. Можна налаштувати час і дні, в які буде виконуватися реплікація, також можна здійснити примусову реплікацію.

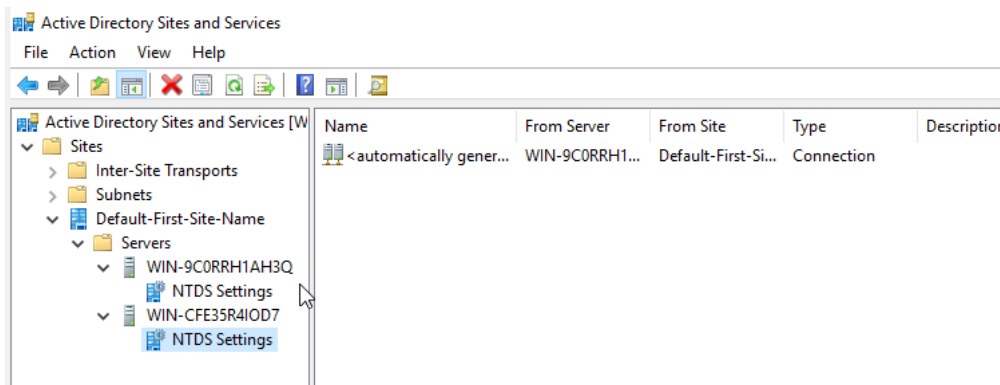


Рисунок 3.82 – AD Sites and Services

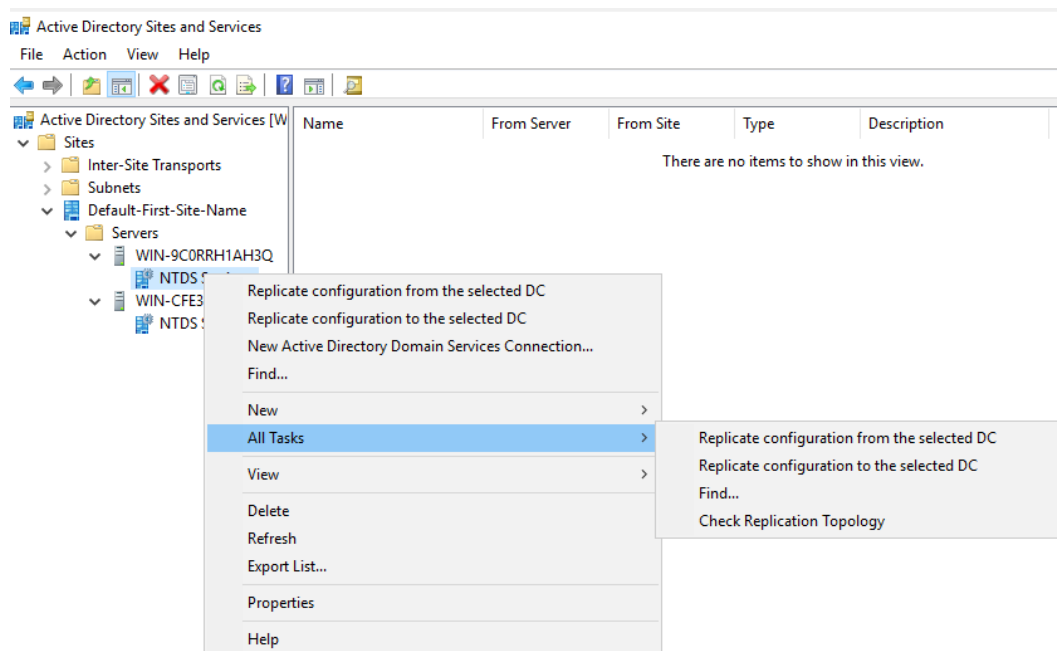


Рисунок 3.83 – Регенерація топології реплікації

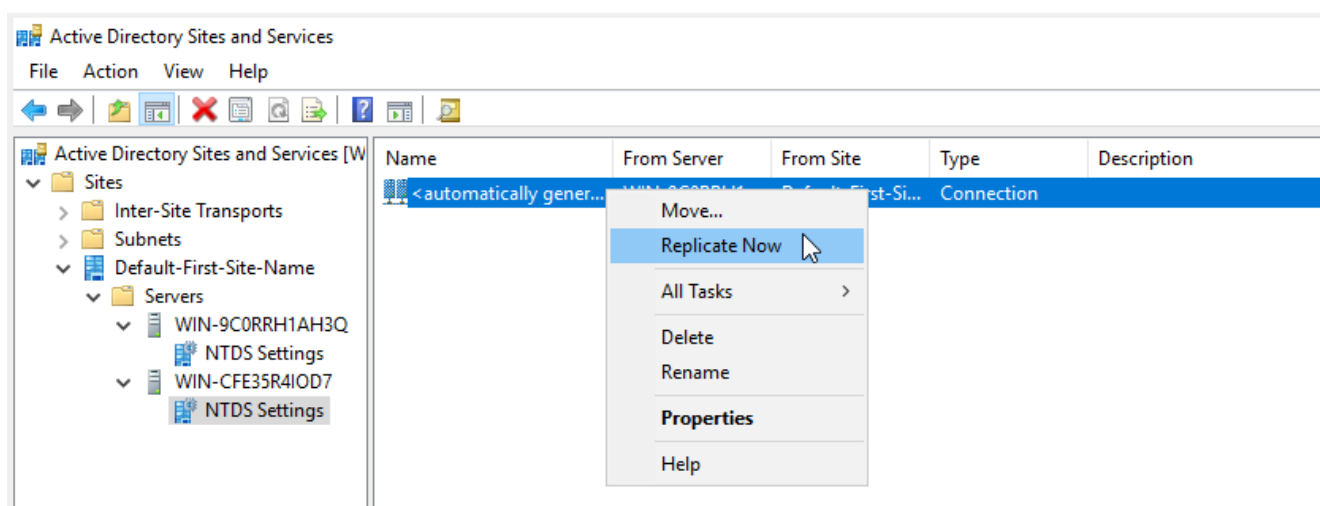


Рисунок 3.84 – Примусова реплікація

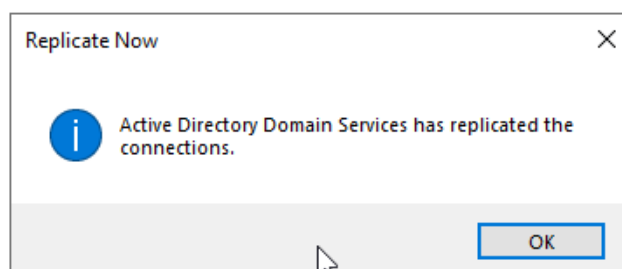


Рисунок 3.85 – Успішне виконання

## Налаштування спільних принтерів

Для початку потрібно завантажити драйвера для нашого принтера з офіційного сайту виробника, потім відкриваємо скачаний архів с функцією саморозпаковування та знаходимо папку з драйвером за допомогою Win+R і вводимо %temp%. В панелі керування запускаємо функцію додавання нового принтера, та вставляємо шлях до папки з драйвером та вибираємо драйвер зі списку (рис 3.86)

