ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента Іванова Дмитра Анатолійовича
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему „Проект мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows ".

2. Актуальність роботи зумовлена потребою у розробці та впровадженні у практику роботи закладів вищої освіти інфраструктурних рішень на базі Microsoft Windows .

3. Основний зміст пояснювальної записки роботи викладено на 64 сторінках тексту, записка містить 1 таблицю, 56 ілюстрацій, 10 додатків. Список використаних літературних джерел налічує 30 найменувань. Невід'ємною складовою роботи є реалізований у середовищі моделювання GNS3 проект мережі університету на базі рішень Microsoft Windows.

4. Пояснювальна записка складається з вступу, трьох розділів основного тексту, висновків, списку використаної літератури, додатків.

Розділ 1 присвячений аналізу особливостей організації та функціонування Windows Server, його можливостям, принципам системного адміністрування, особливостям роботи ролей та компонентів Windows Server. Розділ 2 присвячений питанням розробки схеми адресації вузлів мереж та проектуванню налаштувань мережі. Розділ 3 присвячений створенню проекту мережної інфраструктури ЗВО, налаштуванню елементів інфраструктури, перевірці та тестуванню налаштованої мережі.

5. Висновки містять узагальнені результати проведеної роботи.

6. Список використаних літературних джерел має достатній для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

7. Додатки містять скріншоти налаштування різних компонентів та ролей Windows Server та перевірка функціонування налаштувань.

8. Таблиці та ілюстрації оформлені досить якісно, є інформативними та наведені у відповідних місцях роботи.

9. Якість оформлення роботи є високою.

10. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації усунені. Рекомендації стосовно покращення проекту враховані.

11. Ставлення студента до виконання випускної кваліфікаційної роботи – відповідальне.

12. У цілому при написанні випускної кваліфікаційної роботи студент Іванов Д.А. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Архітектура комп'ютера», «Операційні системи», «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж», «Хмарні технології», «Теорія систем і системний аналіз». Також студент Іванов Д.А. показав вміння знайти необхідну літературу та інші інформаційні джерела, правильно проаналізувати їх та використати здобуті знання, створити закінчений цілісний продукт (у вигляді змодельованого проекту) і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Іванова Д.А. написана на високому рівні та може бути допущена до захисту в Екзаменаційній комісії.

Пропонована оцінка – «відмінно».

Науковий керівник
к.т.н., доцент, доцент кафедри КІ та КБ Россінський Ю. М.
1 червня 2020 року

РЕЦЕНЗІЯ
на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Іванова Дмитра Анатолійовича
на тему: „Проект мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows "

Кваліфікаційна робота студента Іванова Д.А. „Проект мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows" присвячена актуальній тематиці – впровадженню у повсякденну діяльність та освітній процес ЗВО сучасних засобів інформаційних технологій.

Робота містить реалізований у середовищі моделювання GNS3 і середовищі віртуалізації VirtualBox проект мережної інфраструктури на базі рішень Microsoft Windows та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, десять додатків.

У першому розділі пояснювальної записки проаналізовано основні можливості операційної системи Windows Server та основні питання адміністрування мереж, розглянуто особливості компонентів та ролей операційної системи Windows Server.

У другому розділі пояснювальної записки проаналізовано поставлене завдання, розбито його на окремі задачі, спроектовано реалізацію кожної із задач, розроблено схему IP-адресації вузлів мережі.

У третьому розділі пояснювальної записки наведено опис створення проекту та опис процесу налаштування його складових, а саме налаштування серверів ОС Windows Server. У цьому ж розділі виконано перевірку працездатності проекту.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані гарні фахові компетентності, які отримані як під час навчання, так і у процесі виконання роботи. Матеріал пояснювальної записки викладено логічно, науково та технічно грамотно. Ілюстративний матеріал (рисунки, таблиці), що міститься у пояснювальній записці роботи, оформлений якісно і наведений у відповідних місцях. Оформлення роботи у цілому відповідає вимогам стандартів. Функціонал розробленого проекту мережної інфраструктури закладу вищої освіти є належним.

Позитивною стороною є те, що отриманий результат має практичну цінність – розроблений проект мережі можна взяти за основу при налаштуванні мережі у реальних умовах. Як недолік роботи варто зазначити, що не приділено достатньої уваги питанням масштабованості проекту.

У цілому кваліфікаційна робота студента Іванова Д.А. „Проект мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows " відповідає вимогам рівня вищої освіти «бакалавр» спеціальності 123 «Комп'ютерна інженерія» і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – «відмінно».

Рецензент,
завідувач кафедри комп'ютерних наук
к.т.н., доцент Сугоняк І.І.
10 червня 2020 р.

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 мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп’ютерна інженерія»
_____ Іванов Д.А.

Керівник, доцент кафедри КІ та КБ
_____ Россінський Ю. М.

Рецензент, завідувач кафедри КН
_____ Сугоняк І.І.

Житомир–2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу

Студента **Іванова Дмитра Анатолійовича**
Тема роботи: **Проект мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Операційна система Windows Server 2019
2. Операційна система Windows 10
3. Програмний продукт віртуалізації VirtualBox
4. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	06.04.20	06.04.20
2	Єфіменко А. А.	25.04.20	25.04.20
3	Єфіменко А. А.	20.05.20	20.05.20

Керівник _____ Россінський Ю. М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 9 квітня 2020	Виконано
2	Пошук та аналіз інформації щодо роботи Microsoft Windows	10 квітня 2020 – 12 квітня 2020	Виконано
3	Пошук та аналіз інформації про адміністрування мережевої інфраструктури на базі рішень Microsoft Windows	13 квітня 2020 – 18 квітня 2020	Виконано
4	Пошук та аналіз інформації щодо ролей та компонентів Microsoft Windows	19 квітня 2020 – 30 квітня 2020	Виконано
5	Пошук та встановлення образів віртуальних машин	1 травня 2020 – 2 квітня 2020	Виконано
6	Розробка схеми мережі	2 травня 2020 – 3 квітня 2020	Виконано
7	Налагодження головного сервера мережі	4 травня 2020 – 17 травня 2020	Виконано
8	Налагодження альтернативного сервера мережі	18 травня 2020 – 21 травня 2020	Виконано
9	Тестування роботи мережі	22 травня 2020 – 24 травня 2020	Виконано
12	Аналіз виконаної роботи	25 травня 2020 – 25 травня 2020	Виконано
13	Написання пояснювальної записки	26 травня 2020 – 29 травня 2020	Виконано
14	Підготовка презентації та виступу	30 травня 2020 – 31 травня 2020	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2020 – 8 червня 2020	Виконано
16	Захист	13 червня 2020	Виконано

Студент _____ Іванов Д. А.

Керівник _____ Россінський Ю. М.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи на тему «Проект мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури.

Текстова частина викладена на 64 сторінках друкованого тексту.

Пояснювальна записка має 59 сторінок додатків. Список використаних джерел містить 30 найменувань і займає 4 сторінки. В роботі наведено 56 рисунків та 1 таблиця. Загальний обсяг роботи – 123 сторінок.

У першому розділі наведена теоретична частина про Windows Server, про основні завдання адміністрування та задачі адміністратора, про копмоненти та ролі Windows Server, як вони працюють і яке їх призначення.

У другому розділі проведено аналіз поставлено завдання та розбиття його на задачі, проектування розробки мережі, адресація мережі.

У третьому розділі проведено налаштування та створення проекту мережі, налаштування ролей та компонентів Windows Server, відбувається перевірка та тестування роботи локальної мережі на базі рішень Microsoft Windows.

Висновок містить результати виконаної роботи.

Ключові слова: WINDOWS SERVER, DHCP, DNS, FOLDER, USER, ADMIN, SERVER, IP, GPO, VIRTUALBOX, WINDOWS, ACCOUNT, SHARED, SUBFOLDER, BACKUP, SCRIPT, POWERSHELL.

ABSTRACT

The explanatory note to the qualification work on the topic "Project of network infrastructure of a higher education institution based on Microsoft Windows solutions" consists of a list of abbreviations, introduction, three sections, conclusions, list of references.

The text is set out on 64 pages of printed text.

The explanatory note has 59 pages of appendices. The list of used sources contains 30 names and occupies 4 pages. The explanatory note contains 56 illustrations and 1 table. The total volume of work is 123 pages.

The first section provides a theoretical part about Windows Server, the main tasks of administration and administrator tasks, the components and roles of Windows Server, how they work and what their purpose.

In the second section, the analysis of the task and its division into subtasks, design of network development, network addressing.

The third section configures and creates a network project, configures roles and components of Windows Server, checks and tests the operation of the local network based on Microsoft Windows solutions.

The conclusion contains the results of the work performed.

Keywords: WINDOWS SERVER, DHCP, DNS, FOLDER, USER, ADMIN, SERVER, IP, GPO, VIRTUALBOX, WINDOWS, ACCOUNT, SHARED, SUBFOLDER, BACKUP, SCRIPT, POWERSHELL.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7

ВСТУП 8

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ МЕРЕЖ НА БАЗІ РІШЕНЬ MICROSOFT WINDOWS 9

1.1 Теоретичні відомості про Windows Server 9

1.2 Теоретичні відомості про адміністрування мереж Microsoft 11

1.3 Теоретичні відомості про ролі та компоненти Windows Server 12

Висновки до першого розділу 21

РОЗДІЛ 2. РОЗРОБКА ІНФРАСТРУКТУРИ МЕРЕЖІ УНІВЕРСИТЕТУ 23

2.1 Аналіз поставленої задачі 23

2.2 Проектування мережі університету 26

2.3 IP-адресація мережі 31

Висновки до другого розділу 32

РОЗДІЛ 3. НАЛАШТУВАННЯ МЕРЕЖІ УНІВЕРСИТЕТУ 33

3.1 Налаштування мережі 33

3.2 Налаштування Windows Server 36

3.3 Перевірка налаштувань Windows Server 50

Висновки до третього розділу 58

ВИСНОВКИ 59

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 60

ДОДАТКИ 64

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – Програмне забезпечення.

VB – VirtualBox.

GNS3 – Graphical Network Simulator.

MS – Microsoft Windows.

DHCP – Dynamic Host Configuration Protocol.

WS – Workstation.

IP – Internet Protocol.

IP address – Internet Protocol address.

GPO – Group Policy Object.

RDP – Remote Desktop Protocol.

DNS – Domain Name System.

DFS – Distributed File System.

ВСТУП

Актуальність теми. Сучасний заклад вищой освіти неможливо уявити без власної мережі. З кожним роком все збільшується і збільшується кількість вищих навчальних закладів, які мають власну локальну мережу на базі рішень Microsoft Windows. З кожним роком кількість студентів зростає, і тому потрібно розширювати локальну мережу кожному вищому навчальному закладу.

Актуальність даної теми полягає в тому, що мережа на базі рішень Microsoft Windows є досить зручним і гнучким інструментом для навчання та здійснення перевірки якості навчання. Також така мережа є досить маштабованою, її легко змінити, або ж додати щось нове.

Метою випускної роботи є створення, налаштування та перевірка мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows.

Зі встановленої мети випливають наступні завдання:

1. пошук та аналіз підходів по створенню та налаштуванню мережі;
2. вибір оптимального підходу;
3. розробка мережі;
4. вибір усіх потрібних компонентів та ролей для сервера;
5. налаштування всіх компонентів та ролей.

Об'єктом дослідження є процес налаштування мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows.

Предметом дослідження є використання можливостей Windows Server для створення мережної інфраструктури закладу вищої освіти.

В процесі виконання випускної роботи було налаштовано Windows Server, створено мережну інфраструктуру закладу вищої освіти, що складається з двох серверів, було налаштовано взаємодію між серверами у разі перевантаження чи виходу з ладу одного з них.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ МЕРЕЖ НА БАЗІ РІШЕНЬ MICROSOFT WINDOWS

1.1 Теоретичні відомості про Windows Server

Windows Server 2019 - це операційна система Microsoft, яка була створена для роботи серверів. Сервери - це спеціалізовані комп'ютери, які в основному працюють у мережі клієнт-сервер; сервери отримують та обробляють запити від клієнтів мережі мережі. Використання операційної системи сервера дає можливість іншим програмам запускатись на апаратному забезпеченні сервера, і це може допомогти заповнити різні функції серверних завдань

Microsoft Windows Server 2019 заснований на популярному Windows Server 2016 і спрямований на зменшення бізнес-ризику та підвищення безпеки за рахунок декількох шарів безпеки та захисту, вбудованих в операційну систему.

Microsoft Windows Server 2019 доступний у двох виданнях, стандартному та центрі обробки даних.

Як і у Windows 10, де Microsoft відтворила значну частину основної операційної системи, враховуючи зміни в ландшафті, спричинені смартфонами та планшетами, Windows Server 2019 являє собою кульмінацію кількох принципів: обчислення, ідентичність, управління та автоматизація, мережа, зберігання та безпека. Windows Server 2019 розбивається на основні елементи ОС, вкладаючи технології віртуалізації, Active Directory, системного адміністрування, управління мережею та програмним забезпеченням (SDN), управління дисками та доступністю, а також інтеграція та управління хмарами разом, щоб принести підприємству майбутні технології - не відмовляючись від обладнання, яким вони зараз користуються.

Windows Server Datacenter 2019 - це повноцінна серверна операційна система. Він пропонує широкий спектр нових та оновлених функцій стандартної версії, при цьому зменшує масштаб інших, пропонуючи доступне, просте у використанні рішення, ідеальне для першого сервера. На відміну від

версій Standard та Server Essentials, не вимагає використання ліцензій клієнтського доступу (CAL) для кожного користувача або пристрою, що звертається до сервера, що є значною економією витрат.

Перехід від попередніх версій Windows Server надає системним адміністраторам та розробникам модернізовану безпеку для захисту віртуальних машин, шифрування мережевих передач за допомогою встановленого програмного забезпечення мережі та надання розширених можливостей захисту від зберігання та відновлення після аварій функції відмови та реплікації.

Нові можливості:

- синхронна реплікація сховищ на рівні блоків з підтримкою географічно розподілених кластерів;
- віртуальний мережевий контролер (software-defined networking stack) для одночасного управління фізичними і віртуальними мережами. Новий формат файлів конфігурації віртуальних машин (.VMCX і .VMRS), з більш високим ступенем захисту від збоїв на рівні сховища. Також можна буде оновлювати версії конфігураційних файлів;
- можна створювати снепшоти прямо з гостьової ОС;
- повноцінний Storage Quality of Service (QoS) - можливість динамічного відстеження продуктивності сховищ і гаряча міграція віртуальних машин при перевищенні цими сховищами порогових значень (IOPS);
- зміни в самому Hyper-V: використання альтернативних акаунтів (зберігання декількох облікових даних однієї людини, можливість використання за часом), можливість управління попередніми версіями Hyper-V в корпоративній інфраструктурі, оновлення і поліпшення протоколу віддаленого управління, можливість безпечного завантаження гостьових операційних систем Linux;
- можливість поновлення Integration Services через Windows Update;

- сумісність з режимом Connected Standby;
- додана підтримка протоколу HTTP / 2;
- Windows PowerShell 5.0.

Відмінні риси Windows Server 2019:

- управління серверами в стилі DevOps за допомогою PowerShell і налаштування стану;
- нові елементи управління і доступу через Active Directory і посвідчення;
- просте управління серверами з будь-якого місця за допомогою Server Management;
- сервіси віддалених робочих столів для поліпшення графіки, масштабування і хмарної інтеграції;
- поліпшення кластеризації і вбудованої віртуалізації завдяки програмно-визначеним обчислень;
- нові рівні захисту від мінливих загроз;
- скорочення місця, займаного центром обробки даних, і площі атаки завдяки Nano Server.

1.2 Теоретичні відомості про адміністрування мереж Microsoft

Адміністратор мережі – фахівець, що відповідає за нормальне функціонування і використання ресурсів автоматизованої системи і (або) обчислювальної мережі.

Адміністрування інформаційних систем включає наступні цілі:

- встановлення і налаштування мережі;
- підтримка її подальшої працездатності;
- встановлення базового програмного забезпечення;
- моніторинг мережі.

У зв'язку з цим адміністратор мережі повинен виконувати такі завдання:

- планування системи;
- встановлення і конфігурація апаратних пристроїв;
- встановлення програмного забезпечення;
- встановлення мережі;
- архівування (резервне копіювання) інформації;
- створення та керування користувачами;
- встановлення і контроль захисту;
- підтримка працездатності;
- моніторинг продуктивності.

Забезпечення працездатності системи вимагає і здійснення профілактичних заходів. Адміністратор повинен забезпечувати задоволення санкціонованих запитів користувачів.

Очевидно, що ефективно виконувати всі ці функції і завдання, особливо в складних великих комп'ютерних мережах, людині дуже важко, а часом і неможливо. Успішне адміністрування, особливо складними комп'ютерними мережами, реалізується шляхом застосування новітніх засобів і систем автоматизації цих процесів.

1.3 Теоретичні відомості про ролі та компоненти Windows Server

Active Directory (AD) - продукт Microsoft, який складається з декількох служб, які працюють на Windows Server для управління дозволами та доступом до мережевих ресурсів.

Active Directory зберігає дані як об’єкти. Об'єкт - це окремий елемент, такий як користувач, група, програма чи пристрій, наприклад принтер. Об'єкти зазвичай визначаються як ресурси - наприклад, принтери чи комп'ютери - або принципи безпеки - такі як користувачі або групи.

Active Directory класифікує об'єкти за назвою та атрибутами. Наприклад, ім'я користувача може містити рядок імені разом з інформацією, пов'язаною з користувачем, таким як паролі та захищені оболонки (SSH).

Основна послуга в Active Directory - доменні служби (AD DS), які зберігають інформацію про каталоги та обробляють взаємодію користувача з доменом. AD DS перевіряє доступ, коли користувач входить у пристрій або намагається підключитися до сервера через мережу. AD DS контролює, які користувачі мають доступ до кожного ресурсу. Наприклад, адміністратор, як правило, має інший рівень доступу до даних, ніж кінцевий користувач.

Інші продукти Microsoft, такі як Exchange Server і SharePoint Server, надають AD DS для доступа до ресурсів. Сервер, на якому розміщено AD DS, є контролером домену.

Групи безпеки можуть надати ефективний спосіб призначення доступу до ресурсів в мережі. За допомогою груп безпеки ви можете виконувати наступні дії:

- призначення прав користувачів групам безпеки в ActiveDirectory. Права користувачів призначаються групі безпеки, щоб визначити, які члени цієї групи можуть виконувати дії в рамках домену. Права користувачів автоматично призначаються деяким групам безпеки при установці ActiveDirectory, щоб допомогти адміністраторам визначити роль адміністратора користувача в домені.
- призначення дозволу групам безпеки для ресурсів. Дозволи не відрізняються від прав користувачів. Дозволи призначаються групі безпеки загального ресурсу. Дозволи визначають, хто може отримувати доступ до ресурса і рівень доступу, наприклад "повний доступ". Деякі дозволи, задані для об'єктів домену, автоматично призначаються для вирішення різних рівнів доступу для груп безпеки за замовчуванням, наприклад для груп «Оператори обліку» або «Адміністратори домену».

Реплікація DFS дозволяє синхронізувати файлові директорії (replicated folders) між серверами, які входять в реплікації групи (replication group).

Сервери в реплікаційній групі пов'язані між собою сполуками (connections), так що існує шлях між будь-якими двома і більше серверами.

Дані можна реплікувати як в межах локальної мережі, так і через глобальну WAN мережу. Технологія DFSR була спроектована з розрахунком на повільні WAN мережі і працює так само надійно через Інтернет, як і в межах однієї будівлі.

Групова політика - це інструмент, доступний для адміністраторів, які працюють з архітектурою Active Directory. Він дозволяє централізовано керувати налаштуваннями на клієнтських комп'ютерах і серверах, підключених до домену, а також забезпечує простий спосіб поширення програмного забезпечення.

Групові політики дозволяють налаштовувати параметри для певного набору користувачів або комп'ютерів всередині домену Active Directory. Також дозволяють вказувати політики в одному місці для групи і застосувати до цільового набору користувачів.

Групові політки надають можливість застосування стандартного набору налаштувань і конфігурацій для груп користувачів або комп'ютерів в домені або за запитом. За допомогою групових політик можна створити набори налаштувань для конкретних груп користувачів в домені. За допомогою Active Directory GPO можна встановити і управляти окремими уніфікованими наборами налаштувань, конкретно для певних груп користувач.

Конфігурації для комп'ютерів або користувачів простіші і ефективніші, тому що розташовані в одному місці і не вимагають повтору на кожному комп'ютері.

Існує два компонента групових політик - серверний компонент і клієнтський, тобто дана структура відноситься до архітектури "клієнт-сервер".

Серверний компонент - оснащення Microsoft Management Console (MMC), яка використовується для вказівки налаштувань групової політики. MMC може бути використана для створення політик контролю і управління

адміністративними шаблонами і налаштуваннями безпеки (скрипти, установка ПО і інше). Кожен з них називається розширенням і в свою чергу кожен з них має дочірнє розширення, яке дозволяє додавання нових компонентів або оновлення існуючих без можливості торкнутися або піддати ризику всю політику.

Клієнтський компонент інтерпретує і застосовує налаштування групової політики для комп'ютерів користувачів або цільових користувачів. Клієнтські розширення - це компоненти, які запущені на користувальницької системі і несуть відповідальність за інтерпретацію обробки і застосування в об'єкти групової політики.

Для адміністрування GPO використовують Group Policy Management Console (GPMC) і Group Policy Management Editor.

Сценарії використання Active Directory GPO:

- централізоване налаштування пакету програм Microsoft Office;
- централізоване налаштування управлінням живленням комп'ютерів;
- налаштування веб-браузерів і принтерів;
- встановлення і оновлення ПЗ;
- застосування певних правил в залежності від місця розташування користувача;
- централізовані налаштування безпеки;
- перенаправлення каталогів в межах домену;
- налаштування прав доступу до додатків і системних програм.

Параметри групових політик розділені на два основні розділи:

- конфігурація комп'ютера управляє параметрами, специфічними для роботи комп'ютера;
- конфігурація користувача управляє параметрами, специфічними для роботи користувача.

DHCP - це абревіатура від Dynamic Host Configuration Protocol. Так називається протокол, який відповідає за динамічне налаштування вузла мережі

з використанням моделі OSI. DHCP отримав нову прикладну реалізацію для сучасного IPv6.

Існує всього три схеми роздачі IP:

- динамічна;
- автоматична;
- ручна.

Схема роботи - клієнт-серверна. DHCP дає можливість автоматично налаштувати IPv4 / IPv6 і виключити з процесу управління параметрами мережі людський фактор. У більшості випадків налаштування зводиться до завдання пулу IP-адрес, які будуть закріплюватися за клієнтськими пристроями. Крім того, адміністратор може задавати час, протягом якого IP-адреса буде закріплена за клієнтським MAC. Після закінчення цього часу IP може зайняти інший мережний пристрій.

Суть першого методу полягає в тому, що ПК отримує IP-адресу на певний термін, або lease time. Після цього мережева адреса може бути закріплена за іншим персональним комп'ютером. Динамічний варіант роздачі застосовується на 95% всіх серверів.

Автоматичний спосіб схожий з вище розглянутим. Різниця полягає в тому, що комп'ютеру присвоюється не динамічний, а статичний IP.

При ручному способі розподілу сисадмін становить матрицю відповідності MAC і IP-адрес. Метод мало популярний і застосовується виключно в мережах з високими вимогами до безпеки.

В локальній мережі має завжди бути два сервера – головний і альтернативний. В такому випадку потрібно налаштувати роботу двох серверів, щоб вони не конфліктували та не заважали один одному. Можуть бути такі шляхи вирішення:

- використання розділених областей (Split Scope) – це розподіл адресного пулу між двома серверами. В такому випадку головний сервер видає певний відсоток адрес, наприклад 75%, а альтернативний

– 25%. Якщо ж головний сервер стане непрацездатним, альтернативний візьме все навантаження на себе і клієнт отримає IP-адресу від нього;

- відмовостійкість (Failover) – в даному випадку не відбувається розподіл адресового пулу, а тільки у разі відмови головного сервера, альтернативний приймає на себе все навантаження.

Рішення відмовостійкості може працювати у двох режимах:

- балансування навантаження (Load Balance Mode) – в даному режимі головний і альтернативний сервер одночасно видають IP-адреси клієнтам. Можна розподілити навантаження на сервера, по-замовчуванню – йде розподіл 50 на 50;
- режим гарячої заміни (Hot Standby Mod) – працює тільки головний сервер, а якщо він перестає працювати, все навантаження на себе приймає альтернативний. Головний сервер являється активним, а альтернативний – пасивним.

Служба доменних імен (DNS) - це один із стандартних галузевих протоколів, що включають TCP / IP, а клієнти DNS і DNS-сервер надають службам дозволи імен IP-адрес комп'ютерів і користувачів.

У Windows Server 2019 DNS є роллю сервера, яку можна встановити за допомогою диспетчера сервера або команд Windows PowerShell. При установці нового лісу Active Directory і домену служба DNS автоматично встановлюється з Active Directory в якості глобального сервера каталогу для лісу та домену.

Служби домену Active Directory Services (AD DS) використовують DNS в якості механізму розташування контролера домену. При виконанні будь-якої з основних Active Directory операцій, таких як перевірка справжності, оновлення або пошук, комп'ютери використовують DNS для пошуку контролерів домену Active Directory. Крім того, контролери домену використовують DNS для розміщення один одного.

Служба DNS-клієнта входить в усі клієнтські і серверні версії операційної системи Windows і працює за замовчуванням при установці операційної системи. Під час налаштування мережевого підключення TCP / IP з IP-адресою DNS-сервера клієнт DNS запитує DNS-сервер для виявлення контролерів домену та дозволяє імена комп'ютерів в IP-адреси. Наприклад, коли користувач мережі з обліковим записом користувача Active Directory входить в домен Active Directory, служба DNS-клієнта запитує у DNS-сервера пошук контролера домену для Active Directory домену. Коли DNS-сервер відповідає на запит і надає клієнту IP-адреса контролера домену, клієнт зв'язується з контролером домену, і процес перевірки автентичності може бути розпочато.

DNS-сервер Windows Server 2019 і служби DNS-клієнта використовують протокол DNS, включений в набір протоколів TCP / IP.

На DNS-сервері є три види зон:

- основна зона (Primary zone) – DNS-сервер з даною зоною стає основим;
- додаткова зона (Secondary zone) – DNS-сервер, на якому налаштований даний вид зони, являється альтернативним і отримує зону від головного сервера;
- зона заглушка (Stub zone) – DNS-сервер стає джерелом відомостей тільки при повноважних серверах імен для цієї зони.

Служба віддалених робочих столів - це програмний компонент, який дозволяє дистанційно запускати додатки або керувати сервером з будь-якого пристрою, на якому встановлений відповідний клієнт і є доступ по локальній мережі або інтернету. Компонент Remote Desktop Services (RDS) в першій версії називався Terminal Services, або «Служби терміналів», він входить в серверні і клієнтські модифікації операційних систем Microsoft Windows. Спочатку протокол розрахований на використання малопотужними клієнтами ресурсів більш продуктивного сервера.

Вона забезпечує роботу з більш потужним комп'ютером (сервером) в віддаленому режимі, тобто щоб підключитися до нього дистанційно і потім працювати там з встановленими додатками. RDS використовується компонентами, які відповідають за функціонування віддаленого помічника, підключення до віддалених робочих столів і швидке переключення користувачів.

У звичайному сеансі роботи RDS з клієнтського комп'ютера на сервер надходять сигнали клавіатури і миші, а також передається зображення з екрану. Ці дані мало важать, тому не створюють навантаження на мережу. Винятки бувають, коли потрібно передати великий обсяг мультимедійних файлів - тоді RDS забезпечує підтримку перенаправлених аудіо і відео сигналів. Також ця служба дозволяє працювати з локальними дисками і принтерами, з PnP-пристроями, вміє передавати позначки часу в електронних листах і файлах. Нещодавно у неї з'явилася підтримка дисплеїв з високою роздільною здатністю (4096 × 2048 пікселів) і передача нарізаного на фрагменти зображення на групу моніторів.

Компонент RDS за замовчуванням поставляється з більшістю версій операційної системи Windows, але в залежності від номера версії його можливості можуть трохи відрізнятися - наприклад, Windows Server без покупки додаткових ліцензій підтримує підключення тільки двох віддалених користувачів до одного робочого столу.

Remote Desktop Services - компонент дозволяє розгорнути на одному пристрої програми, до яких мають доступ користувачі інших (клієнтських) пристроїв. Це корисно в рішенні ряду типових для бізнесу завдань:

- розгортання ПО. Завдяки RDS прискорюється установка будь-якого програмного забезпечення - тепер його можна інсталювати на одному пристрої замість декількох. Це актуально для додатків, які відрізняються складністю і трудомісткістю в розгортанні та налаштування;

- скорочення числа установок до ПО. Додатки виконуються тільки на тій машині, на якій вони встановлені. На інші пристрої передається зображення того, що відбувається під час їх виконання. Це дозволяє знизити вимоги до пропускної здатності мережі, яка використовується для передачі даних між сервером і клієнтськими машинами;
- організація віддаленого доступу. До основного комп'ютера з встановленим ПО можна отримувати доступ з самих різних пристроїв: офісних ноутбуків, домашніх ПК, мобільних пристроїв. При цьому не важливо, як далеко один від одного знаходяться клієнтське і серверне обладнання - головне, щоб між ними був встановлений канал зв'язку (дані можна передавати по локальній мережі або через інтернет). Такий спосіб «спілкування» можна налагодити між віддаленими філіями і центральним офісом компанії.

RDP (англ. Remote Desktop Protocol - протокол віддаленого робочого стола) - проприєтарний протокол прикладного рівня, придатний для організації віддаленої роботи користувача з серверами, на якому закрили службу термінальних підключень. Клієнти існують практично для всіх версій Windows (включаючи Windows CE, Phone і Mobile), Linux, FreeBSD, Mac OS X, iOS, Android, Symbian. Встановлення ролі RDP на сервері Windows відбувається в двох етапах: заздалегідь встановлюється служба віддалених робочих столів, після цього визначається сервер ліцензування.

Резервне копіювання Windows Server – компонент операційної системи Windows Server, який допомагає створювати резервні копії та відновлювати дані з створених резервних копій. Компонент надає можливість створювати резервну копію як цілого сервера, так і деяких томів, або ж копію стану системи, чи певних папок та файлів. Після створення резервної копії, можна відновити дані з неї. Є можливість запланувати створення резервних копій. Зазвичай, бажано запланувати створення вночі, коли на сервер найменше навантаження.

Windows PowerShell - це оболонка, спочатку була розроблена Microsoft для автоматизації завдань та управління конфігурацією. PowerShell тепер є проектом з відкритим кодом, і його можна встановити на платформах Windows, macOS та Linux. Ця оболонка базується на рамках .NET, і вона включає оболонку командного рядка та мову скриптів.

Microsoft розробила Windows PowerShell як інструмент, який допомагає автоматизувати та швидко вирішувати безліч копітких завдань адміністрування. Також є можливість ідентифікувати та вбивати процеси, які не відповідають або фільтрувати конкретну інформацію про комп'ютери в мережі, та експортувати її у форматі HTML.

Windows PowerShell - це надзвичайно потужний інструмент, який входить у Windows, і який доступний для багатьох інших операційних систем. Це приносить багато переваг IT-фахівцям.

Найпоширеніші команди це:

1. Get-.
2. Show-.
3. New-.
4. Remove-.
5. Start-.
6. Stop-.
7. Copy-.
8. Import-.
9. Export-.

Вище зазначені команди можна використовувати для будь-яких цілей. Вони використовуються всюди.

Висновки до першого розділу

В першому пункті розділу було розказано теоретичні відомості про Windows Server. Було розглянуто нові можливості даного продукту, його

відмінності, особливості, частково розглянуто архітектуру. Також порівнювались різні редакції даного продукту.

В другому пункті було розглянуто теоретичні відомості про адміністрування мереж. Було розглянуто цілі системного адміністратора, що він має знати та вміти. Також було розглянуто задачі системного адміністратора.

В третьому пункті було розглянуто теоретичні відомості про ролі та компоненти Windows Server. Було розглянуто детально про кожний компонент та ролі, які налаштовувались. Було розглянуто принципи роботи даних ролей та компонентів.

РОЗДІЛ 2. РОЗРОБКА ІНФРАСТРУКТУРИ МЕРЕЖІ УНІВЕРСИТЕТУ

2.1 Аналіз поставленої задачі

Для правильного та легкого налаштування роботи операційної системи Windows Server, потрібно спочатку проаналізувати поставлене завдання і вимоги до серверу. У даному випадку, потрібно налаштувати мережеву інфраструктуру закладу вищої освіти на базі рішень Microsoft Windows. Налаштовуємо мережу університету. Нехай даний заклад матиме назву «ZSTU». В ньому буде два факультети – «FIKT» та «FEM». Виходячи за цього, потрібно зрозуміти, які задачі будуть реалізовуватись.

Однією з перших задач, це буде створення системи серверів на базі рішень Microsoft Windows. Декілька серверів потрібні для того, аби підтримувати працездатність системи. Маючи два, або більше, сервери, постійна робота мережі гарантована, адже у разі припинення роботи одного з серверів, інший візьме на себе його роль та все навантаження, поки інший сервер буде ремонтуватись. Для даного університету достатньо буде лише двох серверів.

Наступна задача пов’язана з попередньою. Так як в даному університеті буде не один, а два сервера, потрібно налаштувати між ним вз’яємодію. Це потрібно для того, щоб використати всі можливості, які надаються та зробити, аби сервери не конфліктували між собою.

Головною підзадачею буде те, що у разі припинення роботи головного сервера, альтернативний приймав усе навантаження на себе і ставав тимчасовим головним сервером. Також потрібно врахувати той факт, що після відновлення роботи головного сервера, має відбутися синхронізація даних. Це потрібно для того, аби не відбулося втрати даних.

Додатковою підзадачею буде налаштування серверів так, щоб у разів великого навантаження одного сервера, інший приймав частину навантаження на себе. Це корисна практика, адже в такому випадку менша ймовірність того, що сервер перестане працювати, а також пришвидшиться відповідь сервера,

адже якщо головний сервер зайнятий і не можу відповісти на той чи інший запит, альтернативний сервер прийме даний запит на себе і виконає його замість головного сервера.

Однією з останніх задач при налаштуванні сервера є створення власної резервної копії. Це потрібно для того, аби відновити дані та стан системи сервера, у разі повного або часткового знищення системи сервера. Бажано зберігати резервну копію у місце, доступне з іншого сервера, а не на самий сервер.

Наступною задачею є надання доступу до мережі користувачам. У даному випадку буде 4 вида користувачів:

– адміністратори;
– студенти факультету «FIKT»;
– студенти факультету «FEM»;
– викладачі.

Усі користувачі матимуть доступ до мережі, але при цьому матимуть свій рівень пріоритетів. Найвищий рівень, звичайно, у адміністратора. Найнижчий – у студента будь-якого факультету. На рисунку 2.1 показана ієрархія облікових записів користувачів відповідно до рівня пріоритетів.

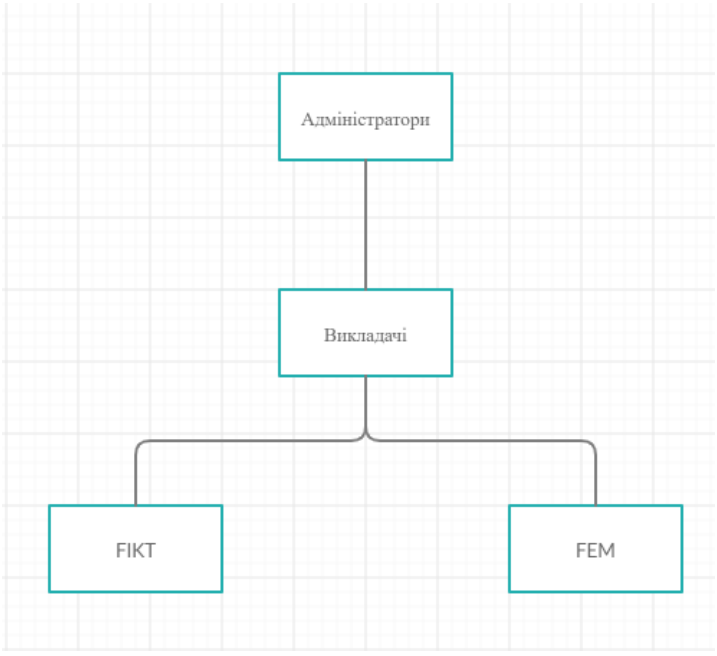


Рис. 2.1. Ієрархія облікових записів

Наступною задачею є налаштування спільного доступу до ресурсів. В даному випадку на сервері університету буде створена та поширена на всіх користувачів мережі папка. В даній папці буде три підкаталоги:

– підкаталог факультету «FIKT»;
– підкаталог факультету «FEM»;
– підкаталог результатів.

Кожен студент матиме доступ лише до свого факультету, курсу та групи. У даних підкаталогах він зможе змінювати файли, додавати свої файли із виконаним завданням. У підкаталозі результатів, студенти матимуть лише можливість перегляду, а викладачі матимуть повний доступ.

Підзадачею буде доступ до принтерів. Для студентів буде доступно декілька принтерів, але для кожного факультету буде доступний лише свій принтер. Це буде реалізовано для того, аби зменшити навантаження на один принтер та збільшити продуктивність друку.

Однією з головних задач буде налаштування групових політик. Групові політики надають широкий спектр можливостей. Завдяки коректному налаштуванню групових політик, можна дозволяти, або забороняти, користувачам, або робочим станціям, певні дії, можливості, функціонал. На рисунку 2.2 показано як працють групові політики. А найголовніше, за допомогою групових політик можна розповсюджувати ПЗ. Використовуючи такий метод встановлення та налаштування ПЗ, економиться велика кількість часу та зусиль, а також при такому підході на всіх робочих станція мережі буде встановлено однакове ПЗ. Для даного університету за допомогою групових політик встановимо декілька програм – веб-браузер та архіватор.

Додатковою задачею буде налаштування віддаленого доступу для викладачів. Це корисно, адже якщо студент забуде пароль і потрібно швидко його змінити, або потрібно швидко встановити нове ПЗ для роботи на занятті, то викладач матиме можливість сам підключись до сервера і налаштувати або змінити все, що йому треба.



Рис. 2.2. Принцип роботи групових політик

Після аналізу усіх поставлених задач, потрібно спроектувати розробку мережі університету «ZSTU». Це буде зроблено у наступному розділі.

2.2 Проектування мережі університету

В попередньому пункті було проаналізовано поставлені задачі та визначено основний функціонал мережі університету «ZSTU». В даному розділі буде спроектовано розробку даної мережі. Це потрібно для того, аби швидко та якісно створити та налаштувати мережу університету «ZSTU». Налаштування та детальніше пояснення деяких можливостей доступне у наступному, третьому, розділі.

Перед тим, як налаштовувати та протестити створену систему, потрібно буде встановити та налаштувати ПЗ, для роботи системи, адже доступу до реального обладнання немає. Для виконання цієї задачі, буде використано GNS3 та VirtualBox. Після встановлення та налаштування ПЗ, можна переходити до налаштування мережі університету «ZSTU».

Одніє з перших задач, яку було розглянуто, це створення системи серверів. В попередньому пункті було розглянуто та пояснено для чого це потрібно. Для університету «ZSTU» буде використано операційну систему Windows Server, як основну операційну систему для налаштування мережі серверів. Для початку

потрібно налаштувати головний сервер, встановити на нього контролер домену та налаштувати новий домен.

Після виконання цієї задачі, перейдемо до наступної, яка пов’язана з даною – альтернативний сервер. Для цього знадобиться ще один сервер. На нього також встановлюється та налаштовується контролер домену. Але не створюється новий домен. Даний сервер додається в уже існуючий домен. Після того, як це буде виконано, вже можна створювати систему серверів. На головному сервері додаємо інший сервер, який буде виконувати роль альтернативного. На рисунку 2.3 показана частина майбутньої мережі університету «ZSTU».

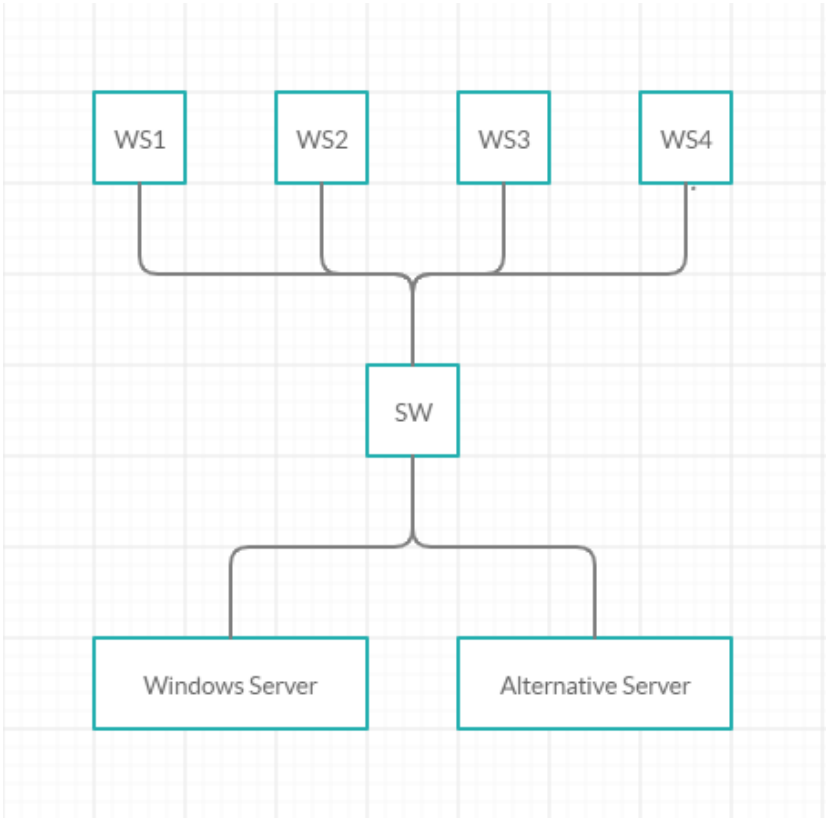


Рис. 2.3. Частина мережі університету

Після налаштування двох серверів та об’єднання їх в систему, перейдемо до наступної задачі. Так, як маємо два сервери, потрібно коректно налаштувати роботу між них. Це стосується таких ролей як DNS та DHCP. Для початку потрібно буде встановити дані ролі на обидва сервери. Після встановлення, спочатку треба налаштувати ролі на головному сервері. Почнемо з DNS.

Спочатку на головному сервері налаштовуємо головну та додаткову зони на головному сервері. Під час налаштування вказуємо IP-адресу альтернативного DNS-сервера. Це буде IP-адрес другого сервера. Після того, як буде налаштовано DNS на головному сервері, налаштовуємо DNS на другому сервері. Все налаштовується аналогічно, але не створюється нова головна та додаткова зони, а використовуються вже існуючі зони, які були створені на головному сервері. Далі налаштовуємо DHCP.

Спочатку налаштовуємо нову DHCP-область на головному сервері. Далі налаштовуємо на другому сервері. Після того, як на головному та альтернативному серверах було налаштовано DHCP, налаштовуємо роботу між ними. У даному випадку потрібно налаштувати розподілення навантаження між серверами. Налаштовуємо таким чином, що у разі припинення роботи головного сервера, альтернативний приймає все навантаження на себе. Під час звичайної роботи, головний сервер буде видавати 75 відсотків адрес, а альтернативний – інші 25. В такому випадку зменшиться навантаження на головний сервер. Далі налаштовуємо реплікацію між серверами.

Реплікація потрібна для синхронізації даними між серверами. Це стосується мережевих каталогів. Для цього потрібно встановити відповідні ролі на обох серверах мережі. Після того, як вони будуть встановлені, потрібно налаштувати реплікацію відповідних папок. Налаштовуємо на головному сервері. Для цього потрібно обрати мережеву папку на цьому сервері. Саме вона буде синхронізуватись. Далі потрібно обрати папку, з якою вона буде синхронізуватись. Після цього буде встановлений зв’язок між папками, і як тільки одна з ним буде змінена, ці зміни з’являться в іншій папці. На рисунку 2.4 показаний зв’язок між ними.

Далі налаштовуємо створення резервних копій. Для цього потрібно на обидва сервери встановити відповідні ролі. Після того налаштувати створення резервних копії на кожному сервері. У даному випадку, краще створювати резервні копії вечером-вночі, адже в цей час найменше навантаження на

сервери. В даному випадку резервні копії будуть створюватись о 22:00. Зберігатися резервні копії будуть у мережевій папці «Backups».

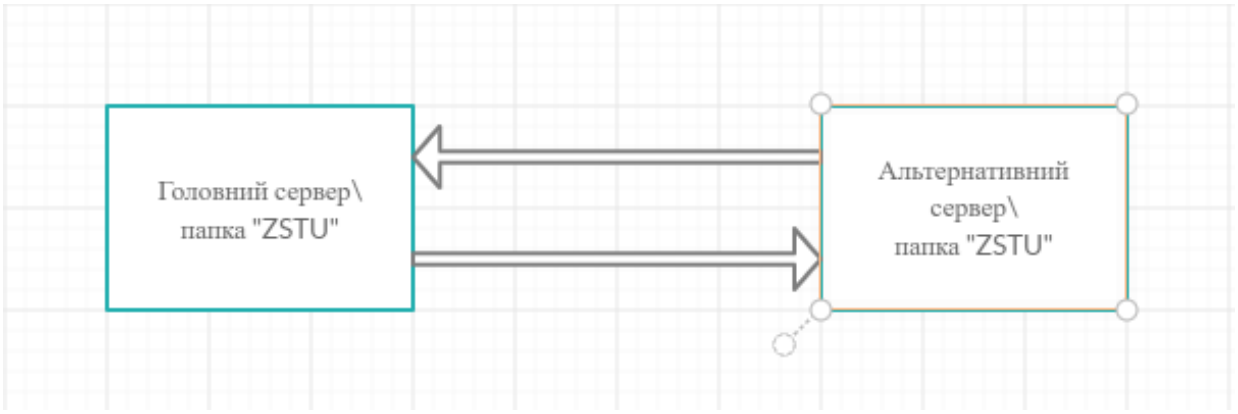


Рис. 2.4. Зв’язок між мережевими папками

Додатково також потрібно розглянути створення резервної копії в даний момент. Для цього використаємо можливості PowerShell та напишемо скрипт, запускаючи який, буде створюватись резервна копія диску «C» та стану системи сервера. Дану резервну копію також будемо зберігати у мережевій папці «Backups». В ній буде створюватись підкаталог, який матиме у назві повну дату та час створення резервної копії.

Далі налаштовуємо доступ користувачів до мережі. У даному випадку буде зручно порозбивати все на групи користувачів. Це буде зручно у майбутньому, адже у такому підході легше щось змінити, або додати. Для початку потрібно буде створити підрозділ «ZSTU». В ньому створимо групу користувачів для факультету FIKT, FEM та викладачів. Також створимо підрозділ для аналогічних груп користувачів. У підрозділі для викладачів створимо облікові записи викладчів та додамо ці записи до групи користувачів «Teachers_ALL». Далі для кожного з факультетів створимо групи користувачів для кожного з чотирьох курсів. У підрозділах для кожного з факультетів створимо підрозділ для студентів цього факультету та групи користувачів для кожної групи студентів. У підрозділі вже створюємо облікові записи користувачів. Додаємо дані облікові записи до відповідних груп користувачів відповідної групи. Далі відповідну групу додаємо до відповідного курсу. Після цього додаємо відповідні курси факультетів до груп користувачів «FIKT_ALL» та

«FEM_ALL». Після того, як все це буде налаштовано, можемо переходити до реалізації наступної задачів.

Далі створюємо мережу папку на головному сервері. Надамо доступ до цієї папки всім користувачам мережі університету «ZSTU». Цю папку розділяємо на три підкаталоги: папка для студентів FIKT, для студентів FEM та для результатів студентів. Надаємо доступ до даних підкаталогів відповідним групам користувачів – до підкаталогу «FIKT» надаємо доступ групі користувачів «FIKT_ALL». Для підкаталогу «FEM» потрібно провести аналогічні дії. Підкаталогу «Results» надаємо доступ обом групам користувачів, але з обмеженими правами. Далі, в підкаталогах «FIKT» та «FEM» створюємо підкаталоги для кожного курсу та надаємо доступ групам користувачів відповідних курсів відповідних факультетів. Далі створюємо підкаталоги для кожної групи та надаємо доступ відповідній групі користувачів. На рисунку 2.5 показана структура мережевої папки для факультету «FIKT».

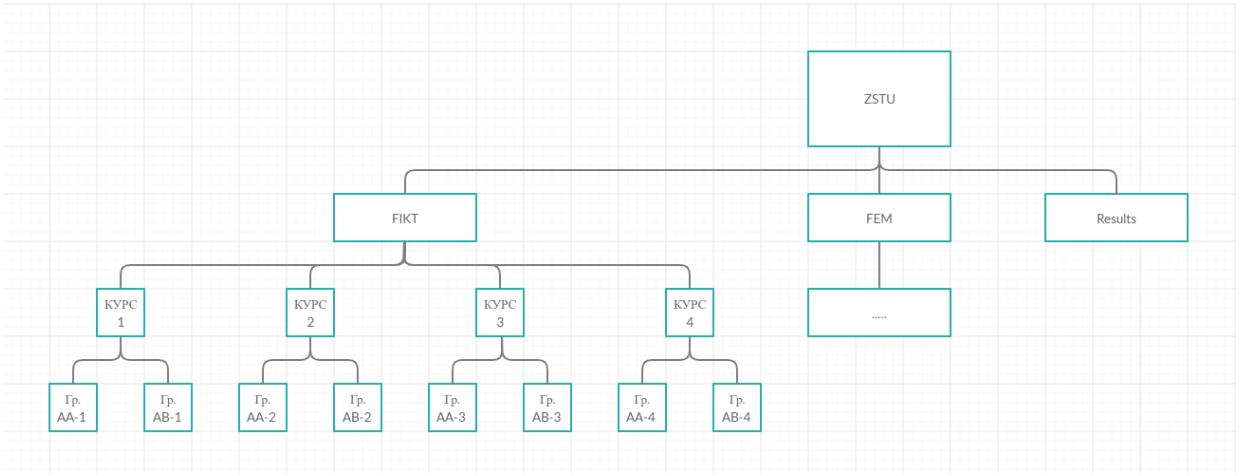


Рис. 2.5. Структура мережевої папки «ZSTU»

Далі налаштуємо роботу з принтерів. Налаштуємо три принтера – для кожного з факультетів та один для викладачів. Далі використаємо налаштоввані раніше групи користувачів. Надамо доступ до таких гру користувачів – «FIKT_ALL», «FEM_ALL» та «Teachers_ALL».

Далі налаштуємо роботу групових політик. Створимо об’єкти групових політик на основі груп користувачів – «FIKT_ALL», «FEM_ALL» та

«Teachers_ALL» та зв’яжемо їх. Далі налаштовуємо дозволи та заборони для відповідних факультетів. Ці налаштування прив’язані до облікових записів і будуть застосовуватись на відповідні облікові записи. Тобто, всі ці зміни застосовуються під час входу користувачів в облікові записи. В наступному, третьому, розділі під час налаштування буде детально описано усе, що було налаштовано.

Також, за допомогою групових політик встановимо ПЗ. Для його встановлення потрібно буде скачати інсталяційні файли з розширенням «.exe». Детально описаний процес встановлення та налаштування буде в наступному розділі.

2.3 IP-адресація мережі

В даній мережі університету «ZSTU» налаштуємо просту мережу. Розробимо схему адресації. Адреси з 1 по 32 будуть зарезервовані, і використовуватись не будуть. Вони будуть використовуватись для серверів, робочих станцій, які повинні мати статичний IP-адрес, маршрутизаторів та, якщо потрібно, комутаторів. Також не будуть використовуватись адреси з 233 по 254. Вони будуть використовуватись для принтерів та подібних пристроїв. Всі інші IP-адреси будуть роздаватись робочим станціям. Нижче буде представлена таблиця IP-адресії.

Табл. 2.1

Адресація мережі

Тип адреси	Діапазон	Префікс
Зарезервований	198.2.8.1 – 198.2.8.32 198.2.8.233 – 198.2.8.254	/24
Вільний	198.2.8.33 – 198.2.8.232	

Висновки до другого розділу

В першому пункті розділу було проаналізовано поставлене завдання та розбито його на задачі, для кращого розуміння. Також було виділено підзадачі, котрі було б користу реалізувати.

В другому пункті було спроектовано налаштування мережі університету «ZSTU». Було детально описано та пояснено за допомогою чого та як буде відбуватися налаштування мережі університету «ZSTU».

В третьому пункті було проведено розробку адресації даної локальної мережі університету «ZSTU».

РОЗДІЛ 3. НАЛАШТУВАННЯ МЕРЕЖІ УНІВЕРСИТЕТУ

3.1 Налаштування мережі

Для початку потрібно створити схему мережі університету «ZSTU». Так як GNS3 та VirtualBox вже встановлені та налаштовані, потрібно лише встановити образи серверів та робочих станцій та об’єднати все це у мережу. Почнемо з образів Windows Server.

На рисунку 3.1 показано вибір операційної системи. Обираємо операційну систему, яка показана на рисунку. Далі просто встановлюємо образ. Чекаємо поки закінчиться процес скачування та встановлення.

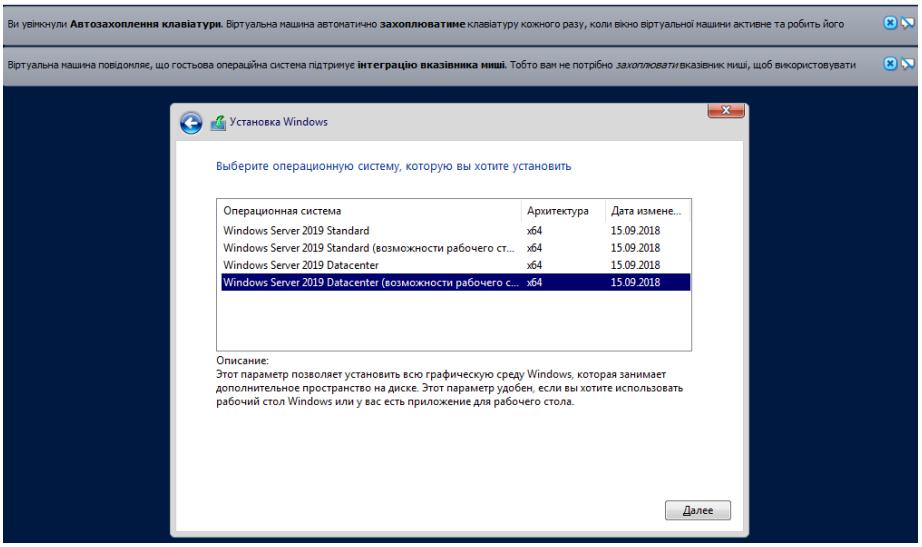


Рис. 3.1. Вибір операційної системи

На рисунку 3.2 показано процес створення облікового запису для адміністратора. Після введення паролю, образ буде доступний до використання.

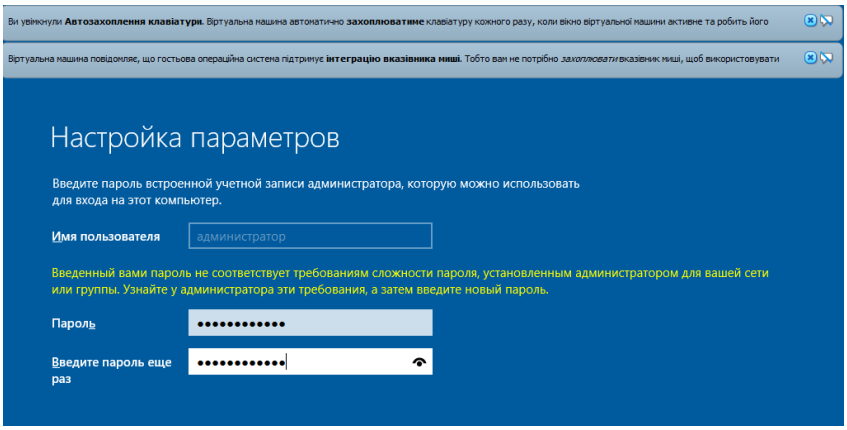


Рис. 3.2. Створення облікового запису

Далі потрібно встановити декілька образів Windows 10. Це потрібно для того, аби протестувати налаштування Windows Server. Процес встановлення аналогічний. Після встановлення також потрібно створити обліковий запис для адміністратора. На рисунку 3.3 показано встановлений образ Windows 10.