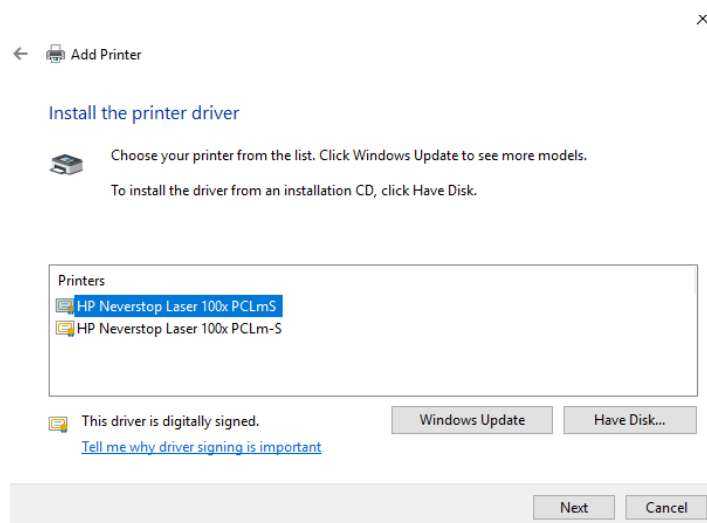


Рисунок 3.86 – Вибір драйвера

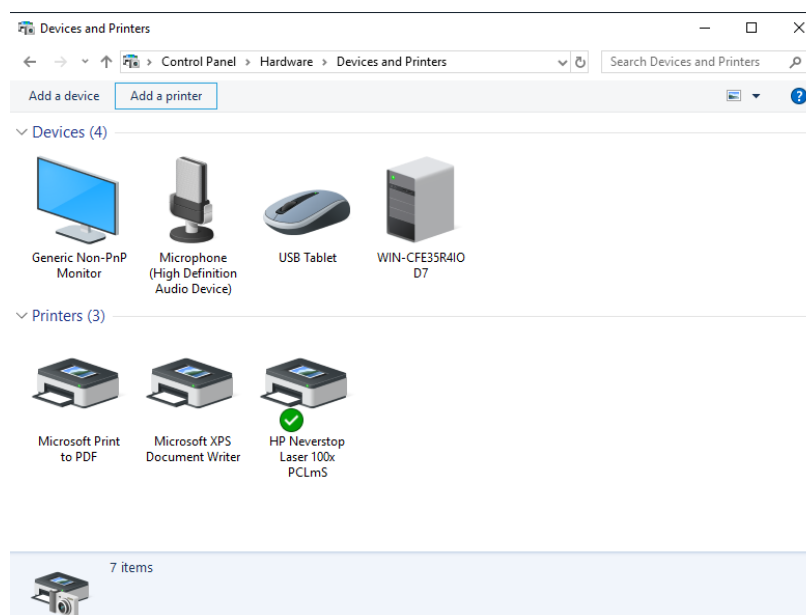


Рисунок 3.87 – Список пристроїв

|      |      |               |        |      |                          |      |
|------|------|---------------|--------|------|--------------------------|------|
|      |      | Яхимович В.С. |        |      | КІК.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Головня О.С.  |        |      |                          | 92   |
| Змн. | Арк. | № докум.      | Підпис | Дата |                          |      |

Встановлюю роль для принтерів на контролері (рис.3.88)

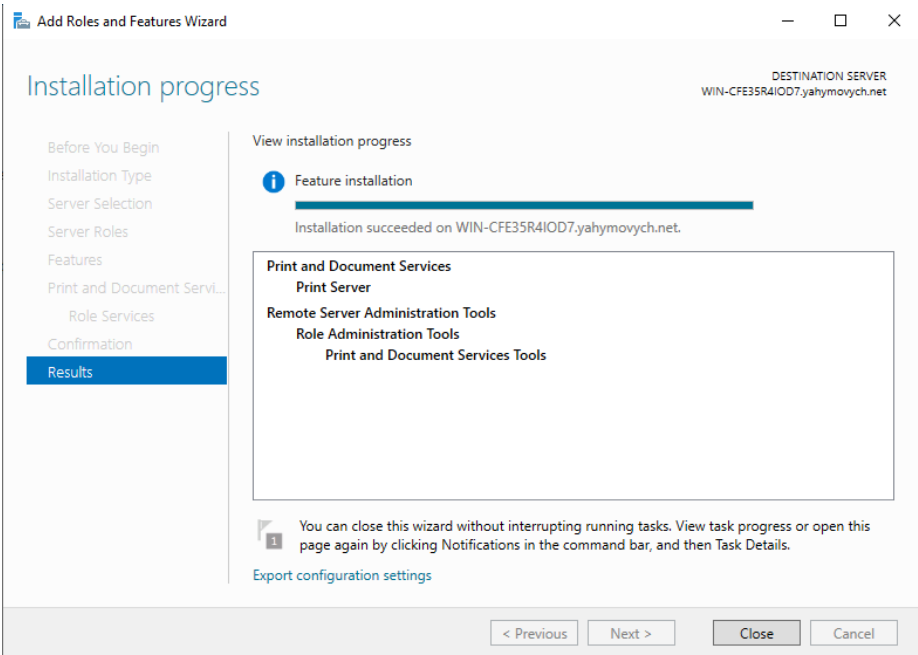


Рисунок 3.88 – Встановлення ролі

Розгортаю принтер для спільного використання користувачами (рис 3.89)