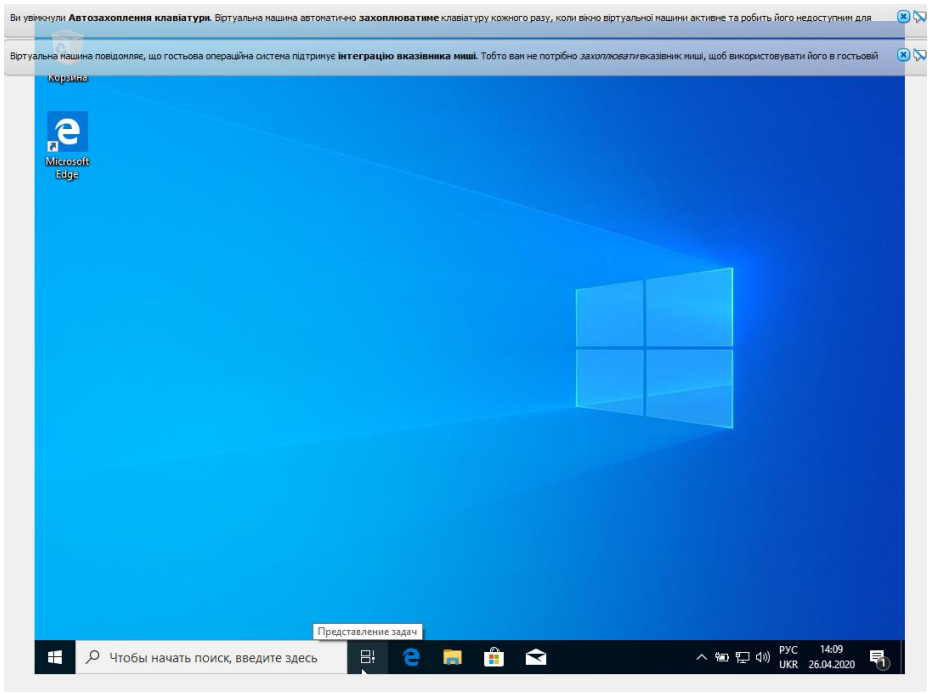


Рис. 3.3. Встановлений образ Windows 10

Далі потрібно все це об’єднати у єдину схему. У GNS3 додаємо новий шаблон. Під час налаштування потрібно вказати, що це образ VirtualBox і він буде з його допомогою запускатися. На рисунку 3.4 показано, що потрібно додати для коректного налаштування. Далі потрібно обрати образ, який потрібен. На рисунку 3.5 показано процес вибору потрібного образу.

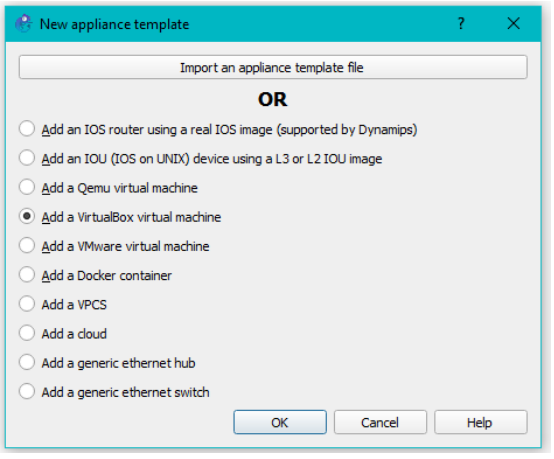


Рис. 3.4. Процес додавання образу в GNS3

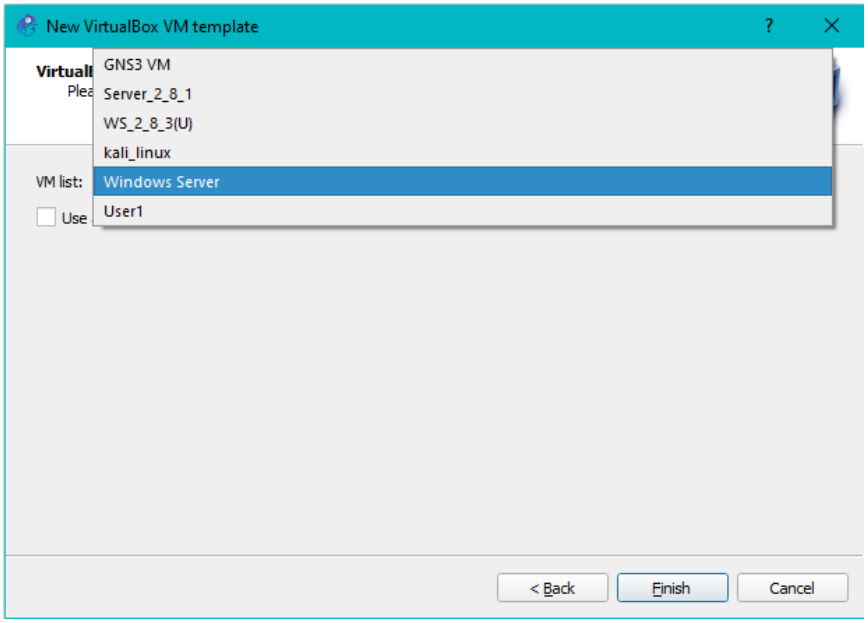


Рис. 3.5. Вибір потрібного образу

Після того, як всі образи були додані в GNS3, потрібно все це додати у проект мережі та скласти схему. Додаємо образи серверів, робочих станцій та комутатора, для того, аби все разом з'єднати. На рисунку 3.6 показана складена та працююча схема.

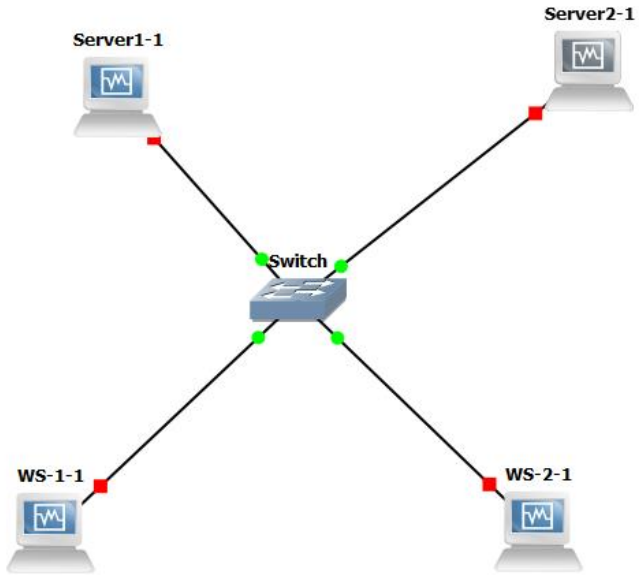


Рис. 3.6 Складена схема мережі університету

3.2 Налаштування Windows Server

В даному пункті відбуватиметься налаштування Windows Server. Для початку встановимо Active Directory. На рисунку 3.7 буде показано початок налаштування Active Directory.

На рисунку 3.8 показано всі доступні сервери, обираємо той, що нам потрібен.

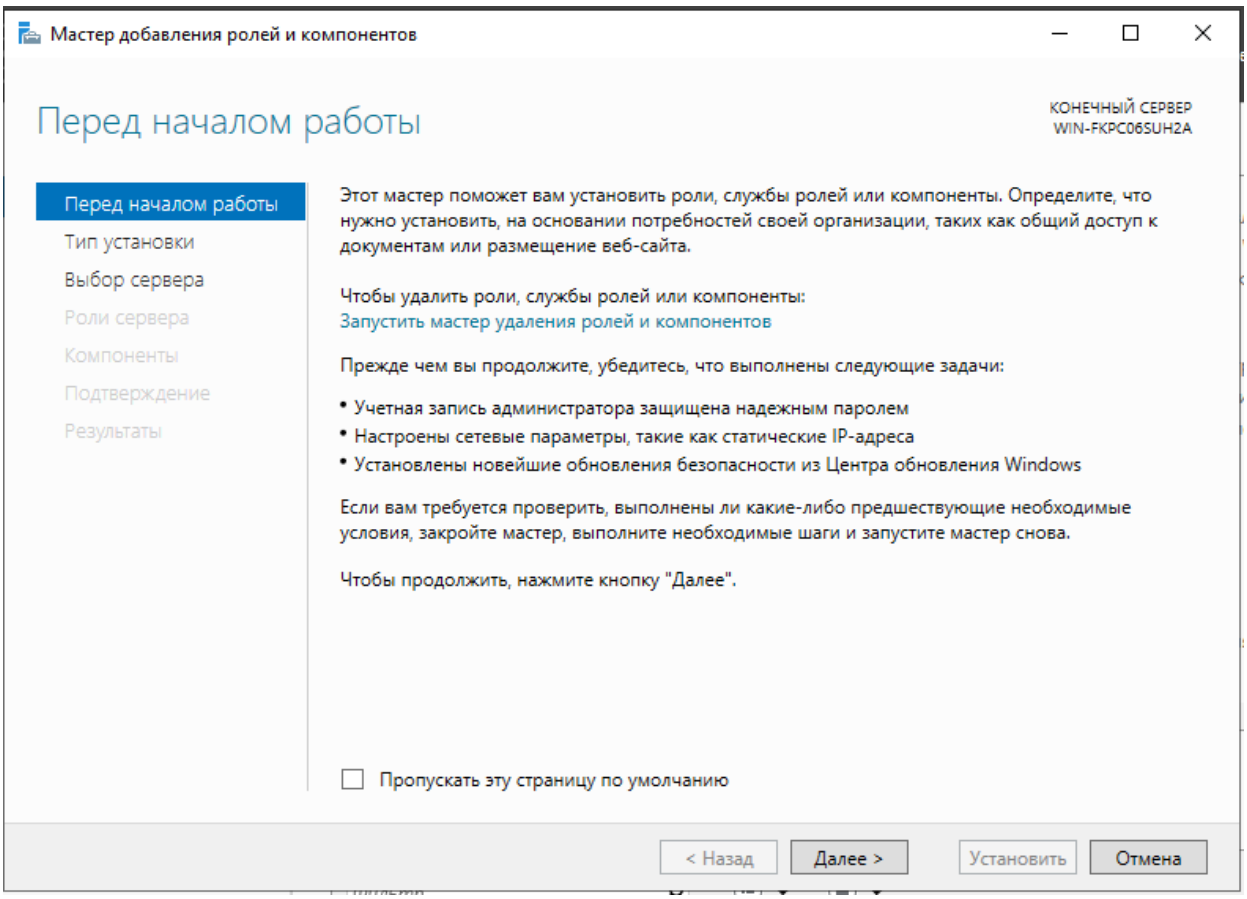


Рис. 3.7. Початок налаштування Active Directory

Далі обираємо компоненти для встановлення. На рисунку 3.9 обираємо потрібний компонент. У нашому випадку Active Directory.

На рисунку 3.10 позано процес встановлення Active Directory. Після завершення процесу встановлення Active Directory буде доступна для налаштування.

Після встановлення потрібно налаштувати Active Directory. На рисунку 3.11 показано процес налаштування Active Directory.

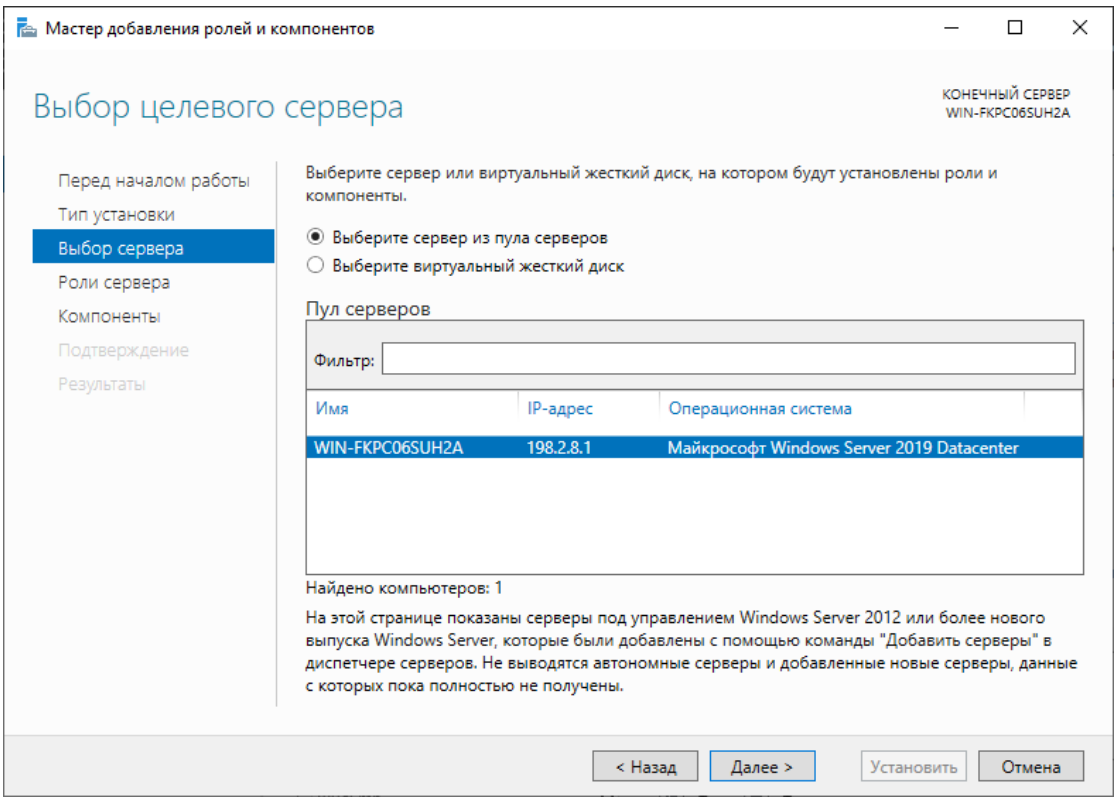


Рис. 3.8. Вибір сервера на який встановлюємо компоненти

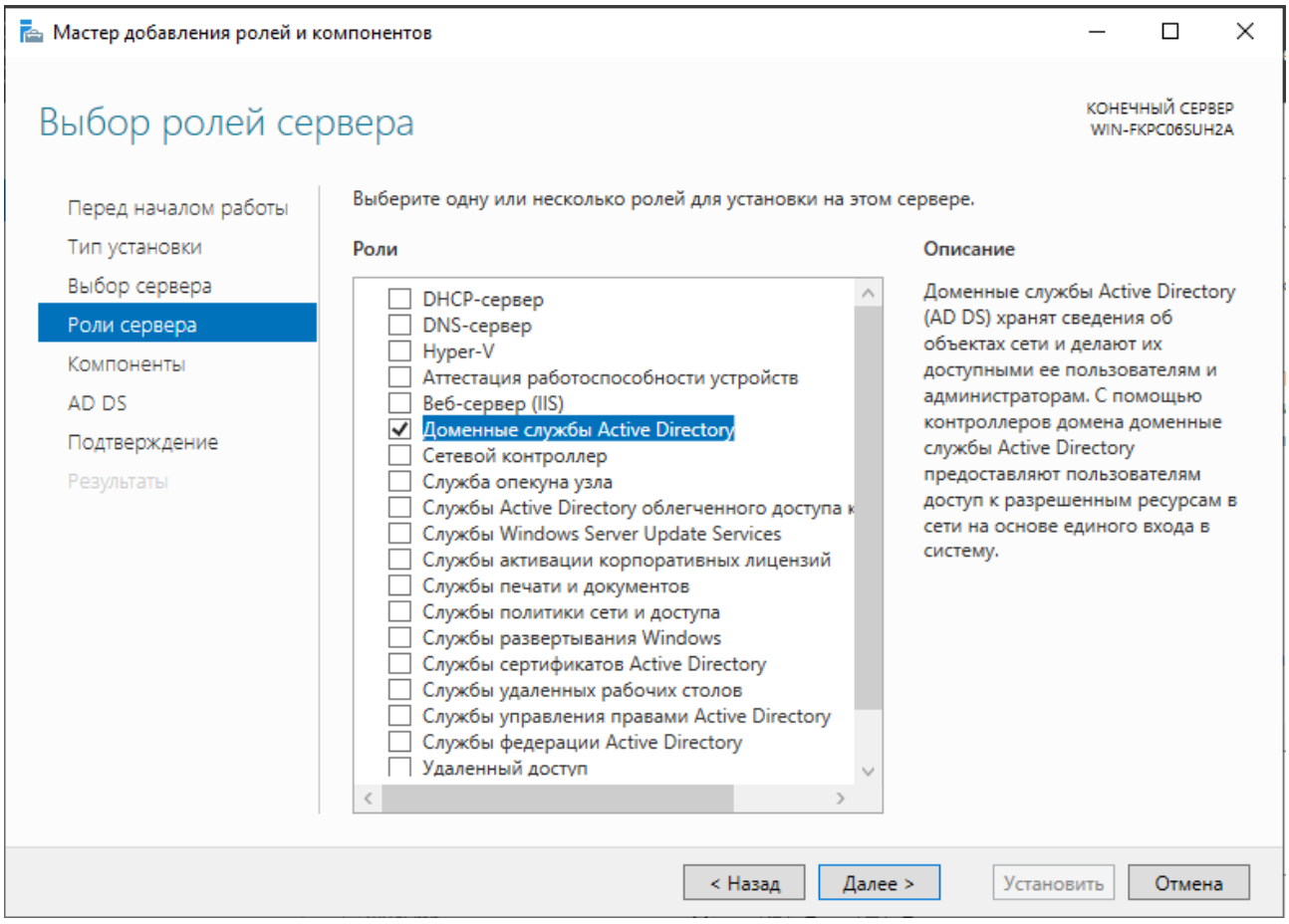


Рис. 3.9. Вибір компонентів для встановлення

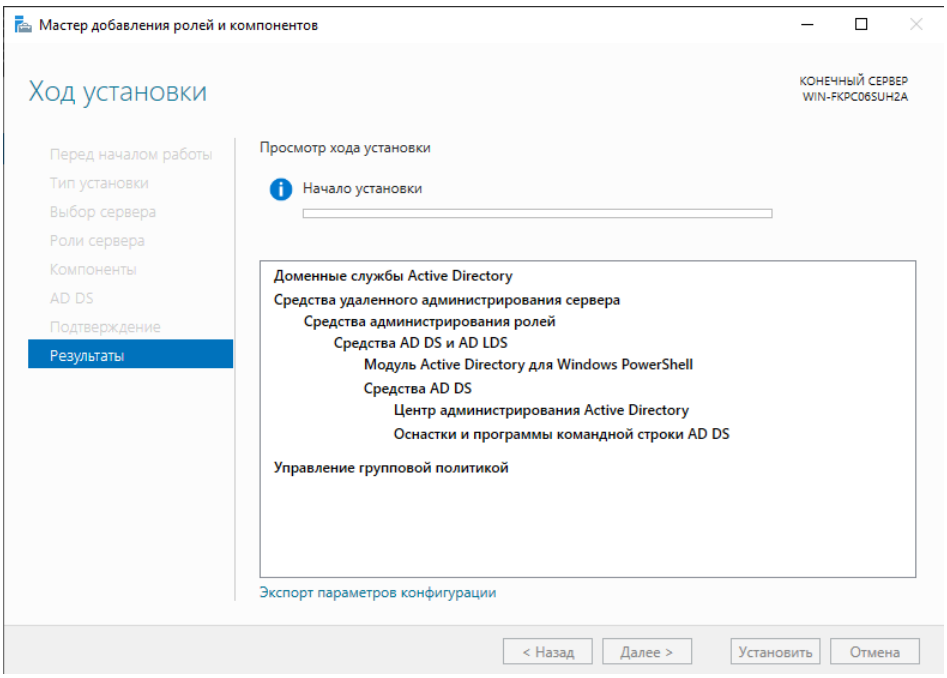


Рис. 3.10. Встановлення Active Directory

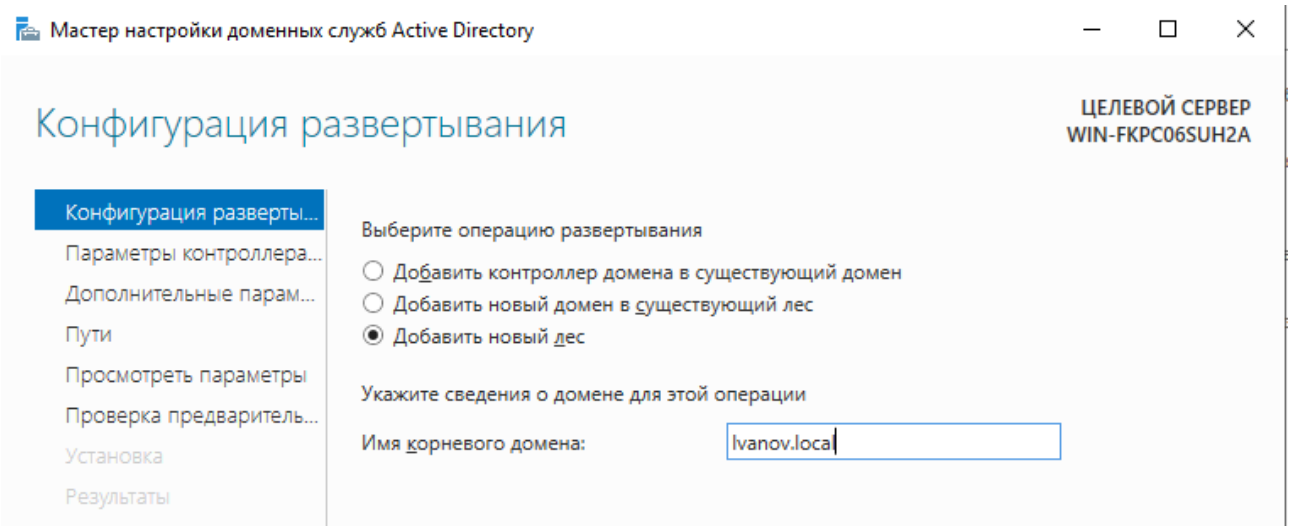


Рис. 3.11. Налаштування Active Directory

Після встановлення та налаштування Active Directory, додаємо додатковий, альтернативний сервер. Це потрібно для того, аби в разі несправності головного сервера, або великої кількості запитів, перенаправити, або зменшити навантаження на головний сервер. На рисунку 3.12 показано додання альтернативного сервера.

До того, аби мати змогу додати сервер, для початку треба ввести його в домен. На рисунку 3.12 показано успішне введення альтернативного сервера у домен.

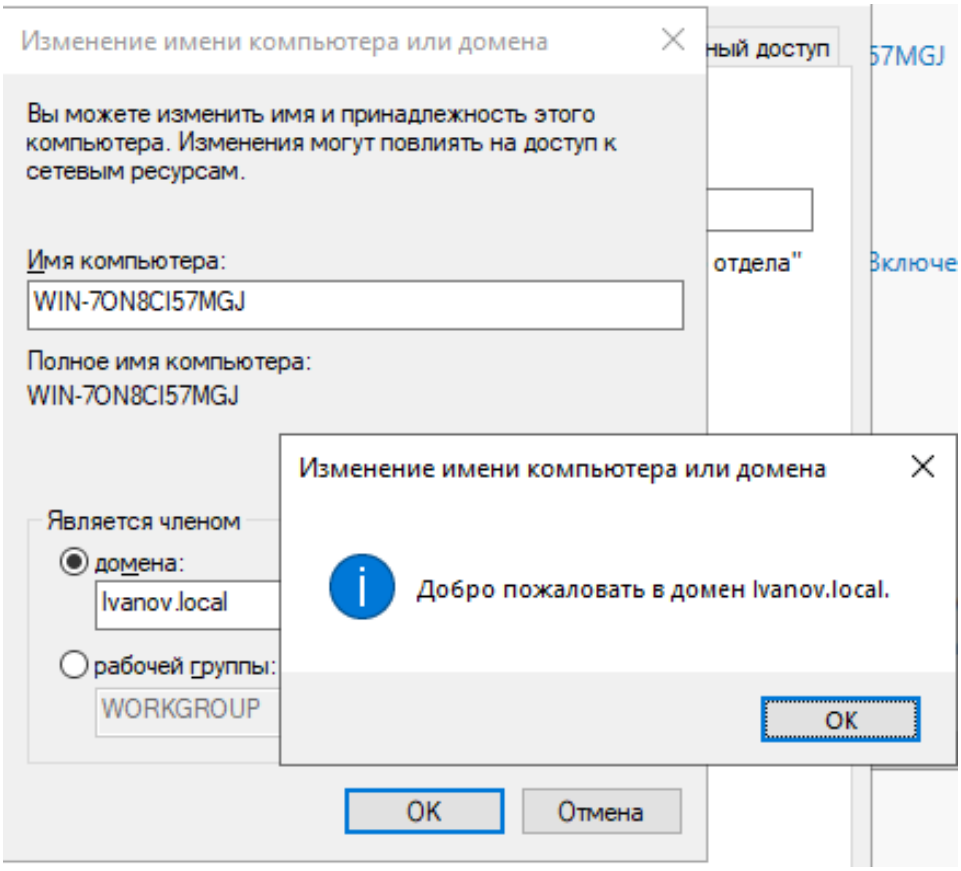


Рис. 3.12. Введення сервера у домен

Після того як сервер був введений у домен, потрібно його додати, щоб він буд доступний на головному сервері. На рисунку 3.13 показано процес додання сервера.

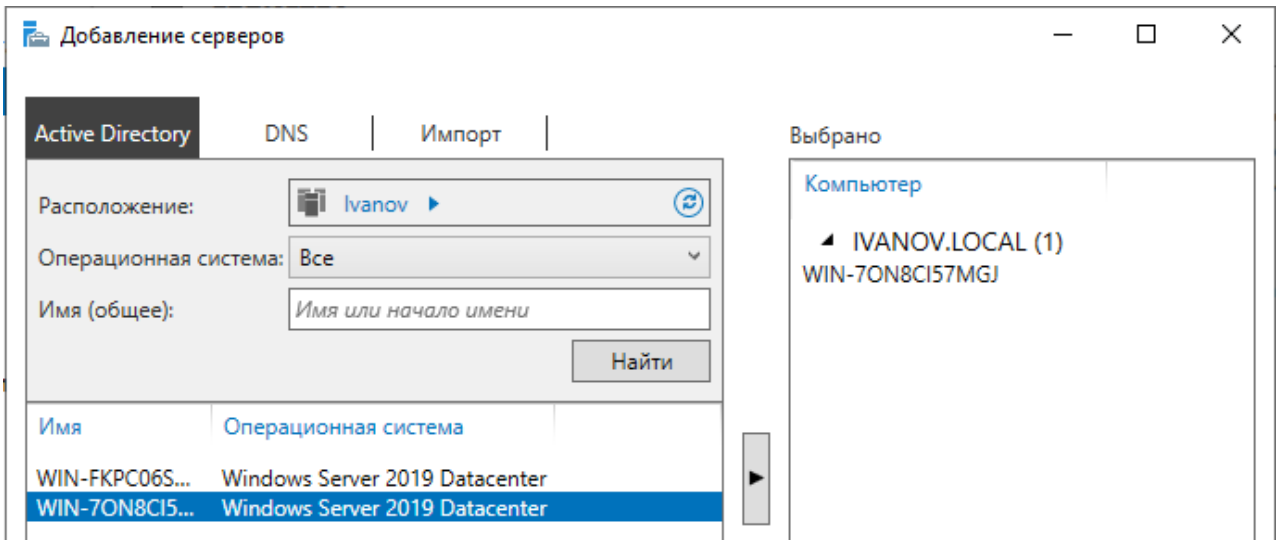


Рис. 3.13. Додання сервера

Після того як сервер був доданий, на головному сервері буде доступно два сервера для встановлення та налаштування ролей та компонентів.

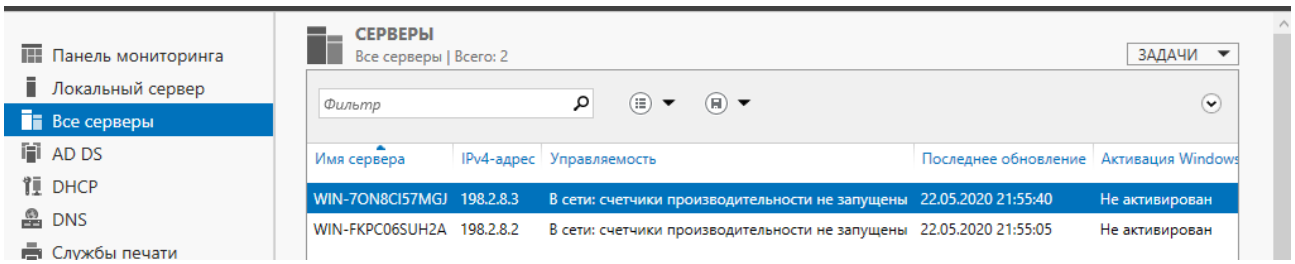


Рис. 3.14. Всі доступні сервери

Після того як сервер був доданий, потрібно налаштувати на ньому Active Directory. В даному випадку не потрібно створювати новий домен, а потрібно лише додати його до вже існуючого. Більше скріншотів налаштування доступно в додатку А.

Після встановлення Active Directory, відбувається налаштування структури університету. На рисунку 3.15 показано ієрархічну структуру підрозділів, груп та користувачів серверу. Для всіх користувачів буде доступна загальна папка «ZSTU». В ній будуть знаходитись підкаталоги – для кожного курсу. Вони, в свою чергу, матимуть свої підкаталоги – для кожної групи. Користувачі зможуть заходити тільки в каталог свого факультету, далі вони доступ до каталогу свого курсу, а далі до каталогу своєї групи. Додавати файли, редагувати існуючі зможуть у підкаталозі своєї групи.

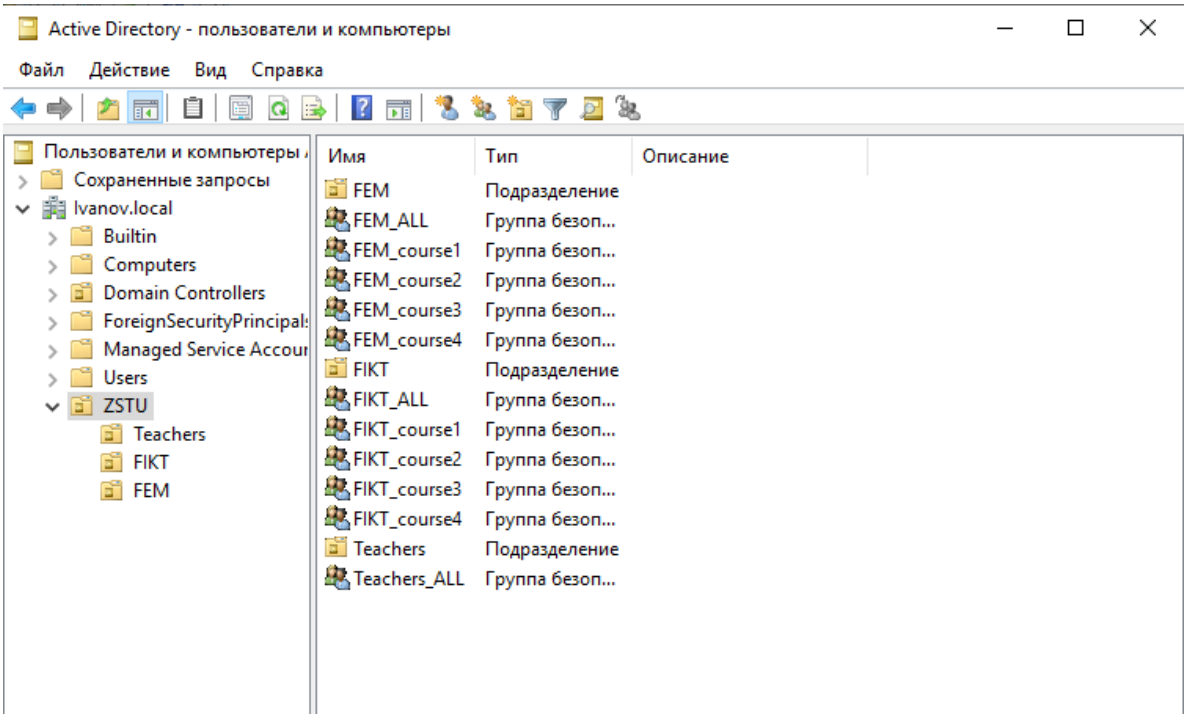


Рис. 3.15. Ієрархічна структура підрозділів

На рисунку 3.16 видно окрему групу – викладачі. Для викладачів буде окремий підкаталог, в якому вони виставлятимуть результати. Редагувати даний каталог зможуть лише викладачі. Студенти зможуть лише переглядати свої результати.

Всі скріншоти пов’язані із створенням та налаштуванням структури будуть доступні у додатку Б.

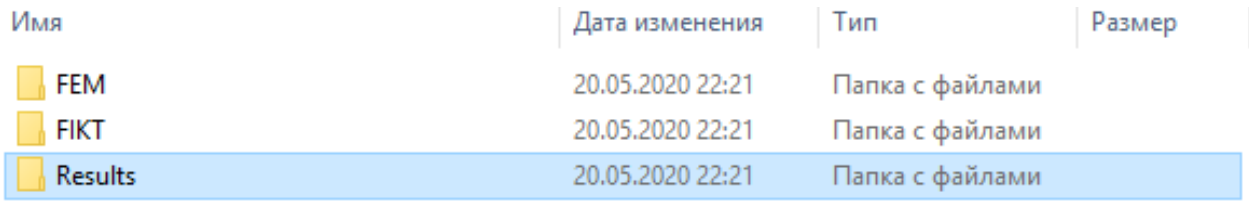


Рис. 3.16. Структура мережвої папки «ZSTU»

Далі налаштовуємо реплікацію. Це потрібно для того, якщо головний сервер вийде з ладу, можна було використовувати альтернативний сервер, а після відновлення роботи головного сервера, дані між сервера синхронізались. На рисунку 3.17 показано створену реплікацію. Додаткові скріншоти налаштування доступні в додатку В.

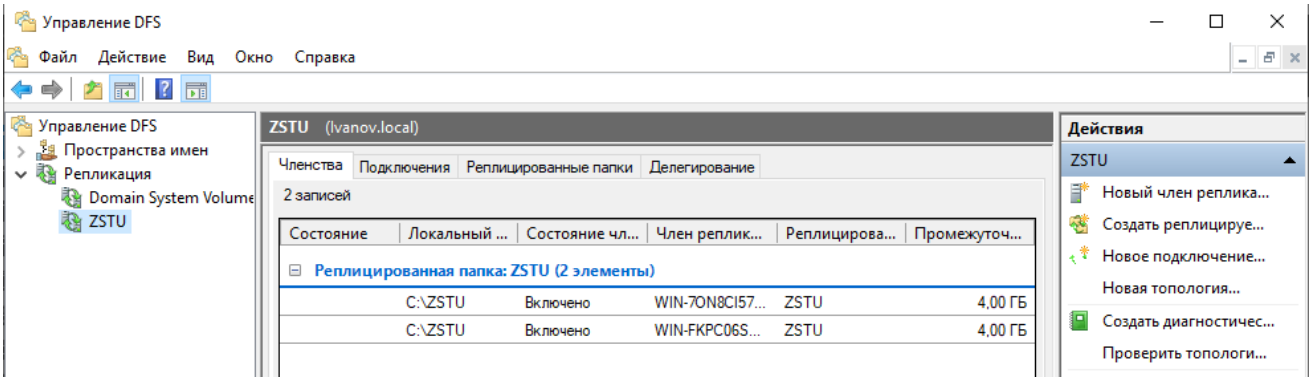


Рис. 3.17. Створена реплікація

Далі налаштовуємо групові політики Active Directory. Додаткові скріншоти встановлення, налаштування та результати групових політик доступні в додатку Г.

Після встановлення, налаштовуємо групові політики. Для кожного факультету, аби краще розібратися у всіх можливостях групових політик, налаштовуємо різні дозволи. Наприклад, студенти одного факультету матимуть

ярлик «Корзина» на робочого столу, а інші – ні. Викладачі, в свою чергу, матимуть інші дозволи.

Для початку створимо групову політику для факультету ФЕМ. Спочатку налаштуємо параметри для користувача, а вже потім для комп'ютерів. Студентам факультету налаштовано такі параметри:

- видалено «недавно додані» з меню «Запуск»;
- видалено та заборонено доступ до команд «Заверешення роботи», «Перезавантаження»;
- видалено посилання «Ігри» з меню «Запуск»;
- заборонено видаляти додатки з меню «Запуск»;
- відлючити спливаючі вікна;
- автоматичне оновлення Windows;
- дозволено пошук принтерів;
- заборонено видалення принтерів.

Вище наведено лише список головних параметрів. Більше налаштованих параметрів знаходиться на скріншотах додатку Г.

Тепер налаштуємо групову політику для студентів факультету ФІКТ. Студентам факультету налаштовано такі параметри:

- закріпити панель задач;
- видалено посилання «Ігри» з меню «Запуск»;
- видалено посилання «Пошук на комп'ютері»;
- заборонити змінення параметрів панелі задач і меню «Запуск»;
- заборонено видаляти додатки з меню «Запуск»;
- додати команду «Виконати» в меню «Запуск»;
- заборонити вручну перенаправляти папки профілей;
- заборонити доступ до ресурсів зміни реєстру.

Після надаштування параметрів для студентів факультету ФІКТ, створимо і налаштуємо групову політику для викладачів. Скріншоти налаштування всіх групових політик будуть знаходитись у додатку Г.

Після налаштування параметрів користувача, налаштуємо параметри комп’ютер.

Після налаштування параметрів користувачів, налаштовуємо параматри комп’ютерів. Встановимо на кожний комп’ютер домену ПЗ – архіватор «WinRAR». Для початку скачаємо інсталюючий файл. Інсталяція відбуватиметься в «silent» режимі. В даному режимі користувачу не потрібно буде нічого підтверджувати. ПЗ інсталюється без втручання. Для інсталяції файлів з розширенням «.exe» потрібно створити скріп, котрий описує процес інсталяції. Також для встановлення в «silent» режимі потрібен ключ. Для архіватора «WinRAR» це /s.

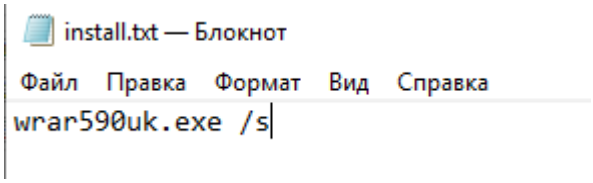


Рис. 3.18. Синтаксис скрипта

Для інсталяції файлів з розширенням «.exe» потрібно створити скріп, котрий описує процес інсталяції. Також для встановлення в «silent» режимі потрібен ключ. Для архіватора «WinRAR» це /s. Створюємо скрипт і в нього прописуємо назву інсталюючого файлу з розширенням «.exe» та ключ – /s. На рисунку 3.18 показано синтаксис скріпта. На ринку 3.19 показано сам скріпт.

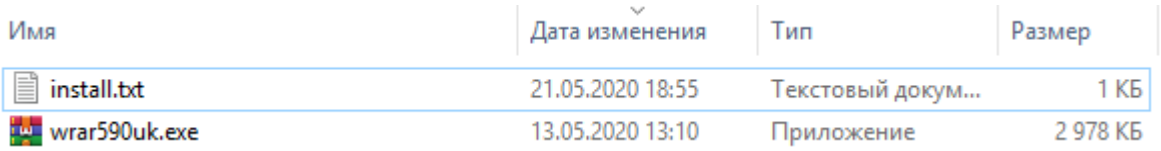


Рис. 3.19. Створений скрипт

Після створення крипта, налаштуємо новий об’єкт групової політики. Після створення нового об’єкту групової політики налаштуємо його. Створюємо нове правило для автозавантаження – це показано на рисунку 3.20. Потім натискаємо кнопку «Показати файли» і у папцу, що відкриється, вставляємо інсталюючий файл і сам скрипт. Після після натискаємо кнопку «Додати» для того, аби обрати скрипт для інсталяції ПЗ.

Після того як додали інсталюючий файл і скрипт для інсталяції ПЗ, дана групова політика застосується до всіх комп’ютерів домену.

Також до створеного і налаштованого об’єкту відключимо параметри налаштування користувачів. Це пришвидшить час застосування політики на робочій станції, адже всі зміни політики відбувалися тільки для комп’ютера, не зачіпаючи при цьому налаштування користувача.

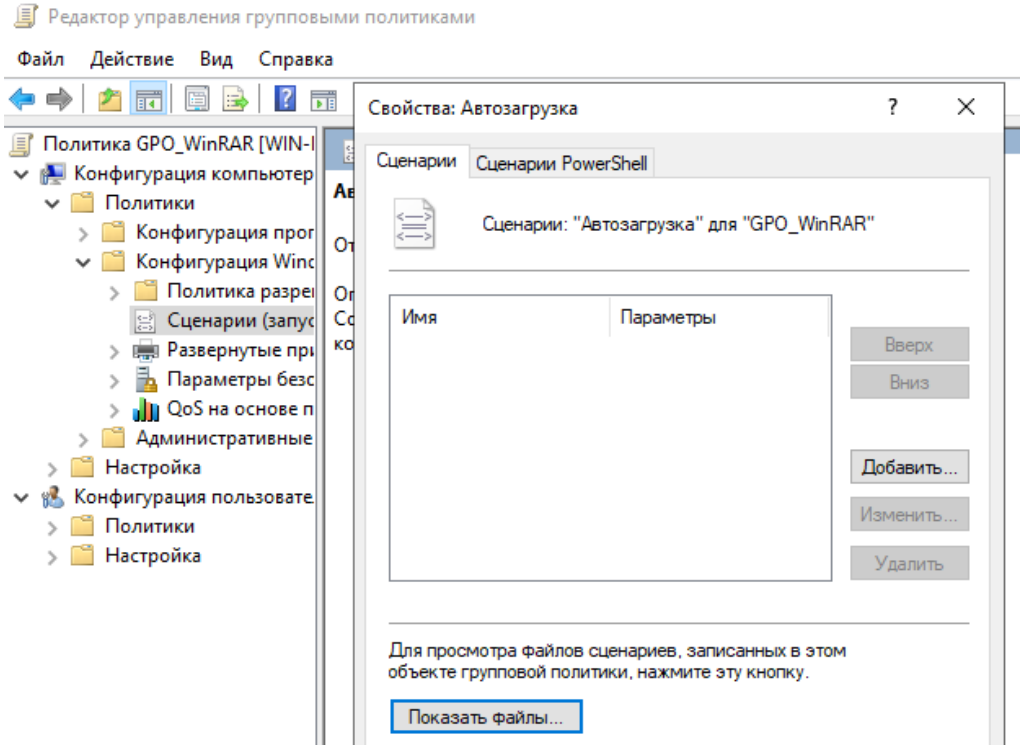


Рис. 3.20. Створення сценарію

Після встановлення архіватора, встановимо на кожен ком’ютер домену веб-браузер. В даному випадку це буде браузер «Chrome». По аналогії з попереднім прикладом створюємо новий об’єкт групової політики. Вказуємо інсталюючий файл та скрипт для інсталяції в «silent» режимі. Для встановлення в «silent» режимі потрібен також ключ. На рисунку 3.21 показаний синтаксис скрипта. Більше скріншотів буде показано у додатку Г.

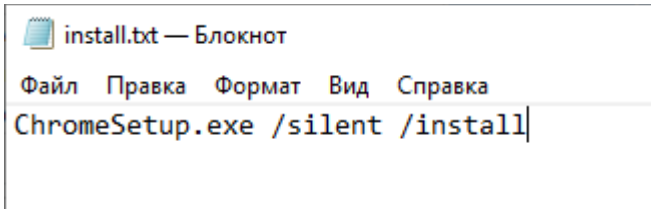


Рис. 3.21. Синтаксис скрипта

Далі налаштовуємо DHCP-сервер. Процес встановлення даного компоненту буде показано на скріншотах у додатку Д.

Після процесу встановлення, потрібно авторизуватися для завершення встановлення даного компоненту. На рисунку 3.22 показана авторизація для налаштування DHCP-сервера після встановлення.

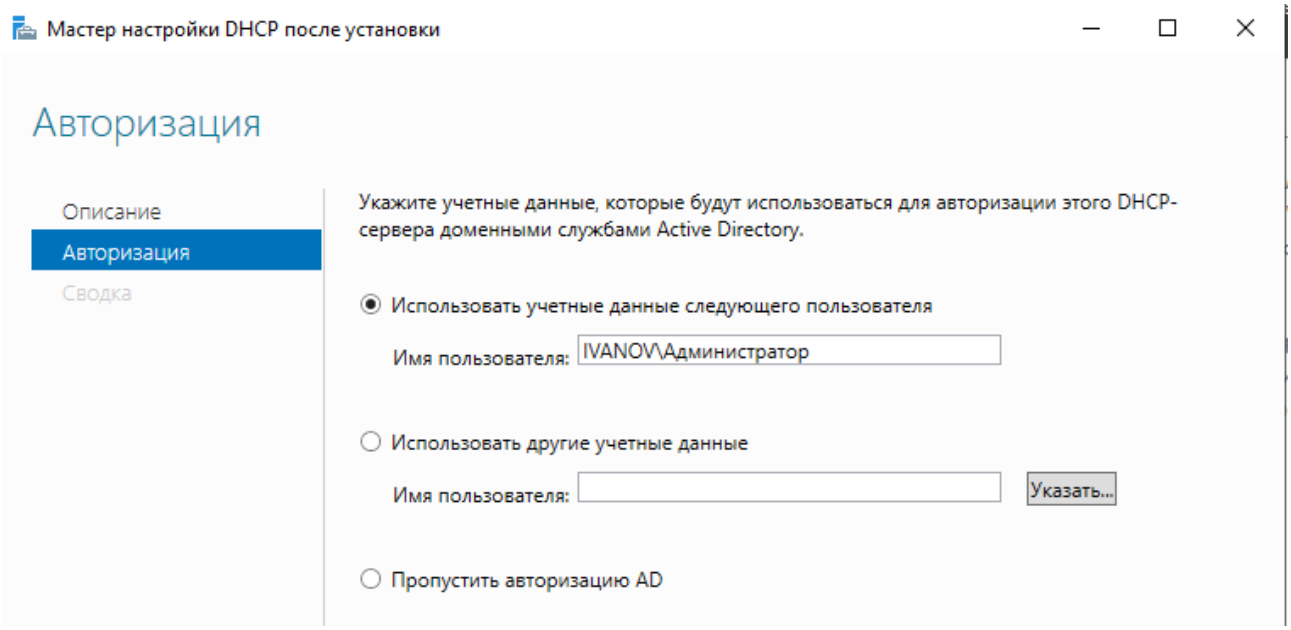


Рис. 3.22. Авторизація для налаштування DHCP-сервера після встановлення

Після остаточного встановлення і налаштування DHCP-сервера, створюємо нову DHCP-область. На рисунках нижче буде показано основні етапи встановлення та налаштування даної області. Всі інші скріншоти будуть показані в додатку Д.

Для початку вводимо початковий та кінцевий IP-адрес мережі, префікс та маску підмережі.

Потім зарезервовуємо IP-адреси, які будуть виключені з обсягу. Дані IP-адреси не будуть присвоюватись робочим станціям. Це адреси починаючи з 1 по 32. Далі налаштовуємо діапазон IP-адрес, котрі будуть присвоюватись робочим станціям. В даному випадку це адреси з 33 по 132.

Після введення всіх даних маємо готовий і налаштований DHCP-сервер, у якого готова та налаштована DHCP-область. На рисунку 3.23 вона показана, показано діапазон IP-адрес та IP-адреси, які не будуть видаватись.

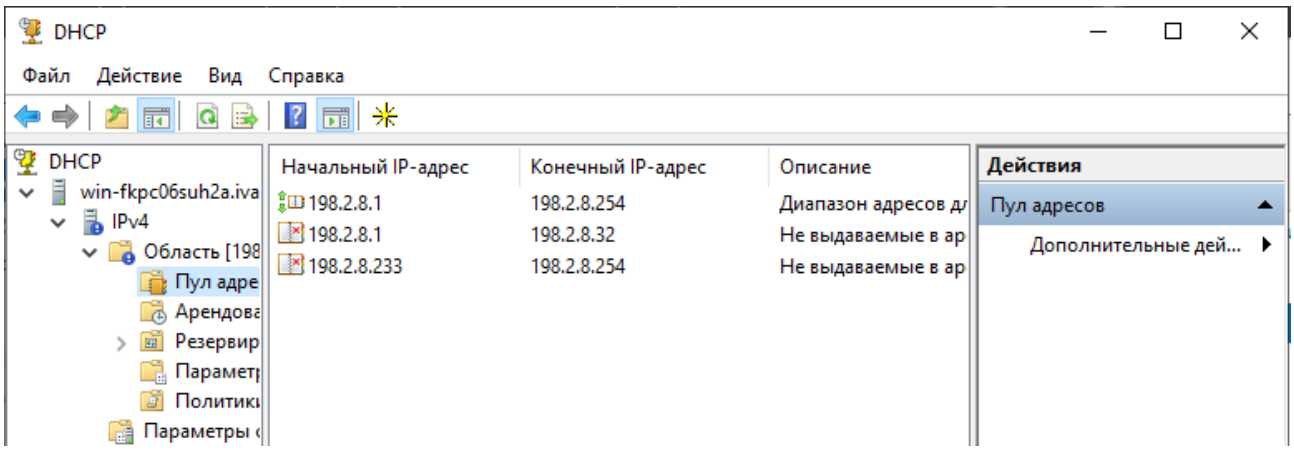


Рис. 3.23. Налаштована DHCP-область

Далі налаштовуємо розділення областей. Налаштовуємо, що головний сервер видає 75% IP-адрес, а альтернативний – 25%. У разі несправності головного сервера, все навантаження на себе приймає альтернативний. Це допомагає у збереженні працездатності мережі. Всі скріншоти будуть показані в додатку Е.

Далі налаштовуємо управління друком. Для кожного факультету буде доступний власний принтер – це зроблено для того, аби зменшити навантаження на один принтер і пришвидшити друк. Більше скріншотів додання принтерів та налаштування буде в додатку Е.

Після додання та налаштування принтерів маємо три принтера для двох факультетів та викладачів – показано на рисунку 3.24.

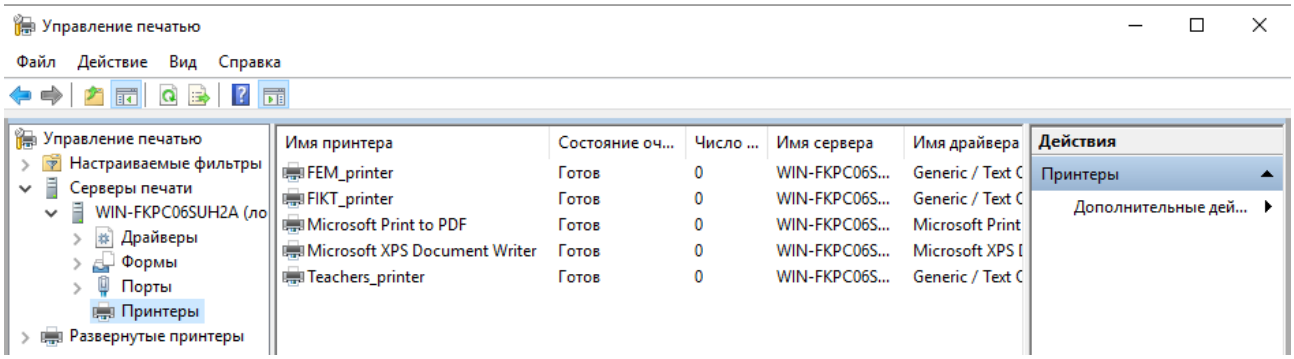


Рис. 3.24. Додані принтери

Далі налаштовуємо групові політики для цих принтері, щоб у студентів різних факультетів були свої принтери, а у викладачів свої. Більше скріншотів налаштування групових політик показано у додатку Е.

Зв’язуємо потрібний принтер зі потрібною групою користувачів. На рисунку 3.25 показано результат зв’язку. Після цього даний принтер буде доступний тільки для користувачів даного факультету. Скріншоти налаштування інших принтерів показано у додатку Е.

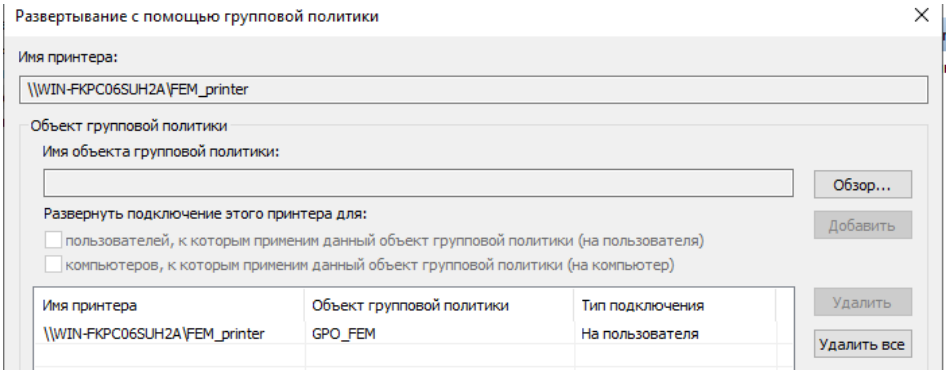


Рис. 3.25. Зв’язок принтера з потрібною групою користувачів

Далі налаштовуємо DNS-сервер. Більше скріншотів встановлення та налаштування DNS-сервера буде у додатку Є.

Спочатку налаштовуємо DNS на головному сервері. Під час налаштування потрібно вказати IP-адрес альтернативного сервера. Це потрібно для того, аби зменшити навантаження на головний сервер, та у разі несправності головного, щоб всі запити йшли на альтернативний. На рисунку 3.26 показано доданий DNS-адрес. Після налаштування головного сервера, потрібно налаштувати альтернативний.

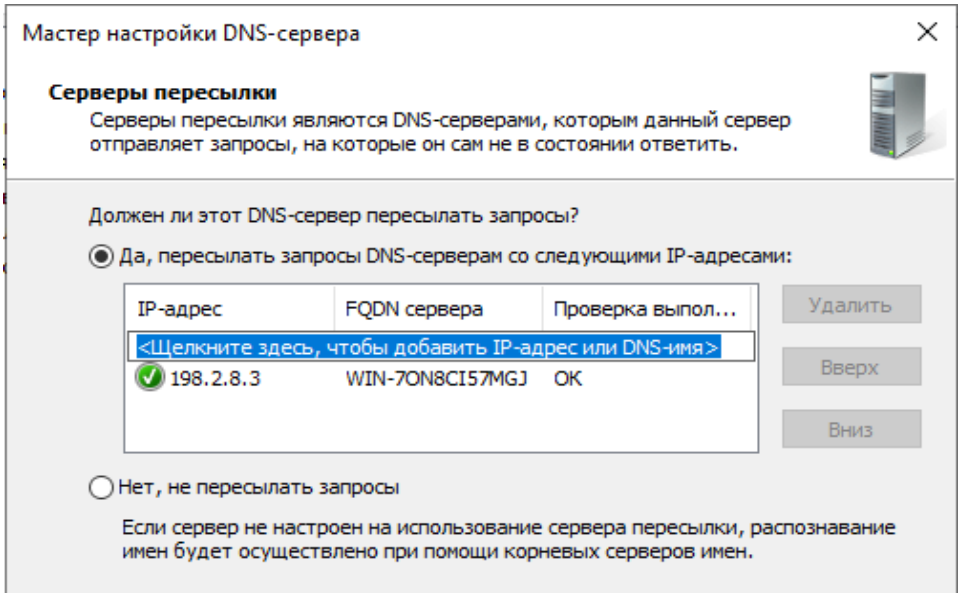


Рис. 3.26. Доданий DNS-адрес

Далі налаштовуємо віддалений доступ та віддалене управління на сервері. Для почакту встановлюємо нову роль на сервері «Служба віддалених робочих столів». Скріншоти встановлення будуть у додатку Ж.

Після встановлення надамо налаштуємо віддалений доступ. Для цьогоо потрібно налаштувати ліцензування. На рисунку 3.27 показана налаштування локальої групової політики для сервера.

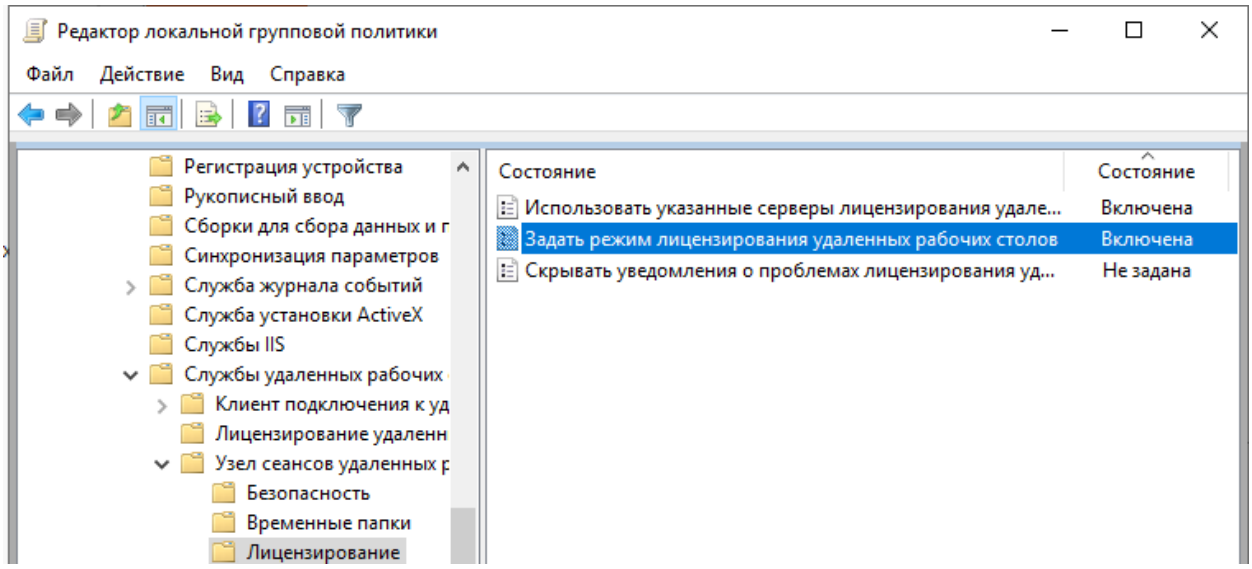


Рис. 3.27. Налаштування локальної групової політики

Далі активовуємо сервер. Це виконується за допомогою майстра активації. Більше скріншотів показано у додатку Ж.

Після активації сервера потрібно активувати ліцензію. Це також виконується за допомогою майстра активації. Більше скріншотів показано у додатку D. Після активації сервера та ліцензії, маємо готовий і працездатний сервер – як показано на рисунку 3.28.