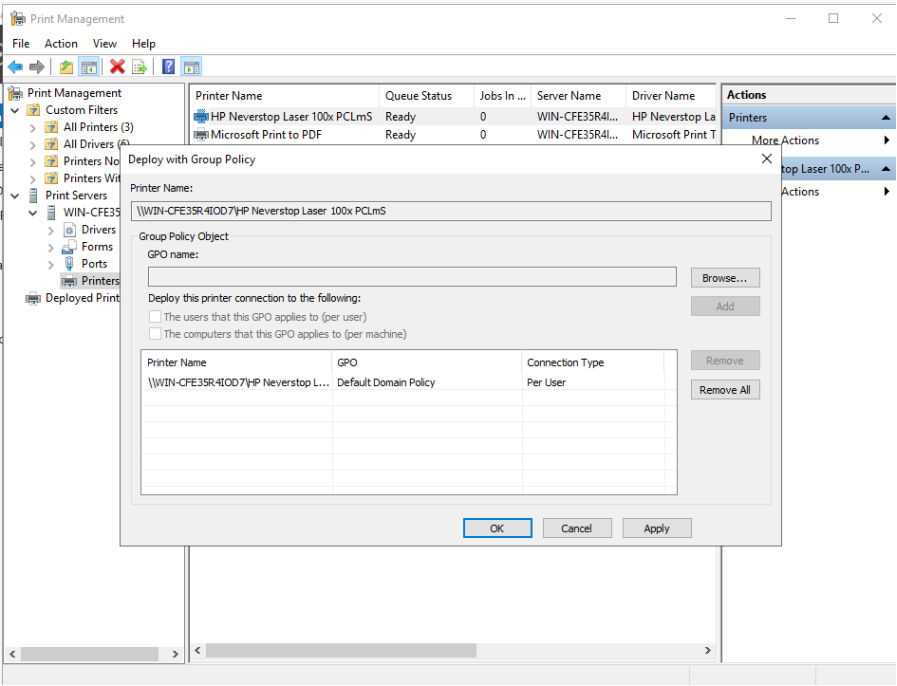


Рисунок 3.89 – Розгортання

## Список розгорнутих принтерів на сервері (рис. 3.90)

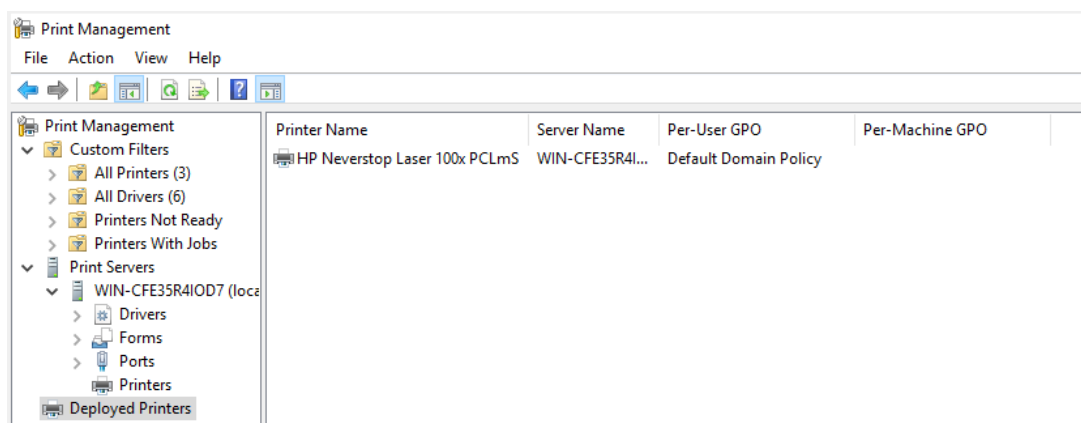


Рисунок 3.90 – Принтер готовий до використання

Засіб Print Management дає змогу переглядати відомості про сервери друку, які працюють у домені, порти, драйвери, форми друку та принтери, а також налаштовувати їх.