Після встановлення та налаштування всього, надамо викладачам можливість використовувати віддлений доступ. Це буде виконано за допомогою членства у групах. Групі викладачів надамо членство у групах «Администратори» та «Користувачі віддаленого робочого столу». Після цього, у викладача буде можливість підключатися до серверу та здійснювати налаштування, які йому потрібні. На рисунку 3.29 буде показано всі групи, до яких належить об’єкт групової політики викладачів.

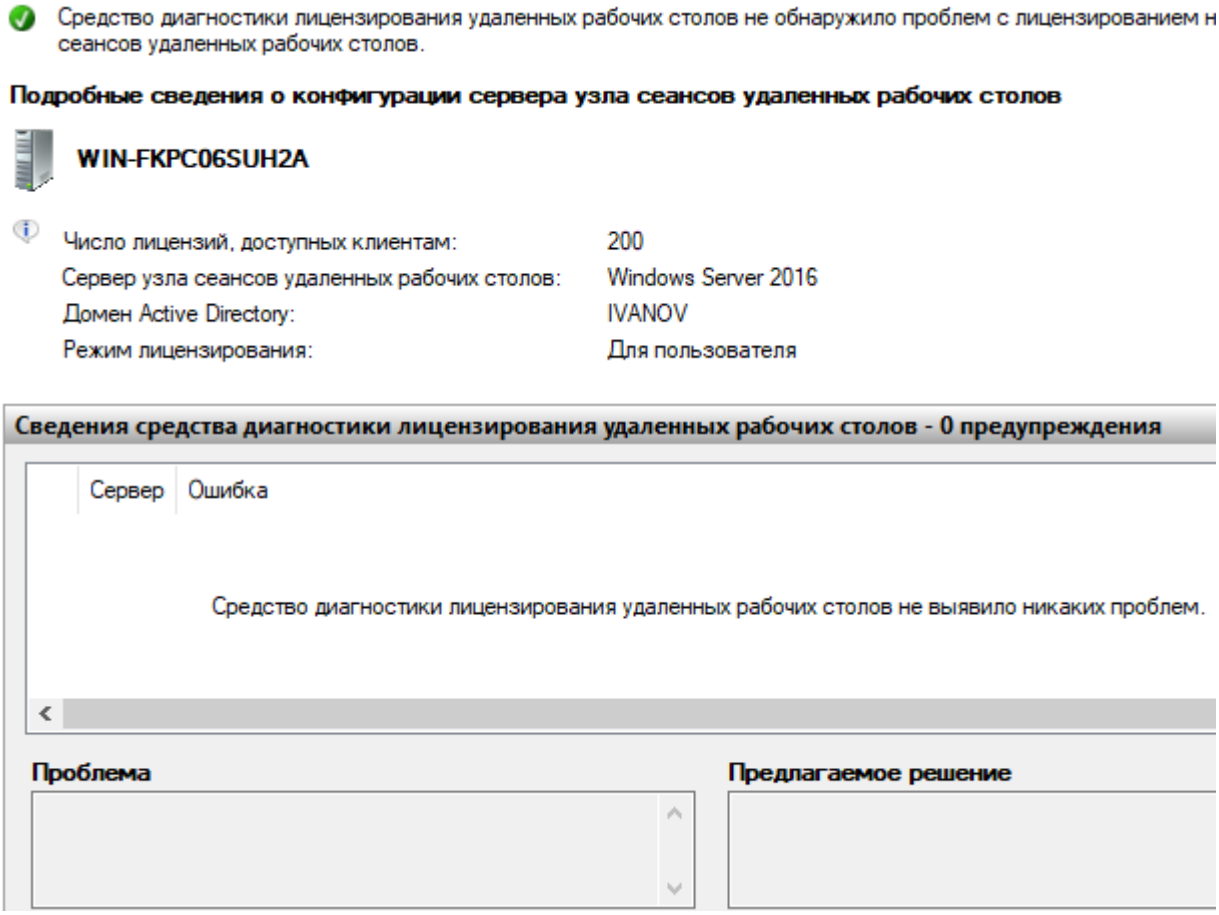


Рис. 3.28. Налаштований сервер та ліцензія

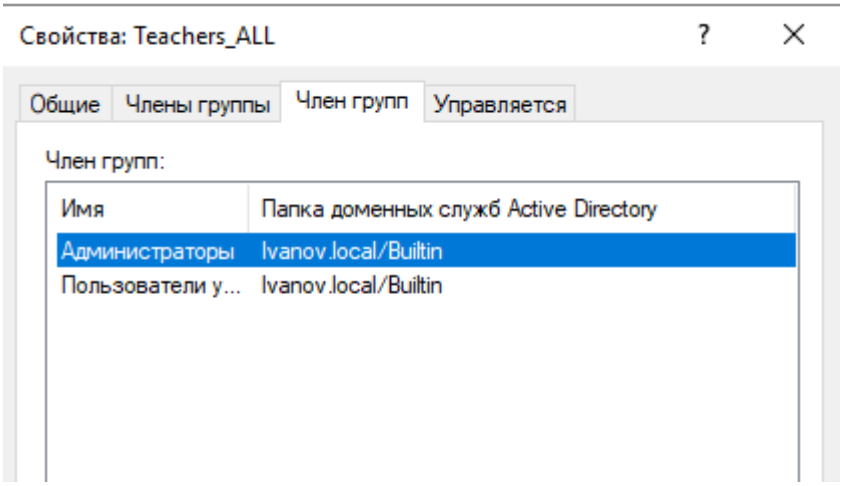


Рис. 3.29. Членство у групах

Далі налаштовуємо архівацію. Це потрібно для того, аби у раз втрати даних на сервері, була можливість відновити всі дані і роботу сервера. Результати налаштування резервної копії показано на рисунку 3.30. Більше скріншотів показано у додатку З.

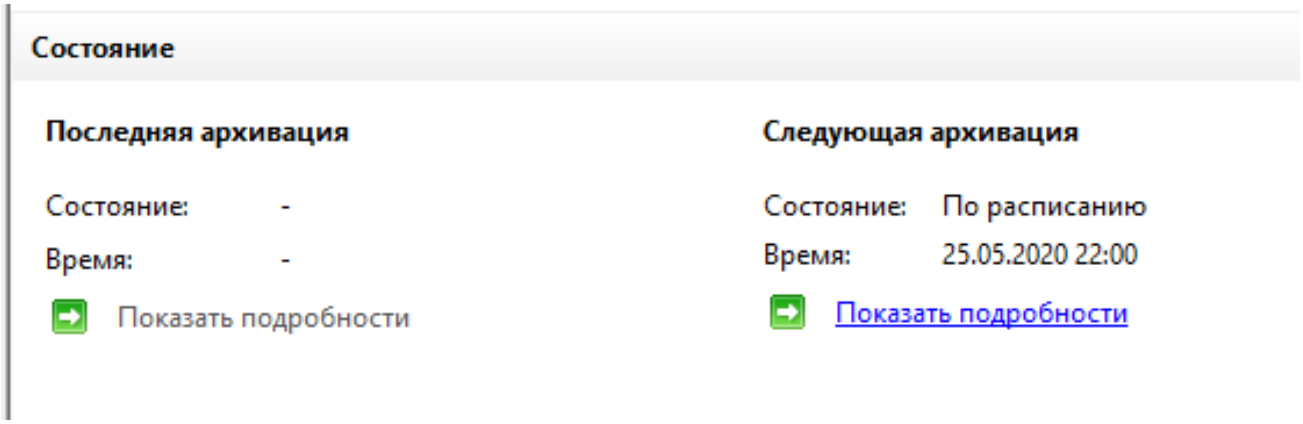


Рис. 3.30. Налаштована резервана копія

Далі розберемо як працює PowerShell. На рисунку 3.31 показаний синтакси скрипта, написаного за допомогою оболонки PowerShell. Даний скрипт був створений для створення резервної копії мережевої папки «ZSTU». При запуску даного скрипта, спочатку в іншій мережевій папці створиться папка для резервної копії. Після цього даний скрипт почну створювати резервну копію. Якщо резервна копія створиться коректно, то в командний рядок виведеться повідомлення, що резервна копія створена коректно.

backup-script.ps1*

```
1   $policy = New-WBPolicy
2   $policy | Add-WBBareMetalRecovery
3   $files = New-WBFileSpec -fileSpec "C:\ZSTU"
4   Add-WBSystemState -policy $policy
5   Add-WBFileSpec -policy $policy -filespec $files
6   $backupTargetDir = ("\\{0}\Backup\{0}\{1:dd-MM-yyyy_hh-mm-ss}" -f $env:computername, (get-date))
7   mkdir $backupTargetDir | out-null
8   $backupLocation = New-WBBackupTarget -NetworkPath $backupTargetDir
9   Add-WBBackupTarget -policy $policy -target $backupLocation
10  Set-WBVssBackupOption -Policy $policy -VssFullBackup
11  Start-WBBackup -policy $policy
12  write-host "Backup Successfull"
13
14
```

Рис. 3.31. Синтаксис скрипта для створення резервної копії

Після всіх налаштувань, перевіримо чи все працює коректно.

3.3 Перевірка налаштувань Windows Server

Для початку підключимо робочі станції до домену. Більше скріншотів показано у додатку І. Після підключення робочої станції до домену має з’явитись повідомлення про успішне підключення до домену. На рисунку 3.32 показано це повідомлення.

Далі, після того як з’явилось дане повідомлення, потрібно просто перезавантажити робочу станції і ввести початкові дані для входу в обліковий запис – логін та пароль.

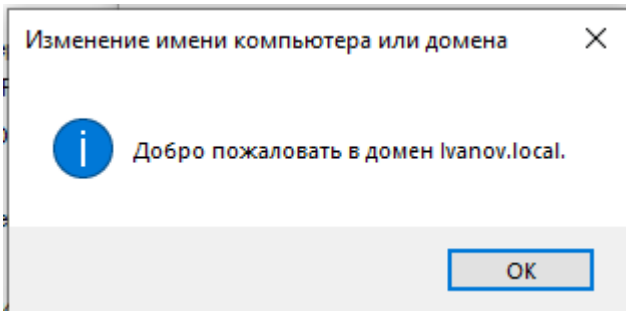


Рис. 3.32. Повідослення про вхід в домен

Після цього перевіряємо структура університету. Спробуємо логінитись під різними обліковими записами. І перевіряємо які підкаталоги доступні в каталозі «ZSTU». Для початку залогінимось під обліковим записом користувача з факультету ФІКТ. На рисунку 3.33 буде показано, що вхід у обліковий запис був успішний. Також користувачу буде доступна лише підкаталог «FIKT».

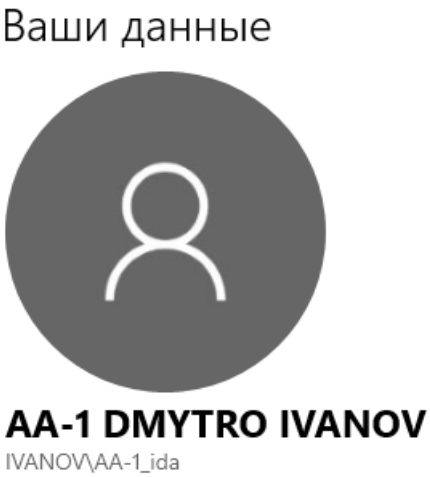


Рис. 3.33. Успішний вхід в обліковий запис

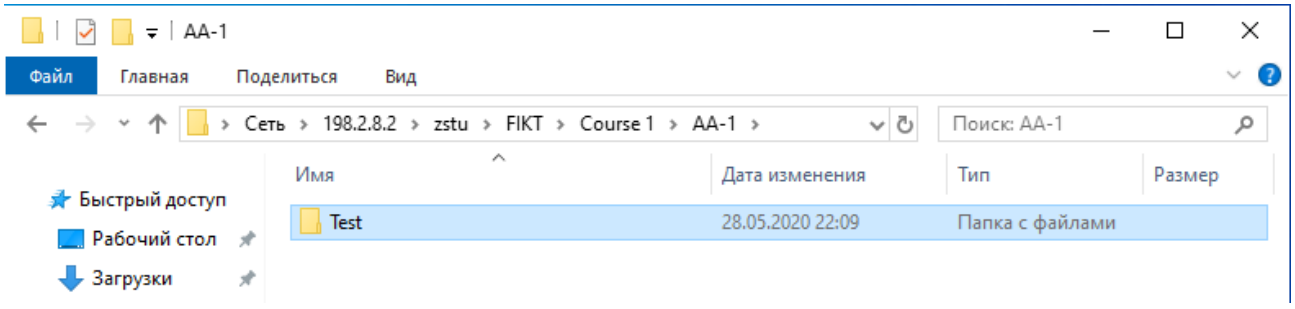


Рис. 3.34. Доступний підкаталог для даного користувача

Тепер увійдемо у обліковий запис студента із іншого факультету. Нижче будуть представлені скріншоти, що підтверджують це.

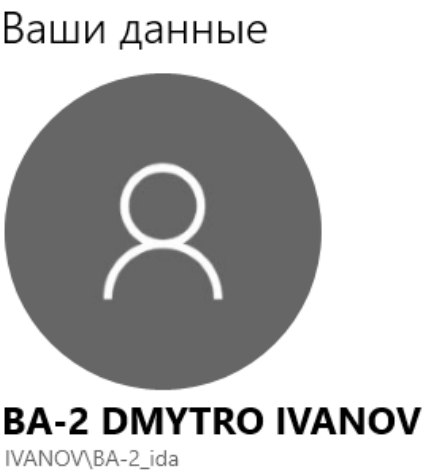


Рис. 3.35. Успішний вхід в інший обліковий запис

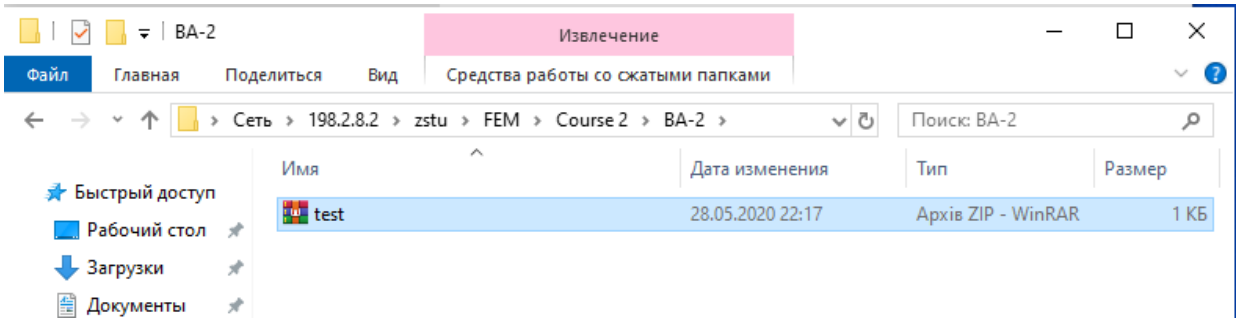


Рис. 3.36. Доступний підкаталог для даного користувача

Далі перевіряємо реплікацію мережевих папок. Після того, як щось було змінено у мережевій папці головного сервера, ці зміни мають синхронізуватися між папками. Це діє і у зворотньому напрямку. На рисунку 3.37 додаємо у мережеву папку альтернативного сервера архів, і перевіряємо реплікацію мережевих папок. Результат показано на рисунку 3.38.

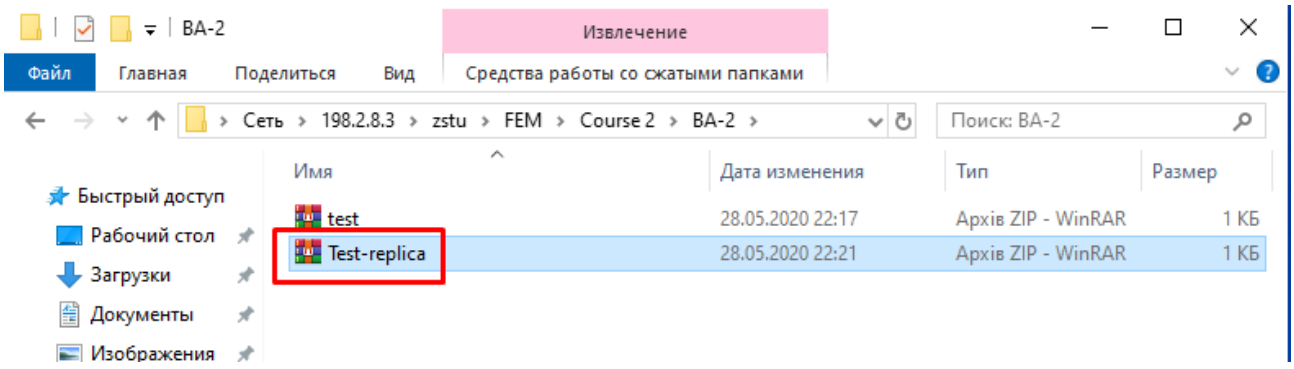


Рис. 3.37. Створення файлу для тестування реплікації

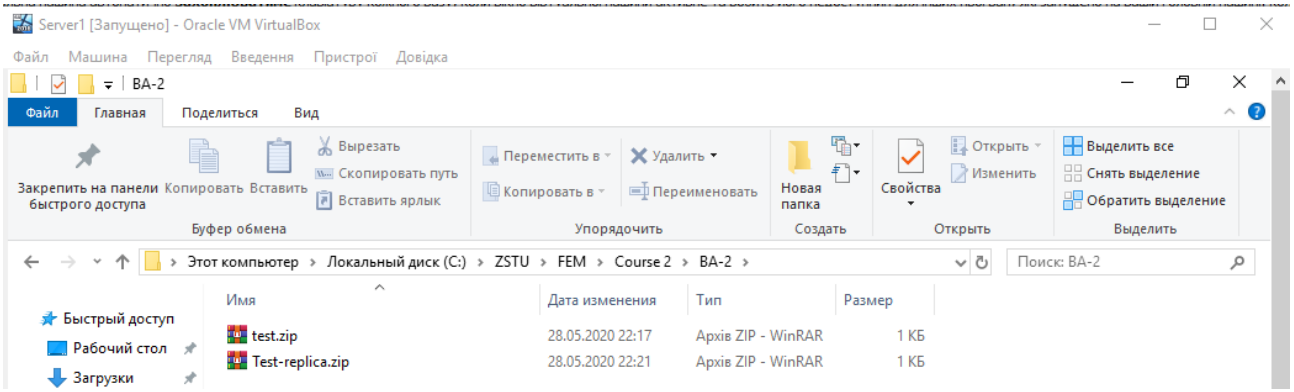


Рис. 3.38. Створений файл на головному сервері

Далі перевіряємо, чи коректно працюють групові політики. Це легко перевірити, увійшовши у обліковий запис студента факультету ФЕМ. Для студентів даного факультету видалено та заборонено доступ до команд «Заверешення роботи», «Перезавантаження». На рисунку 3.39 буде показано, що доступу до цих команд у них немає.



Рис. 3.39. Перевірка роботи групових політик

Також, перевіримо чи встановилось ПЗ через групові політики. На рисунку 3.40 показане встановлене ПЗ за допомогою групових політит. Також раніше було показано, що архіватор «WinRAR» був успішно встановлений.



Рис. 3.40. Встановлене ПЗ через групові політики

Далі перевіримо налаштування DHCP-сервера. При підлюченні робочої станції, їй має присвоюватись IP-адрес, починаючи з адреси 198.2.8.33. На рисунку 3.41 видно, що DHCP-сервер працює коректно.

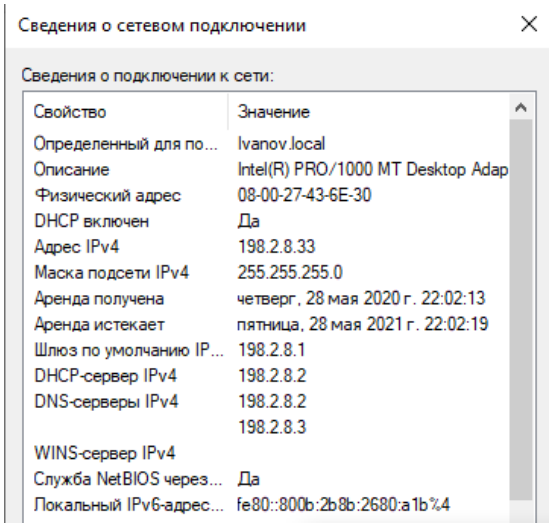


Рис. 3.41. Перевірка роботи DHCP-сервера

Далі перевіряємо, чи працюють налаштовані принтери. Для кожного факультету доступний свій принтер. Для викладачів також окремий принтер. Користувачу будуть показані всі принтери, але доступний буде лише один принтер – принтер його факультету. Якщо користувач захоче використати принтер не свого факультету, та з'явиться повідомлення про відмову у доступі. На рисунку 3.42 показане це повідомлення. На рисунку 3.43 показано, що для студента факультету ФІКТ доступний лише принтер його факультету принтер.

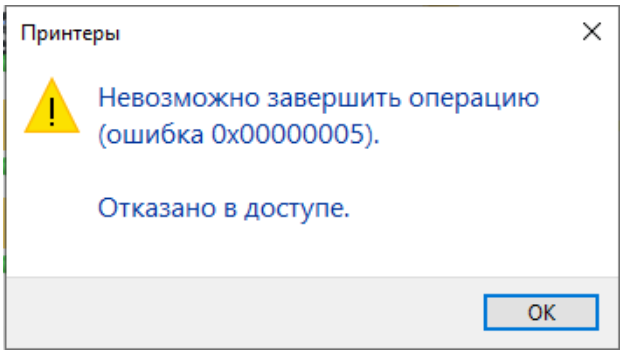


Рис. 3.42. Повідомлення про відмову в доступі

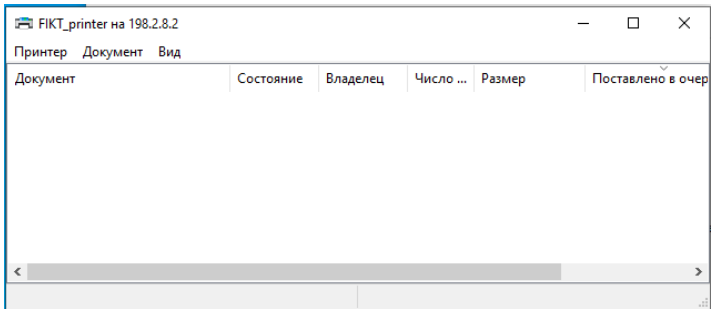


Рис. 3.43. Доступний принтер для факультету ФІКТ

Далі перевіряємо, чи коректно працює DNS. Якби у нас був лише один один сервер, і він перестав працювати – тоді б користувачі не могли б зайти у свої облікові записи. З'являлося б повідомлення, яке показано на риснку 3.44.

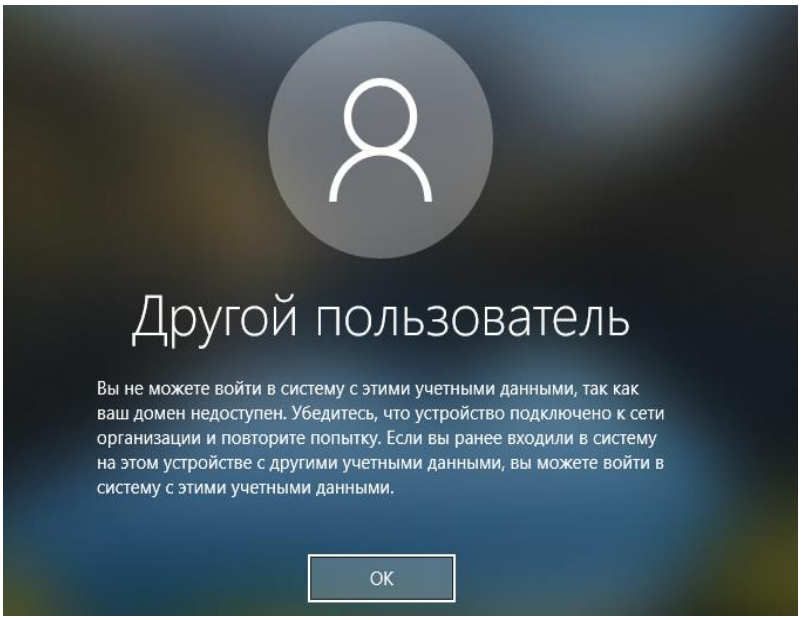


Рис. 3.44. Повідомлення про неможливість увійти

Проте в даному випадку це не проблема, так як є альтернативний, запасний, сервер. У разі припинення роботи головного сервера, альтернативний приймає все навантаження на себе. Відключимо головний сервер, і перевіримо, чи працює DNS. На рисунку 3.45 показано, що головний сервер відключений, а на рисунку 3.46 показано успішний вхід в обліковий запис.

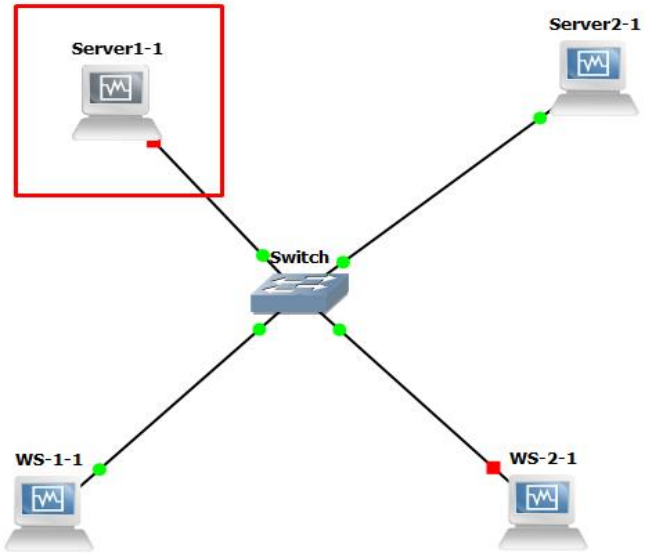


Рис. 3.45. Відключення головного сервера

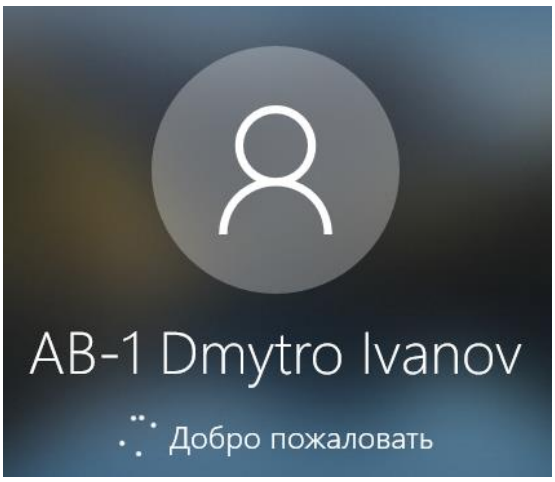


Рис. 3.46. Успішний вхід в обліковий запис

Далі перевіряємо, чи коректно працює створення резервної копії. Було налаштовано, що кожен день створюється резервна копія сервера. Час створення – о 22 кожного дня. Зберагіється резервна копія у мережу папку «Backup». На рисунку 3.47 показано, що резервні копії створюються і зберігаються.

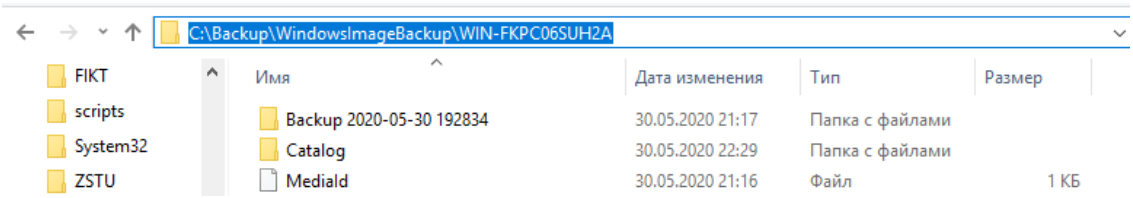


Рис. 3.47. Успішно створена резервна копія

Далі перевіряємо, чи коректно працює скрипт для створення резервної копії. На рисунку 3.48 показано процес виконання скрипта та його успішне заверешення. На рисунку 3.49 показано створену резервну копії за допомогою даного скрипта.

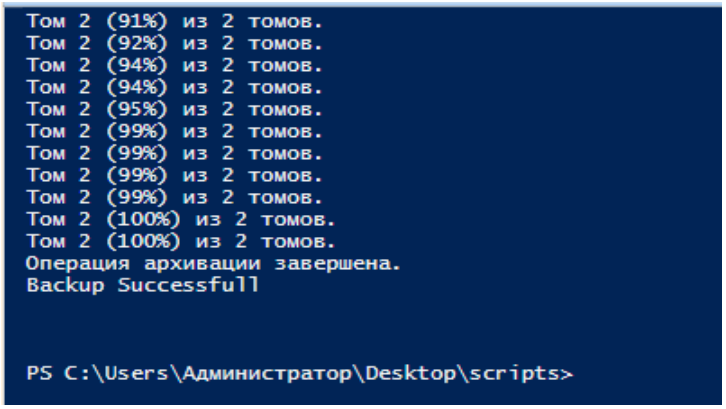


Рис. 3.48. Успішне виконання скрипта

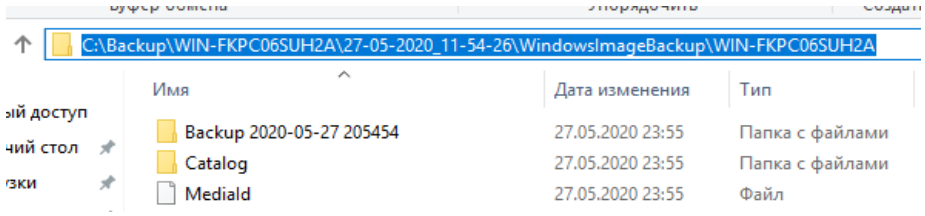


Рис. 3.49. Створена резервна копія

Далі перевіряємо, чи коректно працює віддалений доступ. Для цього потрібно увійти у обліковий запис викладача. Після цього, на робочій станції потрібно дозволити віддалене підключення. Далі вже можна віддалено підключатись до серверів.

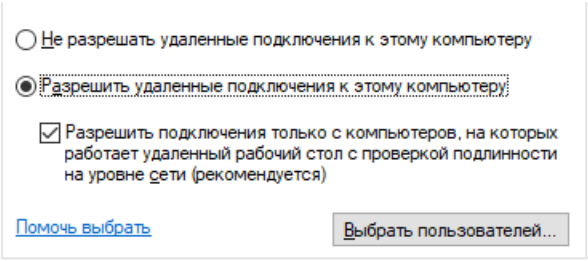


Рис. 3.50. Налаштування робочої станції

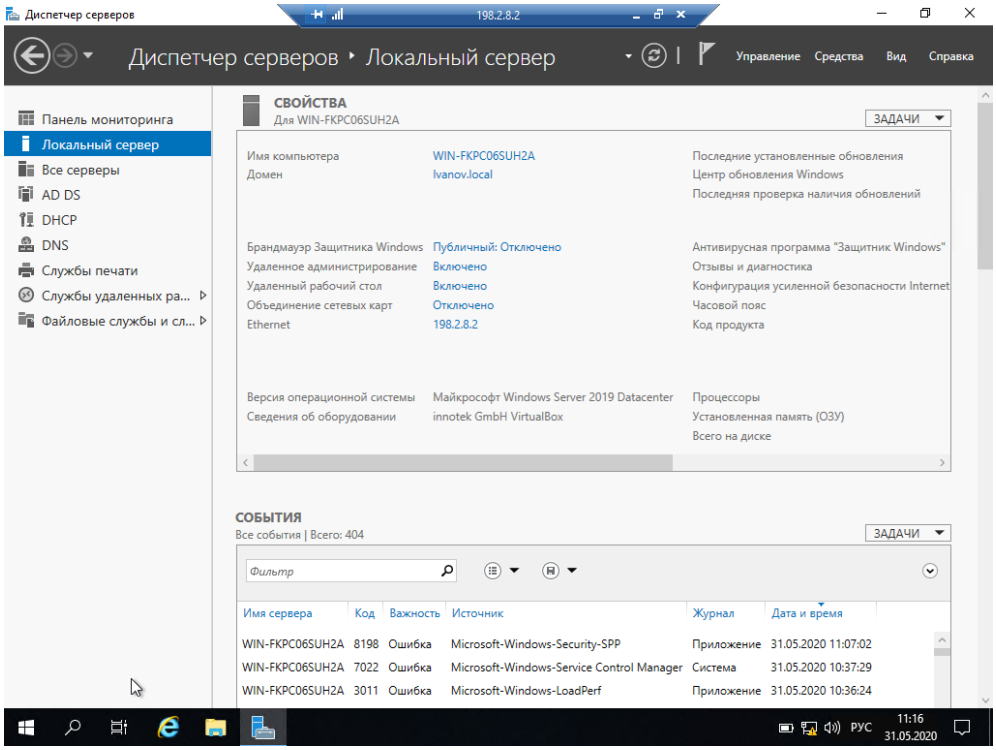


Рис. 3.51. Віддалене підключення до сервера

Як видно за рисунків, все що налаштовано у пункті 3.2 – працює. На рисунках пункта 3.3 все це було показано.

Висновки до третього розділу

В першому пункті даного розділу було налаштовано ПЗ для роботи. Було встановлено потрібні образи, додано їх в GNS3 та складено працюючу схему мережі університету «ZSTU».

В другому пункті даного розділу було налаштування Windows Server. Було налаштовано всі компоненти та ролі, котрі розглядались у третьому пункті першого розділу. Було детально розглянуто особливості та налаштування кожного з компонентів та ролей Windows Server.

В третьому пункті було протестовано налаштування всіх компонентів та ролей, які були налаштовані в попередньому пунктів. По результатам видно, що всі налаштування першого пункту працюють коректно.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було виконано та вирішено ряд наступних завдань:

1. Обґрунтовано актуальність даної теми.
2. Розглянуто теорію про всі потрібні засоби для створення мережної інфраструктури закладу вищої освіти на базі рішень Microsoft Windows.
3. Проаналізовано поставлене завдання та розділено його на задачі.
4. Спроектовано мережу університету.
5. Розроблено адресацію мережі.
6. Налаштовано ПЗ для роботи мережі.
7. Створено проект мережі університету.
8. Проведено налаштування кожного із серверів мережної інфраструктури закладу вищої освіти.
9. Протестовано налаштовану мережну інфраструктуру закладу вищої освіти.
10. Проаналізовано створену мережу.

Створена мережна інфраструктура закладу вищої освіти на базі рішень Microsoft Windows є готовою та працюючої мережею. Її можна використовувати, як шаблон для створення інших мережних інфраструктур закладу вищої освіти на базі рішень Microsoft Windows.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Администрирование школьных локальных сетей [Електронний ресурс] – Режим доступу до ресурсу: https://docplayer.ru/42541619-Dopolnitelnaya-professionalnaya-programma-povysheniya-kvalifikacii-administrirovanie-shkolnyh-lokalnyh-setey-v-geterogennyh-sredah.html.
2. Основы Active Directory Domain Services [Електронний ресурс] – Режим доступу до ресурсу: https://www.youtube.com/watch?v=hAyM1RCiCHM.
3. Обзор доменных служб Active Directory [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.
4. Active Directory [Електронний ресурс] – Режим доступу до ресурсу: https://www.dmosk.ru/terminus.php?object=ad.
5. Файловый сервер на базе Windows Server [Електронний ресурс] – Режим доступу до ресурсу: http://www.unitec.com.ua/fajlovyj-server-na-baze-windows-server-2016/.
6. Файловый сервер [Електронний ресурс] – Режим доступу до ресурсу: https://blog.it-kb.ru/2016/05/23/the-basic-techniques-for-working-with-file-server-on-windows-server/.
7. Active Directory User [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/topics/computer-science/active-directory-user.
8. Управление групповыми политиками Active Directory [Електронний ресурс] – Режим доступу до ресурсу: https://1cloud.ru/help/windows/gruppovye-politiki-active-directory.

9. Управление групповыми политиками в организации. Часть 1 [Електронний ресурс] – Режим доступу до ресурсу: http://www.oszone.net/11674/gpmc1.
10. DHCP Server [Електронний ресурс] – Режим доступу до ресурсу: https://www.heyvaldemar.net/ustanovka-i-nastroyka-dhcp-server-na-windows-server-2012-r2/.
11. Windows server 2019 - установка и настройка сервера печати [Електронний ресурс] – Режим доступу до ресурсу: https://bigro.ru/system/174-win2019srv-setup-print-mfu-gpo.html.
12. Установка ліцензії cal для windows server. Налаштування сервера ліцензій на серверах RD Session Host [Електронний ресурс] – Режим доступу до ресурсу: http://vilonta.ru/uk/bilajjn/ustanovka-licenzii-cal-dlya-windows-server-nastroika-servera-licenzii-na-serverah.html.
13. Служба удаленных рабочих столов [Електронний ресурс] – Режим доступу до ресурсу: https://www.stekspb.ru/blog/it/sluzhba-udalennyh-rabochih-stolov/.
14. Active Directory - от теории к практике [Електронний ресурс] – Режим доступу до ресурсу: https://interface31.ru/tech_it/2012/08/active-directory-ot-teorii-k-praktike-chast-3.html.
15. Установка при помощи групповых политик [Електронний ресурс] – Режим доступу до ресурсу: https://crocotime.com/ru/guide/installation-of-crocotime-client-applications/installation-using-gpo/.
16. Установка роли RDP на сервер Windows [Електронний ресурс] – Режим доступу до ресурсу: https://www.sim-networks.com/wiki/remote-desktop-protocol-setup-to-windows.
17. Active Directory - от теории к практике [Електронний ресурс] – Режим доступу до ресурсу: https://interface31.ru/tech_it/2012/08/active-directory-ot-teorii-k-praktike-chast-3.html.

18. Установка службы удаленных рабочих столов Windows Server [Електронний ресурс] – Режим доступу до ресурсу: https://topnet.com.ua/ustanovka-sluzhby-udalennyx-rabochix-stolov-windows-server/.
19. Общий доступ к сетевым папкам и принтерам [Електронний ресурс] – Режим доступу до ресурсу: https://winitpro.ru/index.php/2018/06/21/obshchij-dostup-k-setevym-papkam-i-printeram-bez-homegroup/.
20. Установка DNS и Active Directory [Електронний ресурс] – Режим доступу до ресурсу: https://bigro.ru/system/142-setup-active-directory-2016.html.
21. Автоматизируем процесс создания бекапов серверных систем Windows Server [Електронний ресурс] – Режим доступу до ресурсу: http://jakondo.ru/avtomatiziruem-protsess-sozdaniya-bekapov-servernyh-sistem-windows-server-2008-r2-2012-r2-s-pomoshhyu-skripta-dlya-powershell/.
22. Настройка резервного копирования сервера с помощью компоненты Windows Backup [Електронний ресурс] – Режим доступу до ресурсу: https://hd.oblakoteka.ru/kb/a17/windows-backup-2012-r2.aspx.
23. Windows Server 2016 — настройка Windows Server Backup [Електронний ресурс] – Режим доступу до ресурсу: https://internet-lab.ru/windows_server_2016_backup.
24. Create a Scheduled Task with unlimited Execution Time Limit in PowerShell [Електронний ресурс] – Режим доступу до ресурсу: https://dscottraynsford.wordpress.com/category/windows-server-2016/.
25. Useful PowerShell Scripts/Commands [Електронний ресурс] – Режим доступу до ресурсу: http://microsoftgeek.com/?p=2759.

26. WindowsServerBackup [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/powershell/module/windowsserverbackup/?view=win10-ps.
27. Windows PowerShell - Написание Windows-служб в PowerShell [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/archive/msdn-magazine/2016/may/windows-powershell-writing-windows-services-in-powershell.
28. Write a Windows Service in PowerShell [Електронний ресурс] – Режим доступу до ресурсу: https://www.sapien.com/blog/2017/07/12/write-a-windows-service-in-powershell/.
29. Create a windows service using PowerShell [Електронний ресурс] – Режим доступу до ресурсу: https://www.yaplex.com/blog/create-a-windows-service-using-powershell/.
30. How to run a PowerShell script as a Windows service [Електронний ресурс] – Режим доступу до ресурсу: https://4sysops.com/archives/how-to-run-a-powershell-script-as-a-windows-service/.

ДОДАТКИ

ДОДАТОК А

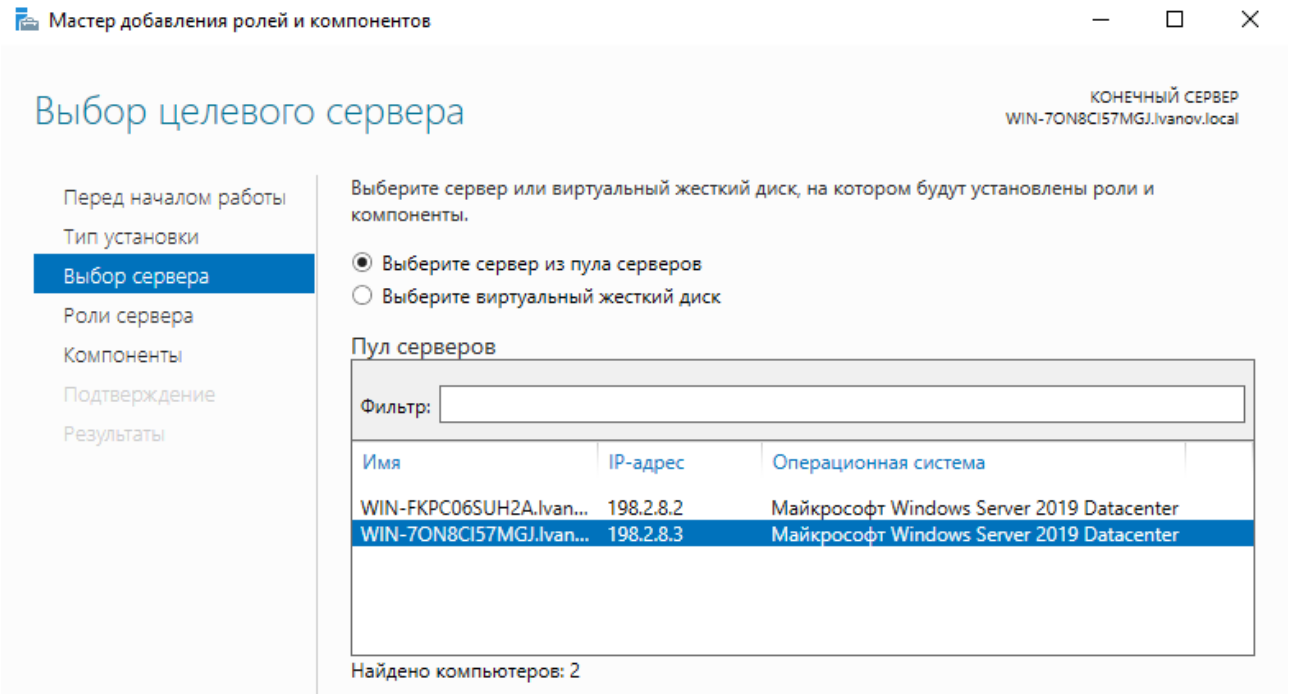


Рис. А.1. Вибір сервера

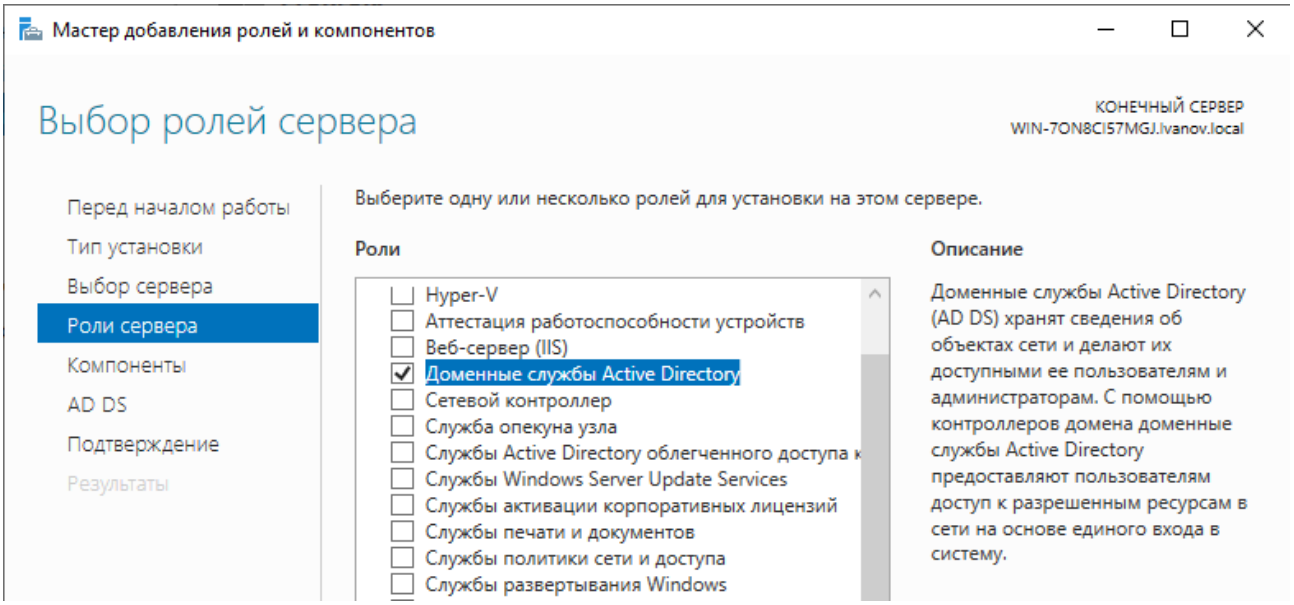


Рис. А.2. Вибір ролі сервера

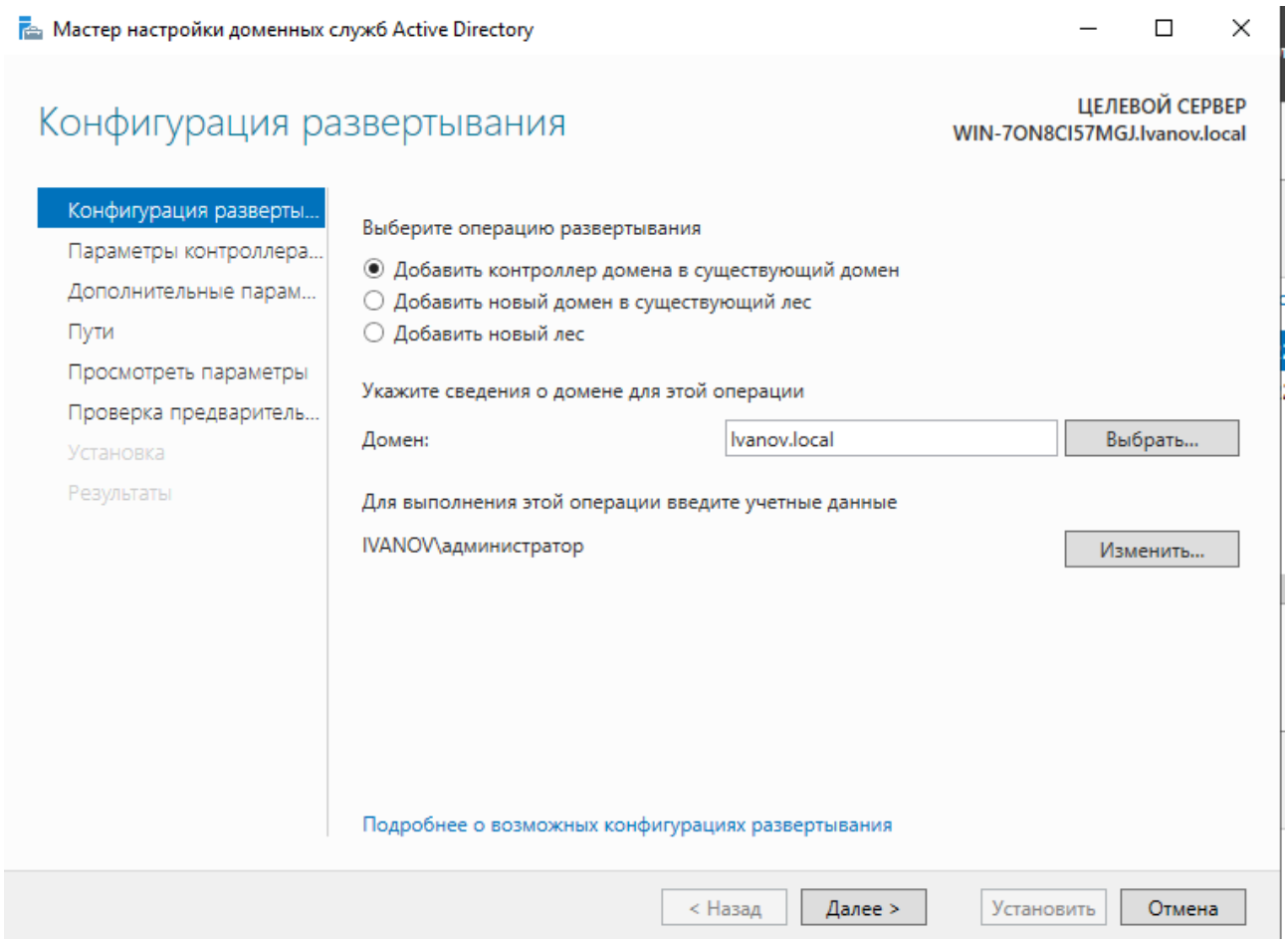


Рис. А.3. Додання нового сервера в існуючий домен

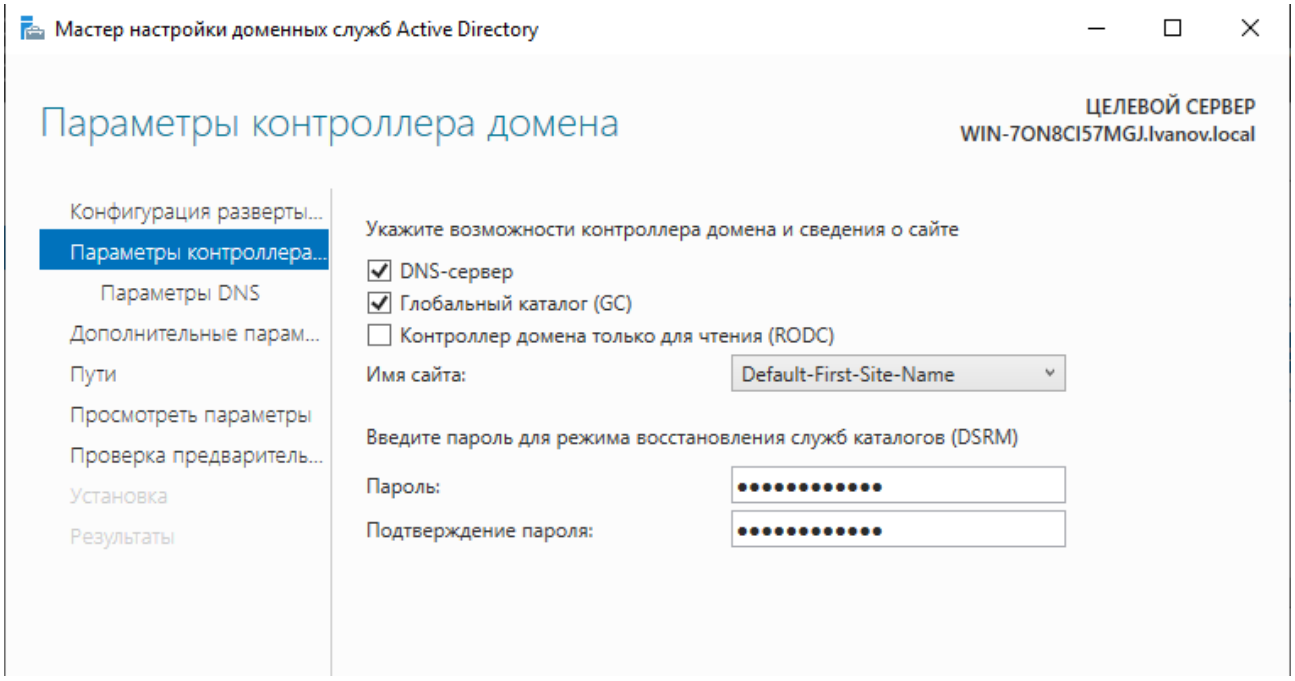


Рис. А.4. Налаштування сервера

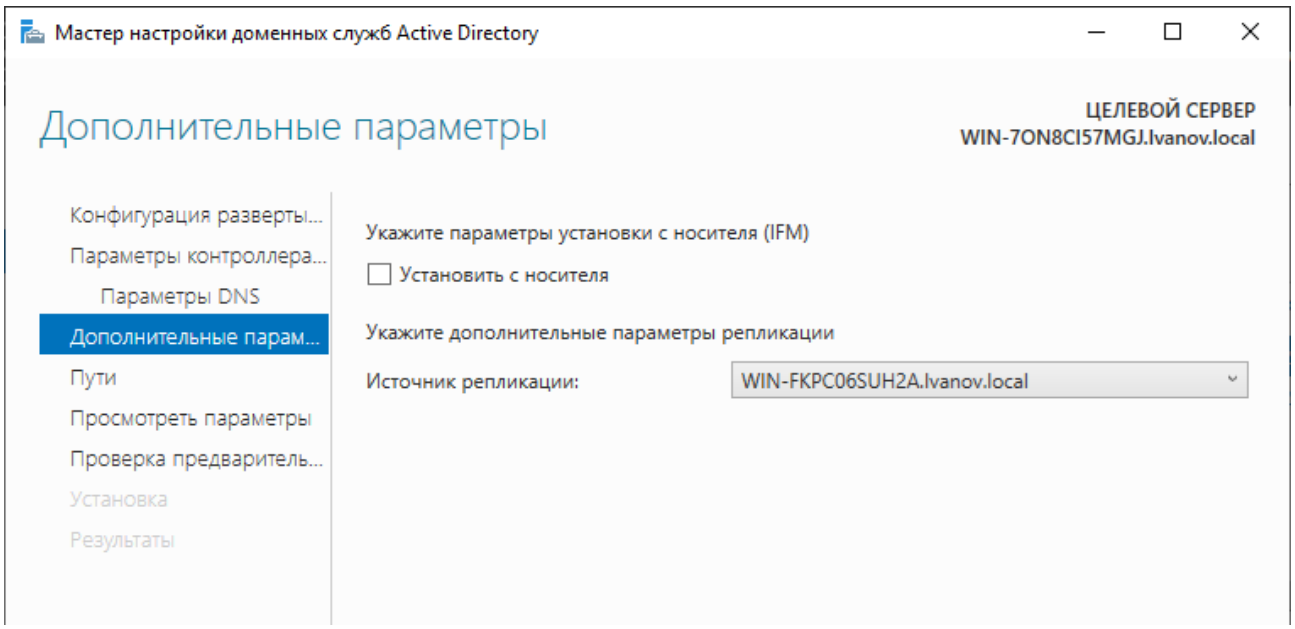


Рис. А.5. Налаштування сервера

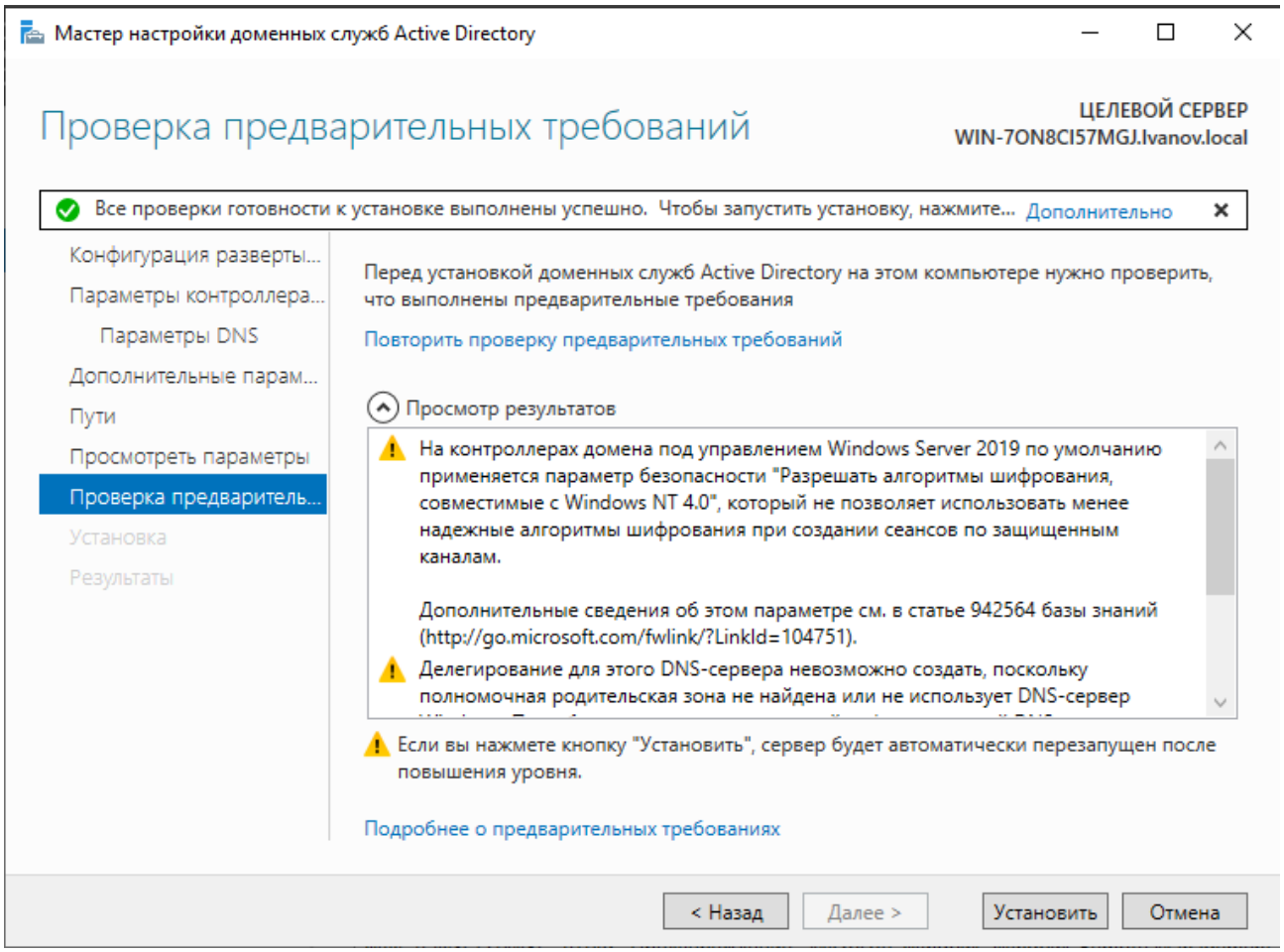


Рис. А.6. Перевірка вимог

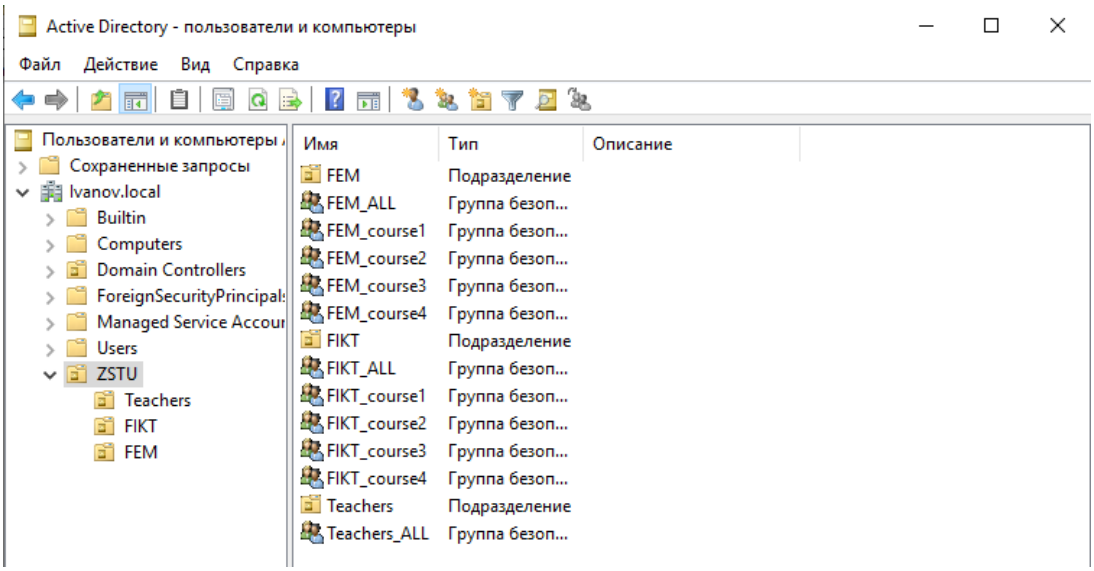


Рис. Б.1. Створені групи користувачів

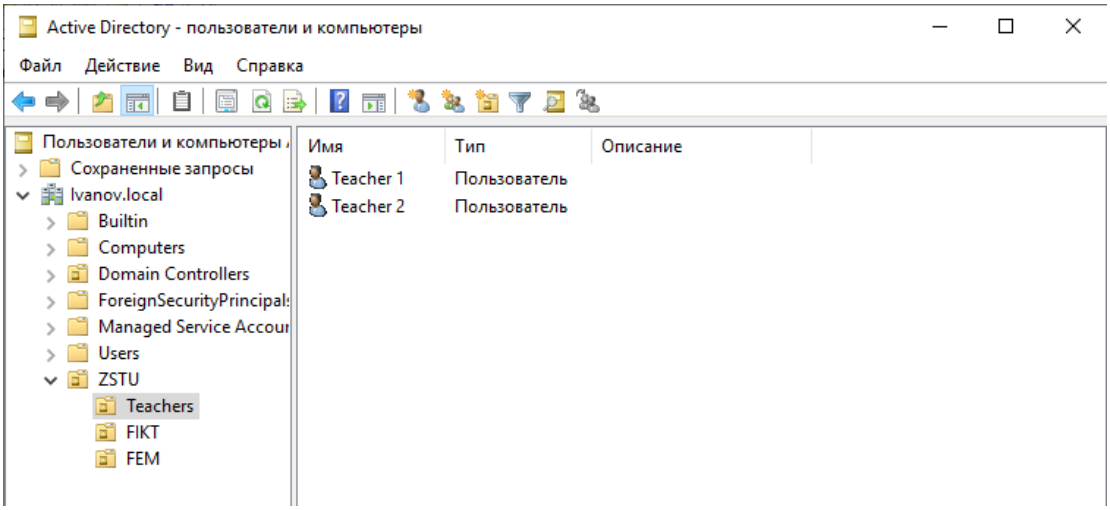


Рис. Б.2. Створені користувачі

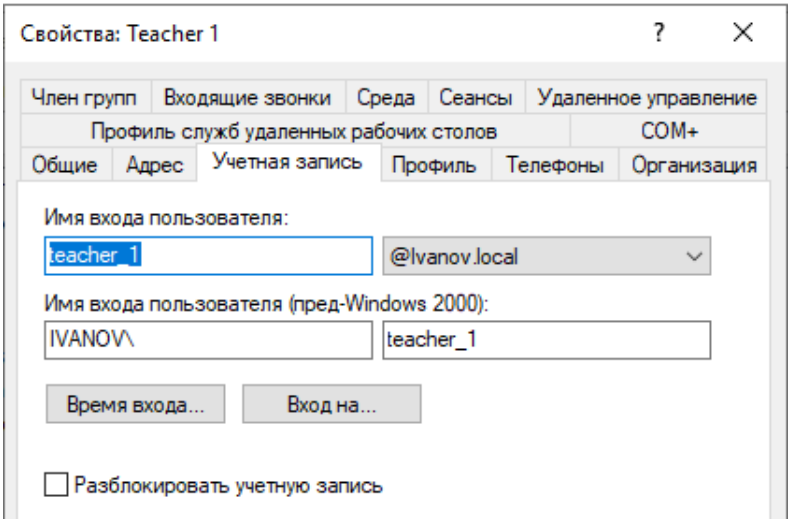


Рис. Б.3. Властивості користувача «Teacher»

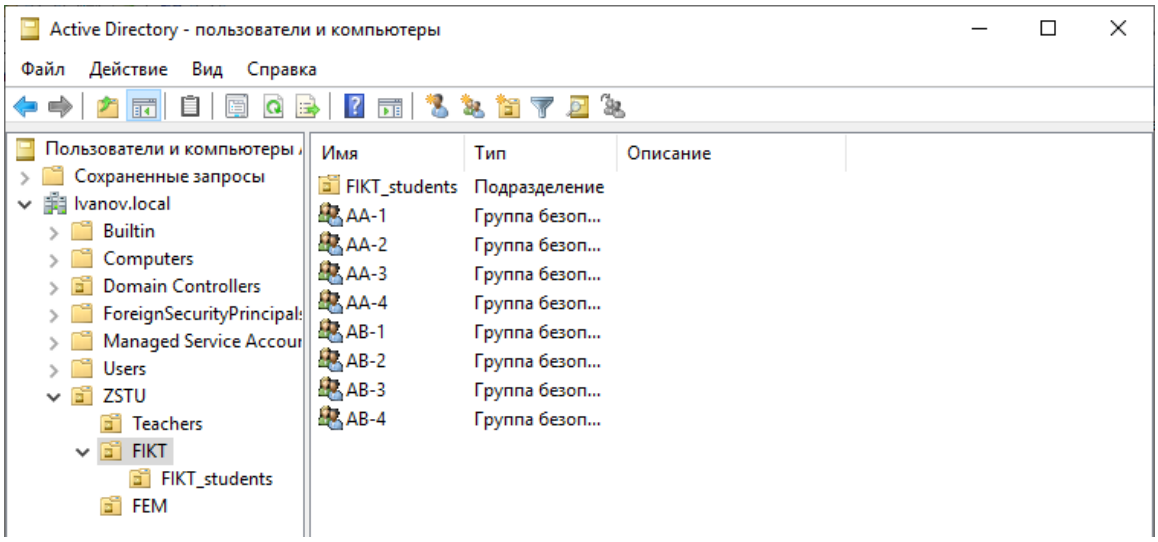


Рис. Б.4. Створені групи користувачів

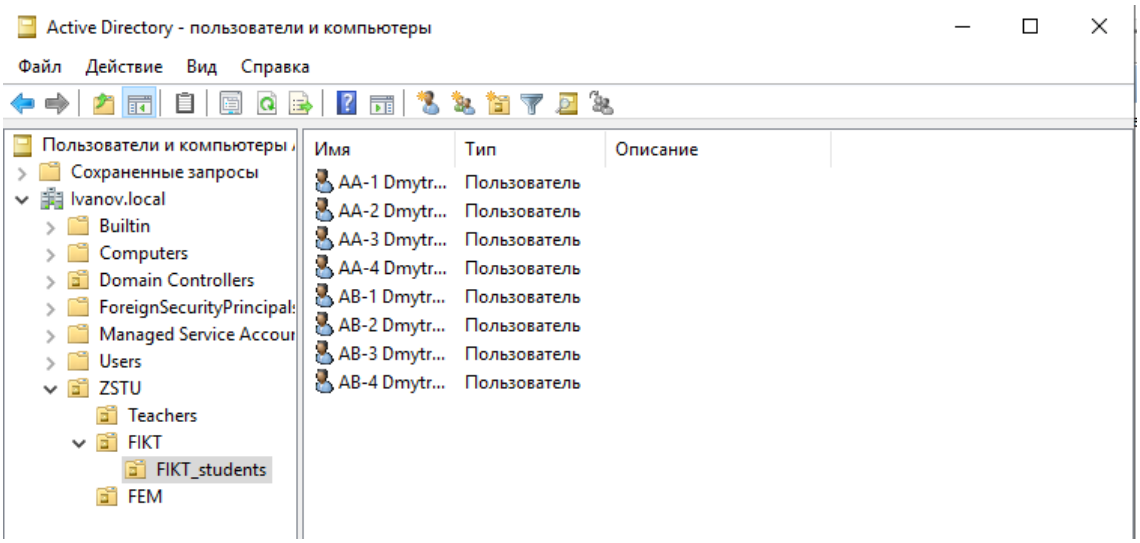


Рис. Б.5. Створені користувачі

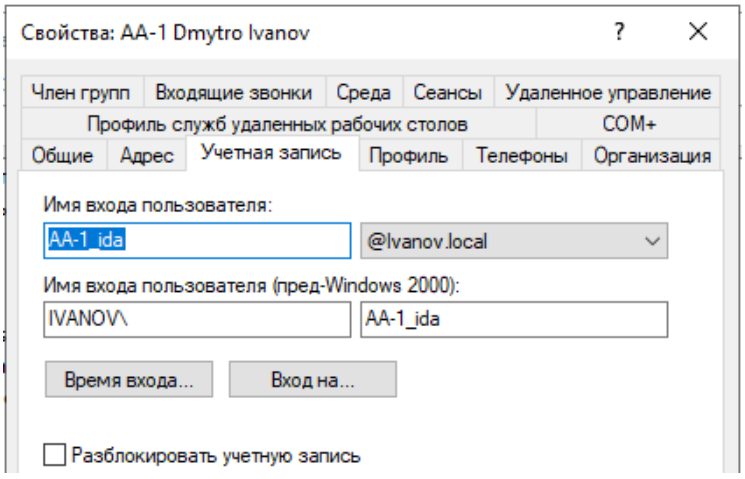


Рис. Б.6. Властивості користувача факультету «FIKT»

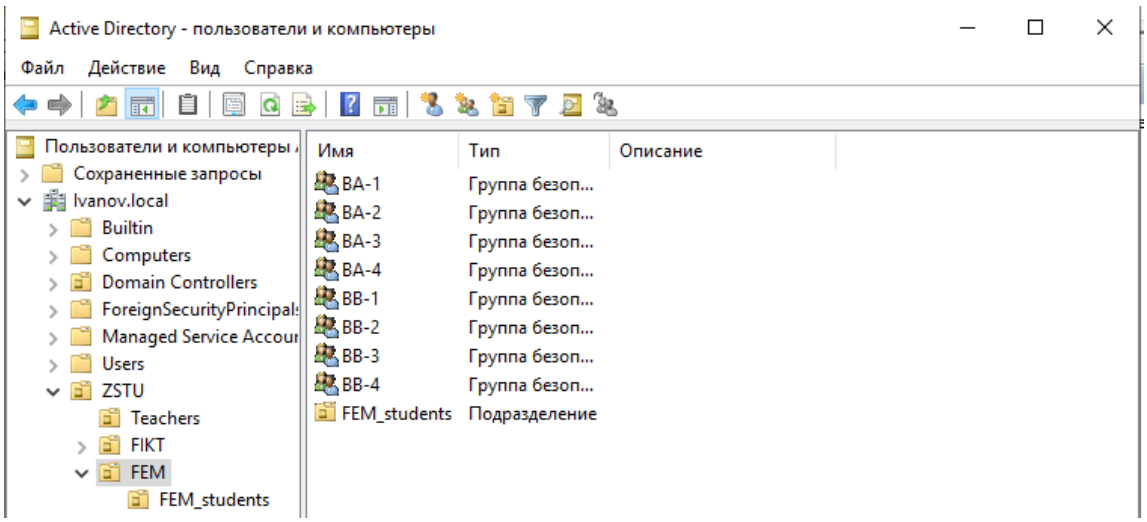


Рис. Б.7. Створені групи користувачів

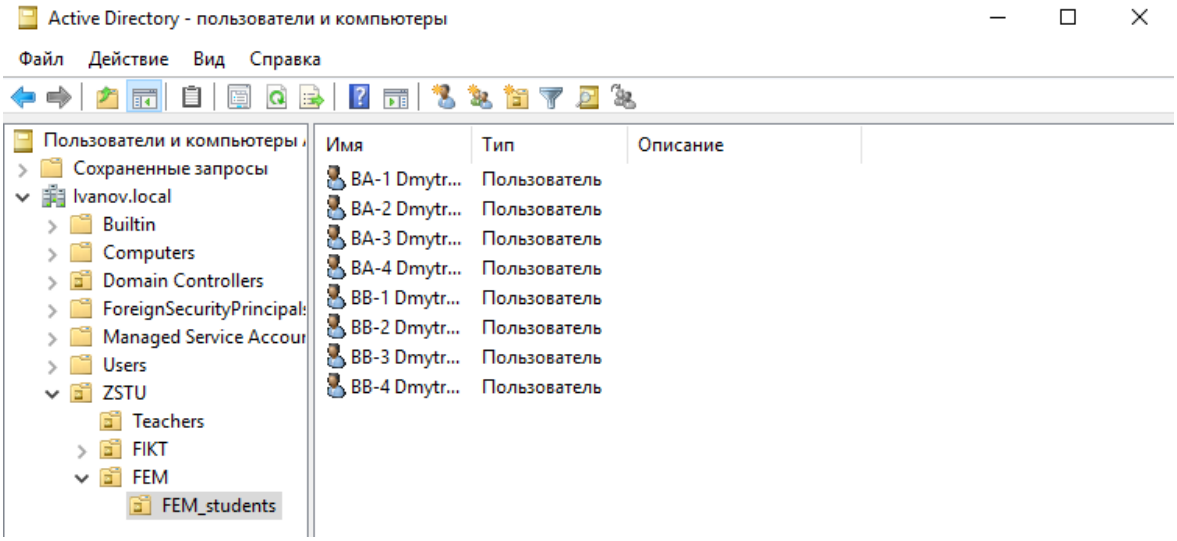


Рис. Б.8. Створені користувачі

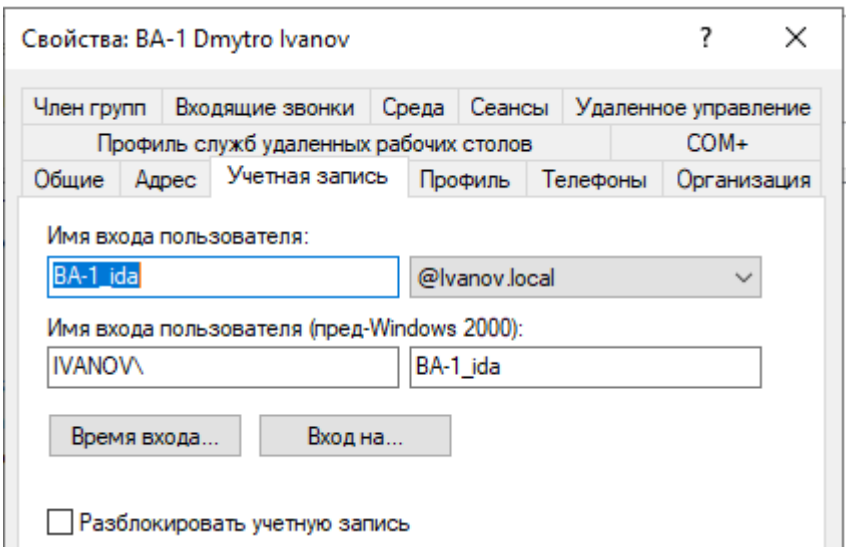


Рис. Б.9. Властивості користувача факультету «FEM»

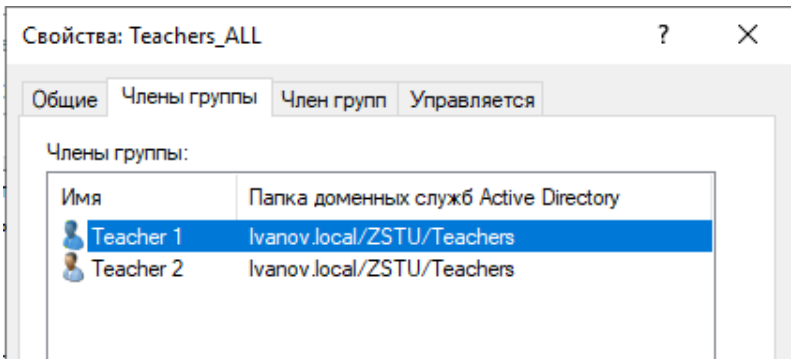


Рис. Б.10. Члени групи

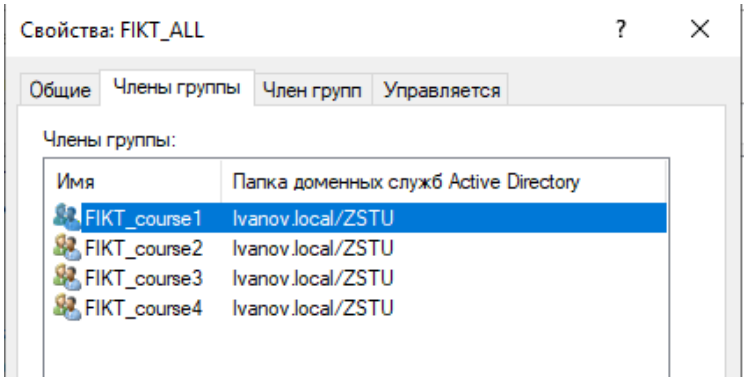


Рис. Б.11. Члени групи

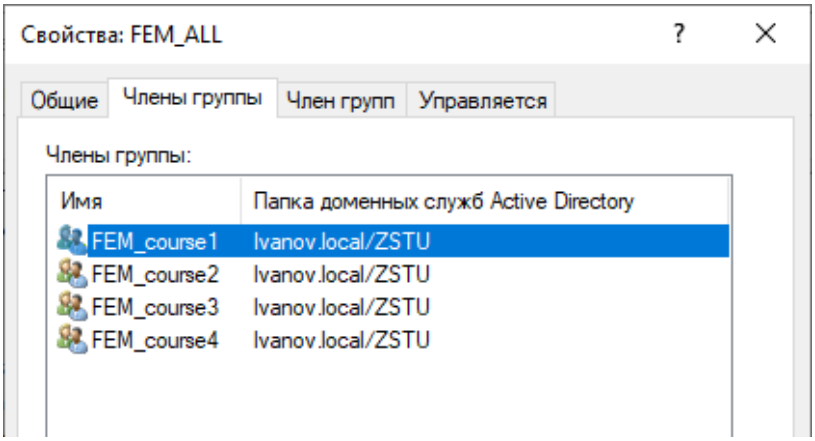


Рис. Б.12. Члени групи

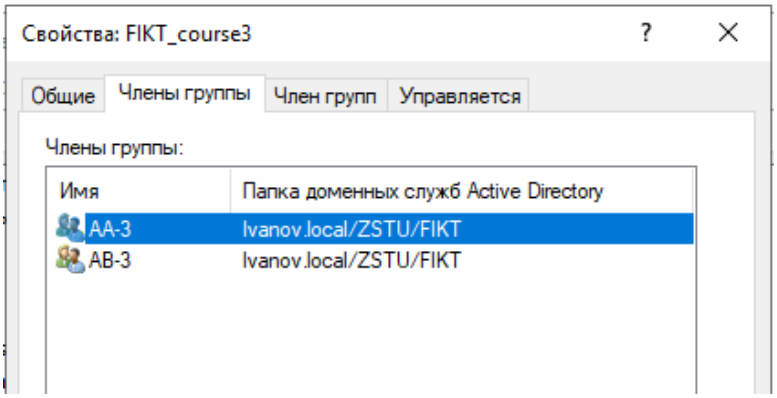


Рис. Б.13. Члени групи

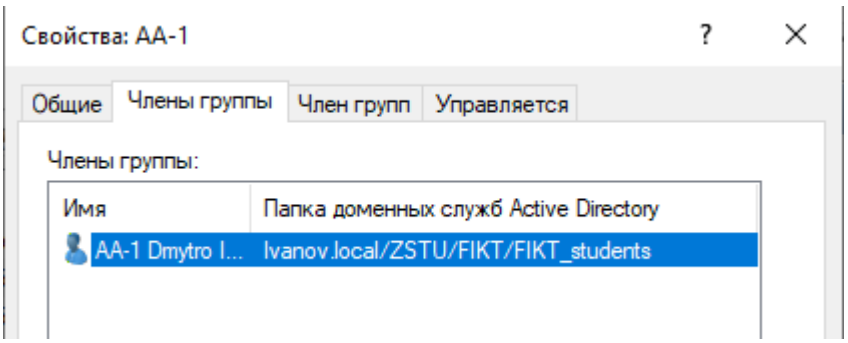


Рис. Б.14. Члени групи

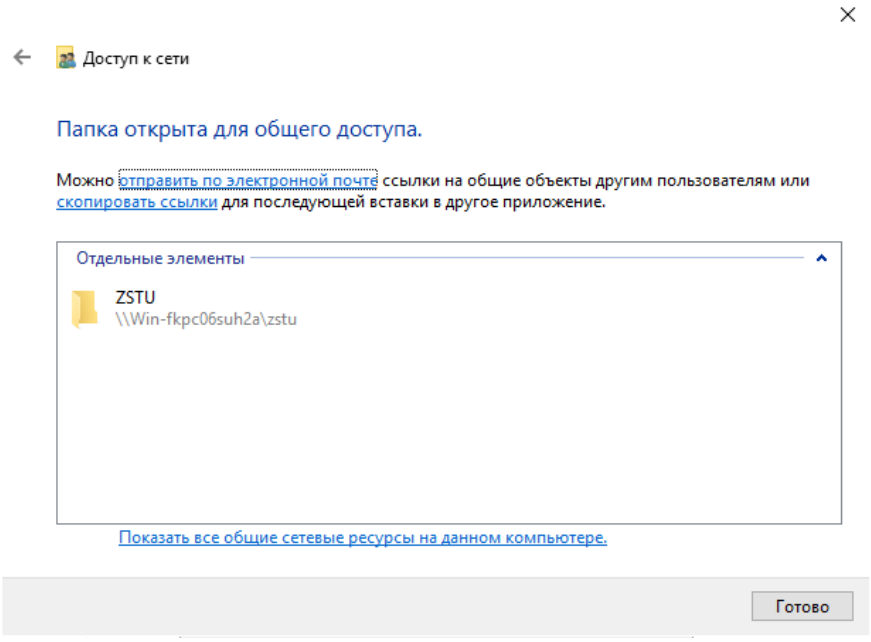


Рис. Б.15. Відкриття доступа до папки

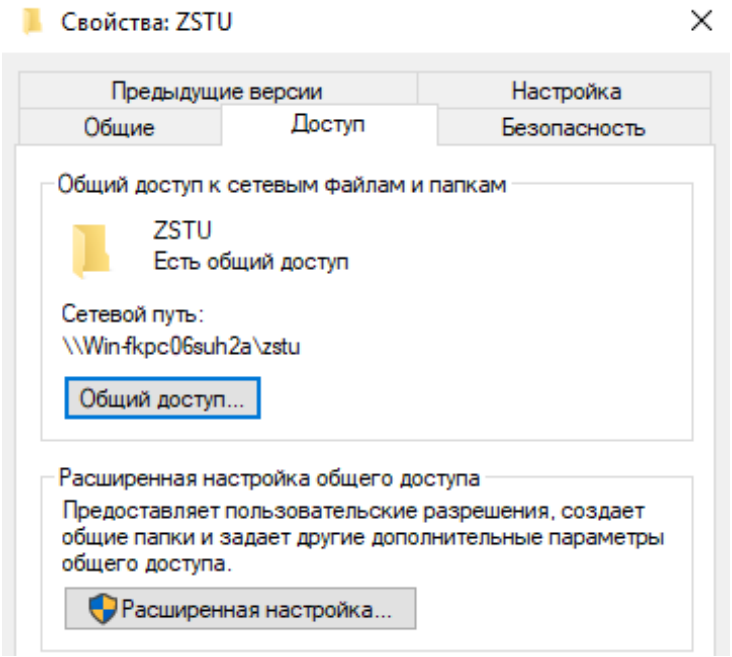


Рис. Б.16. Відкритий доступ

ДОДАТОК В

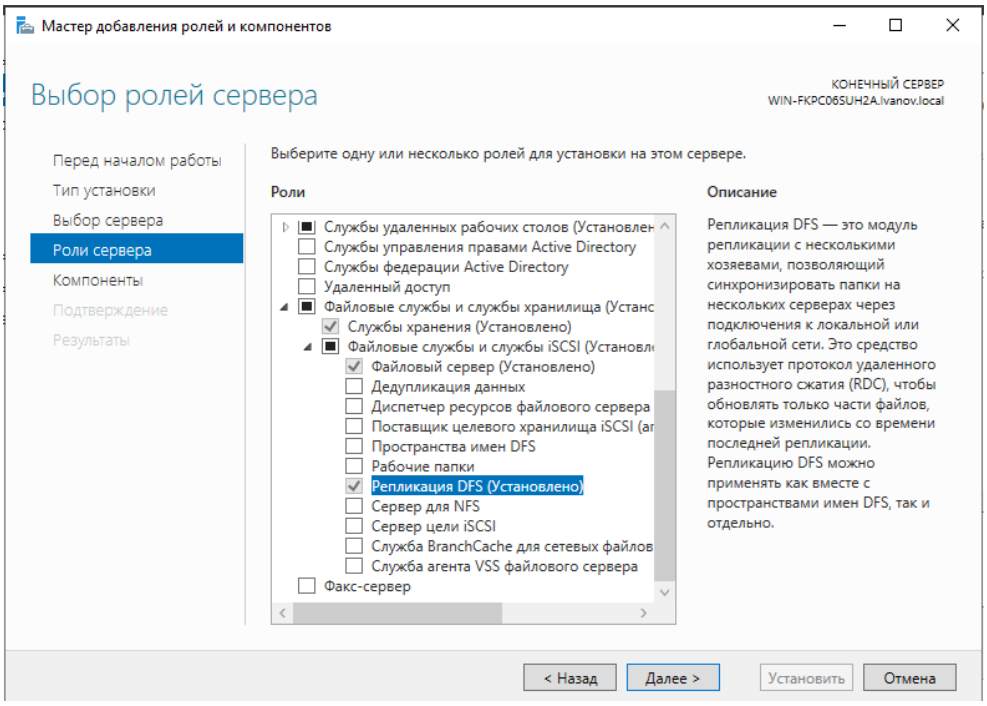


Рис. В.1. Вибір ролі сервера

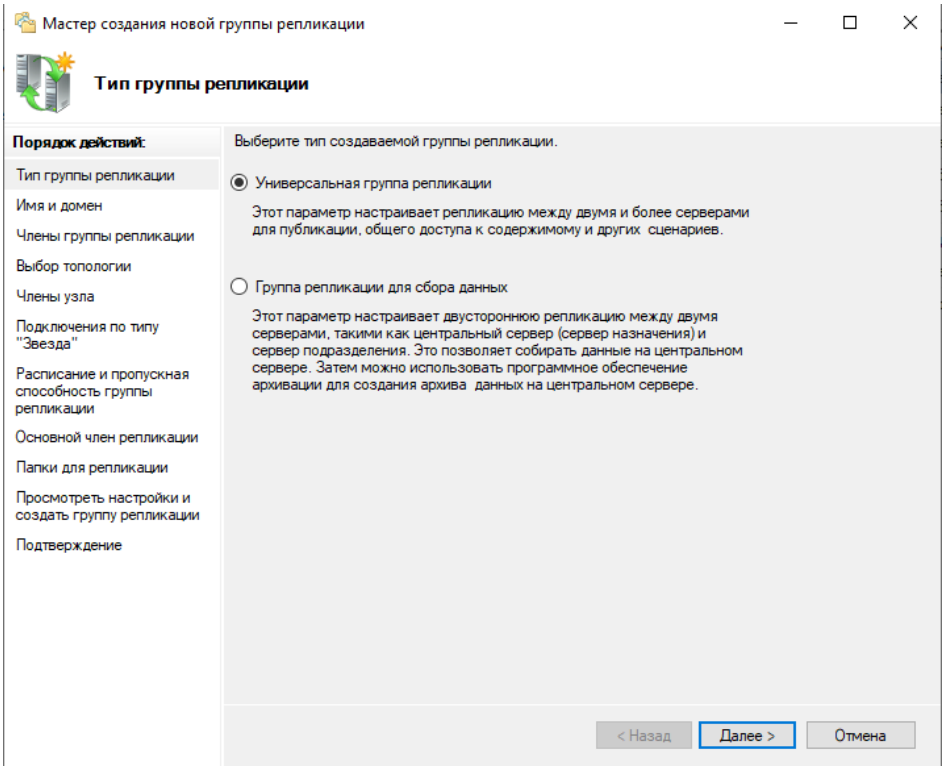


Рис. В.2. Початок налаштування реплікації

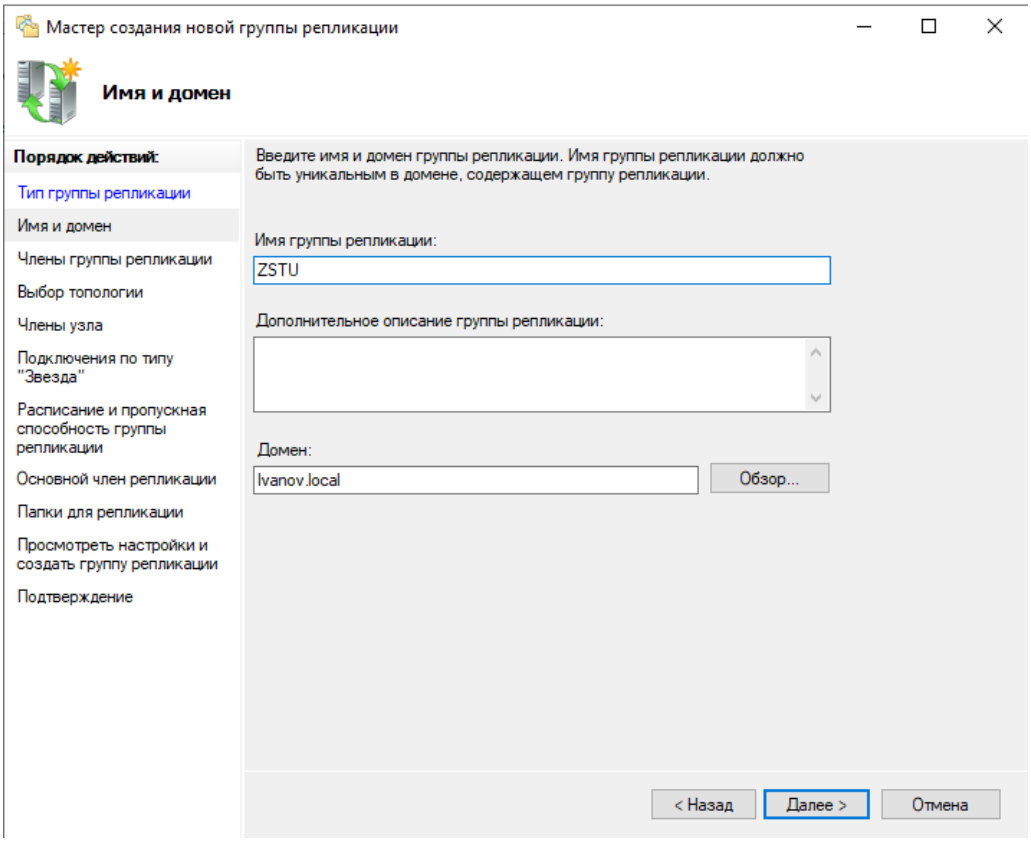


Рис. В.3. Створення групи реплікації

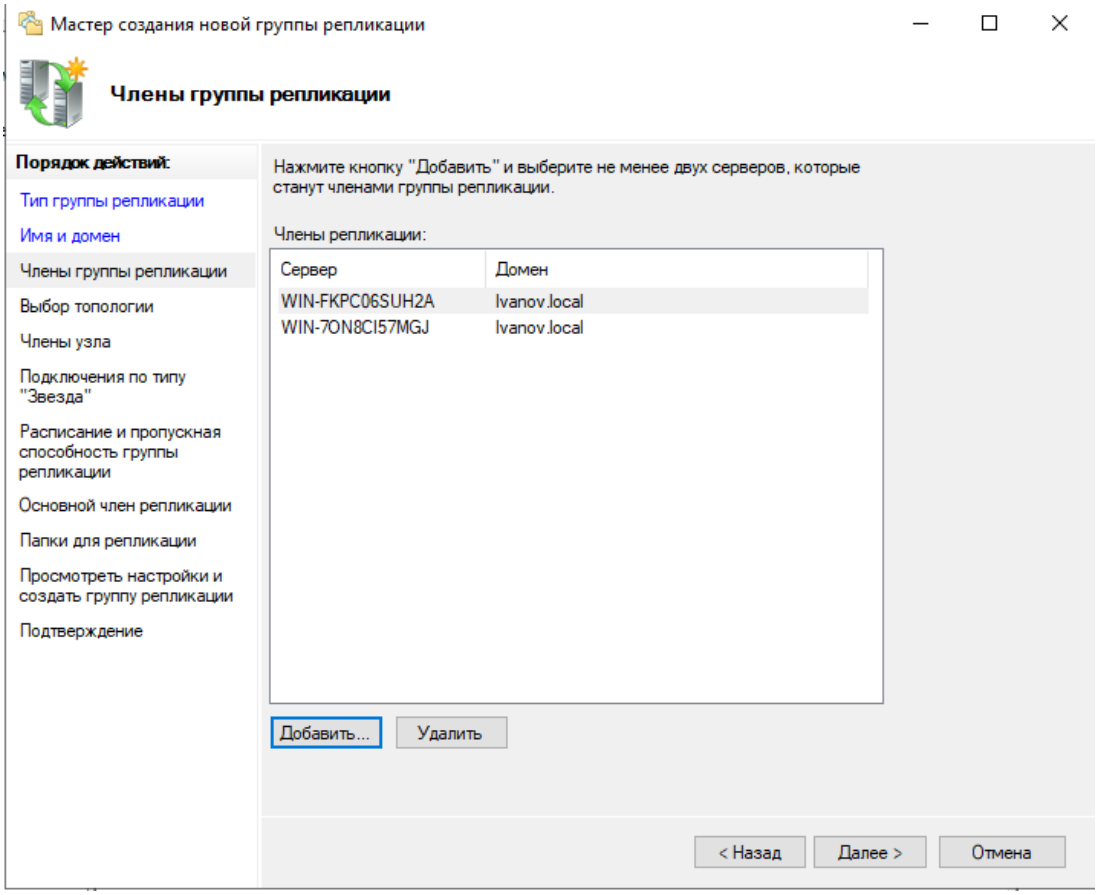


Рис. В.4. Члени реплікації

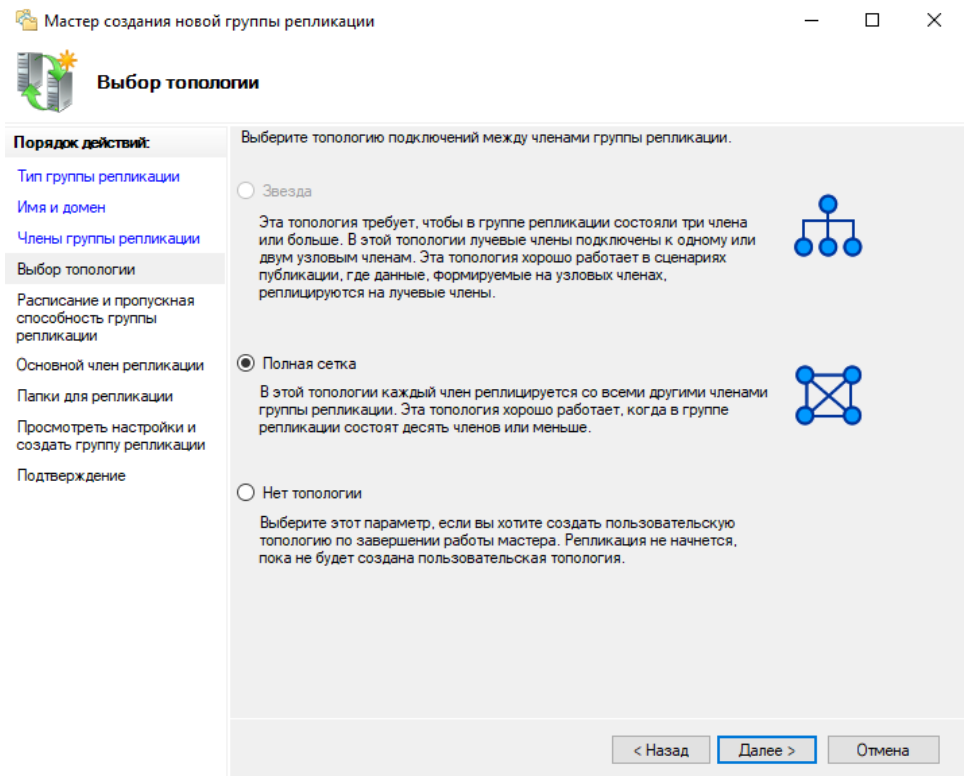


Рис. В.5. Топологія реплікації

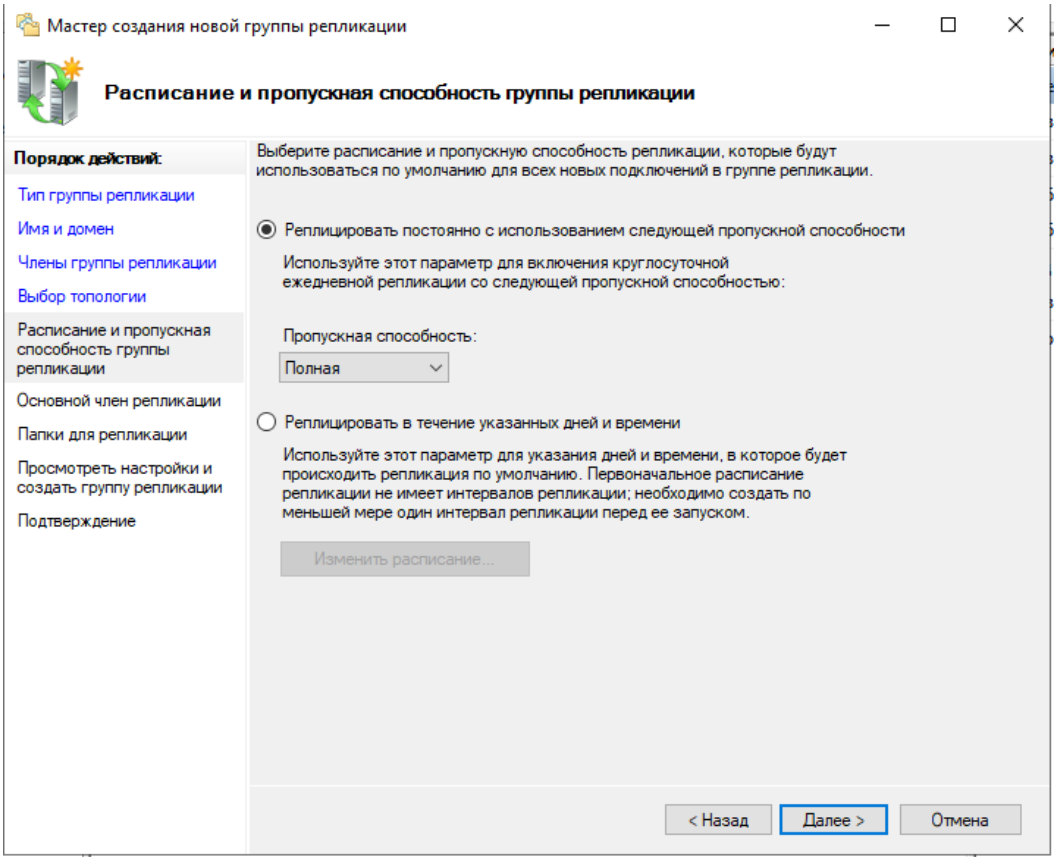


Рис. В.6. Розклад реплікації

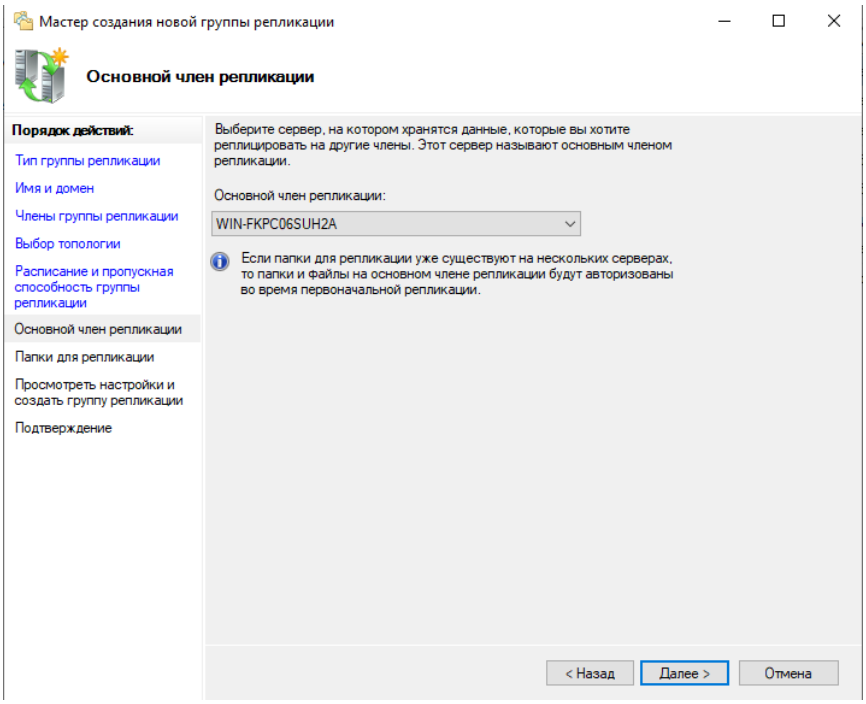


Рис. В.7. Основний член реплікації

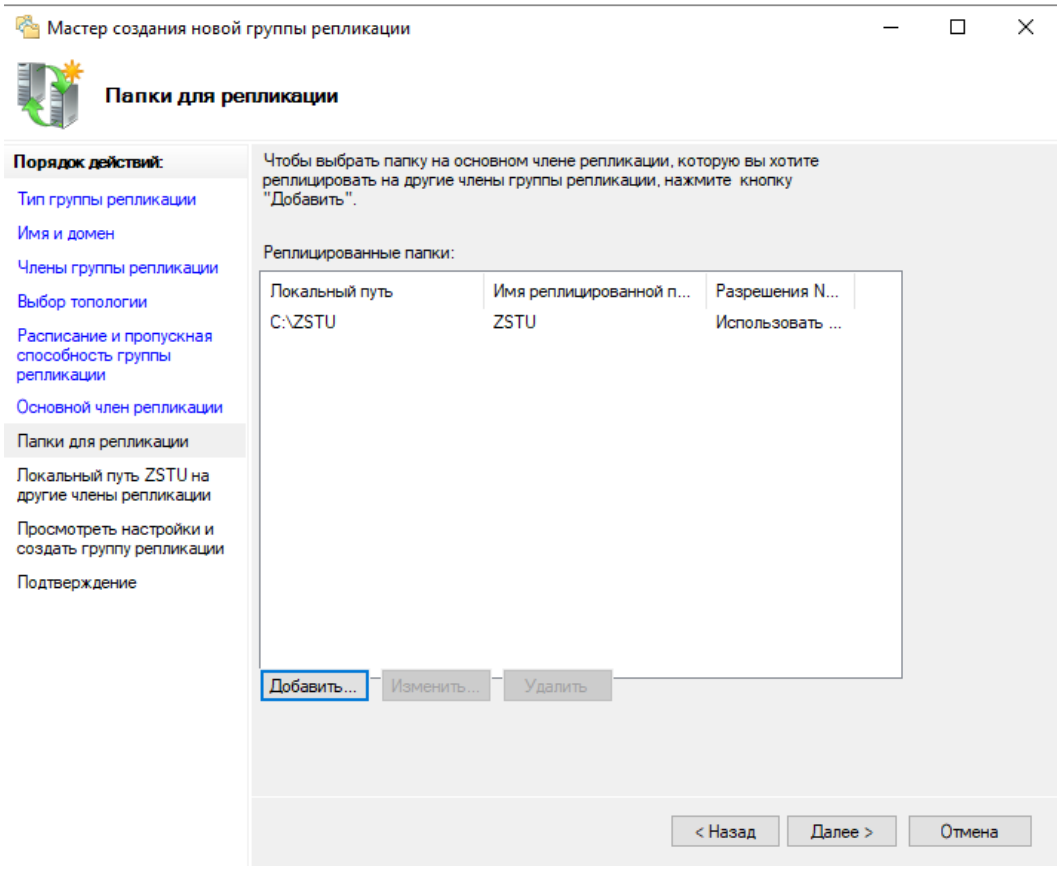


Рис. В.8. Папка реплікації

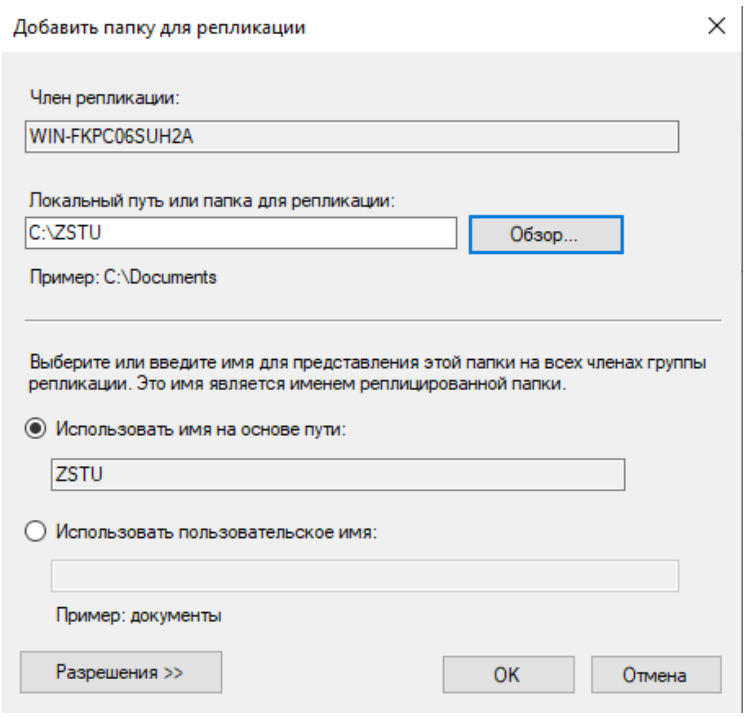


Рис. В.9. Додання папки для реплікації

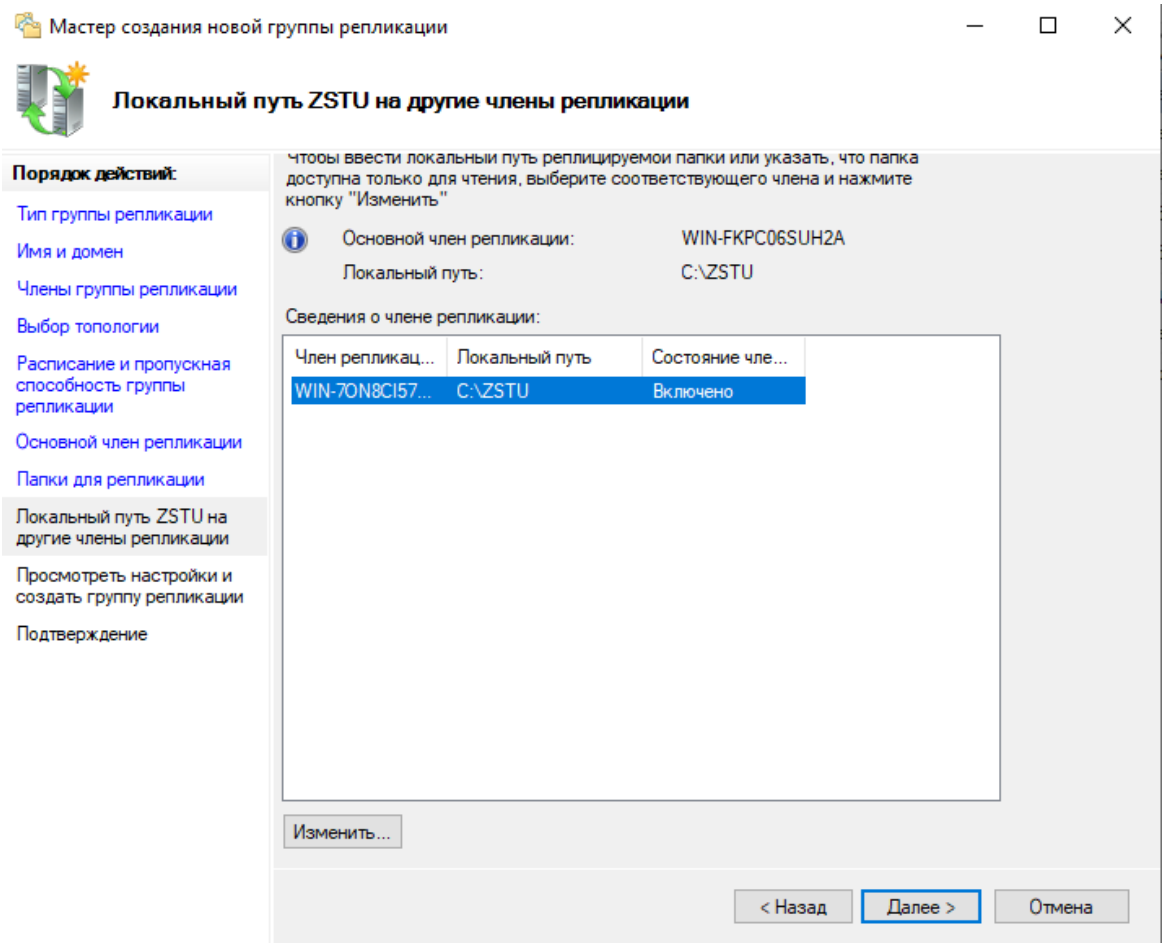


Рис. В.10. Папка реплікації на іншому члені реплікації

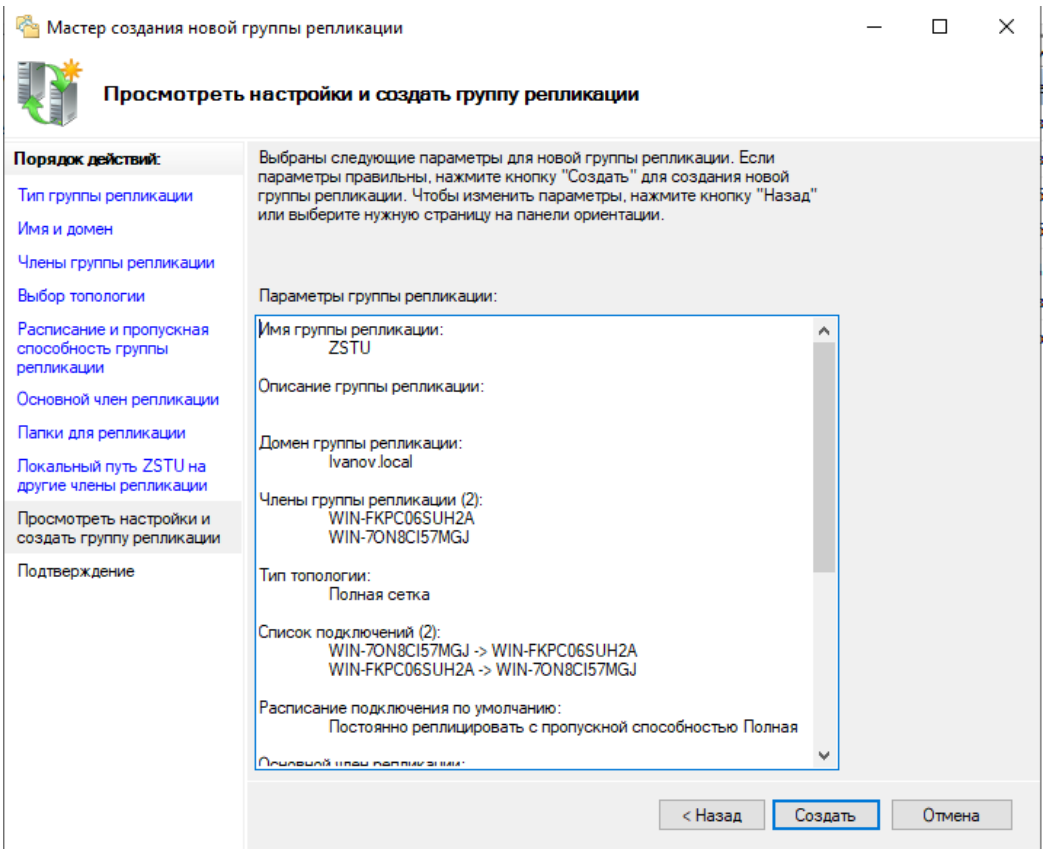


Рис. В.11. Налаштування реплікації

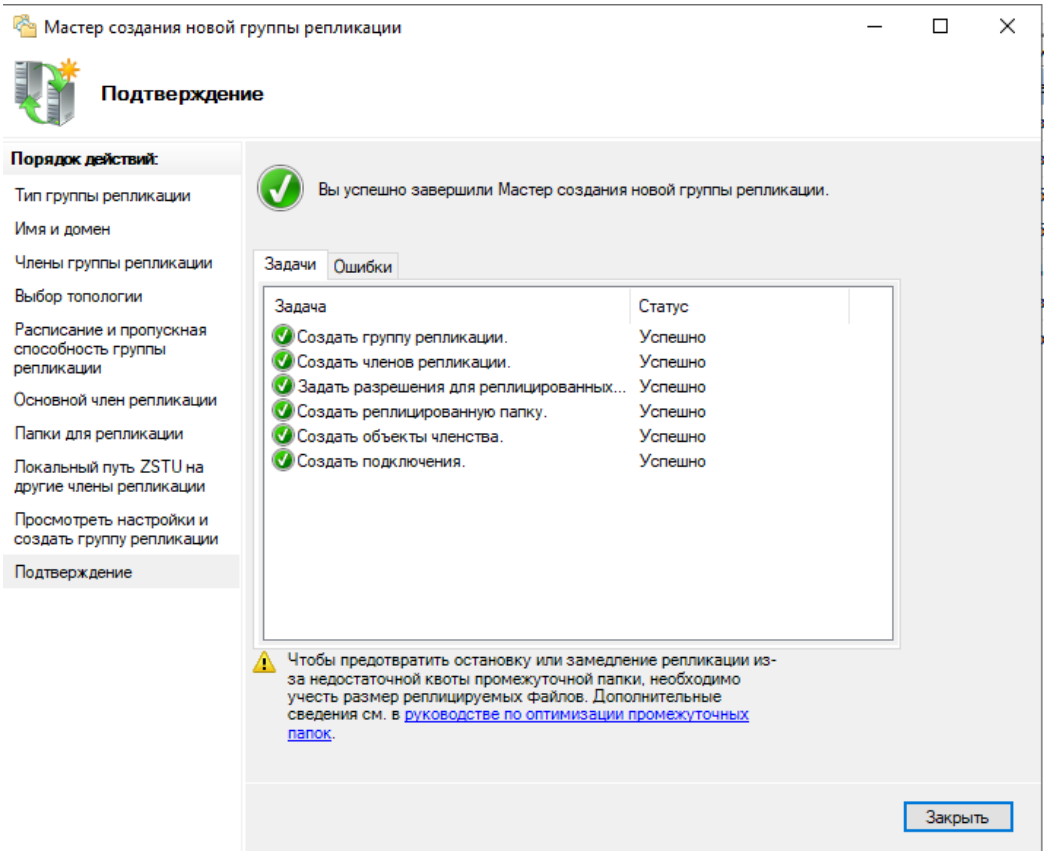


Рис. В.12. Створеня група реплікації

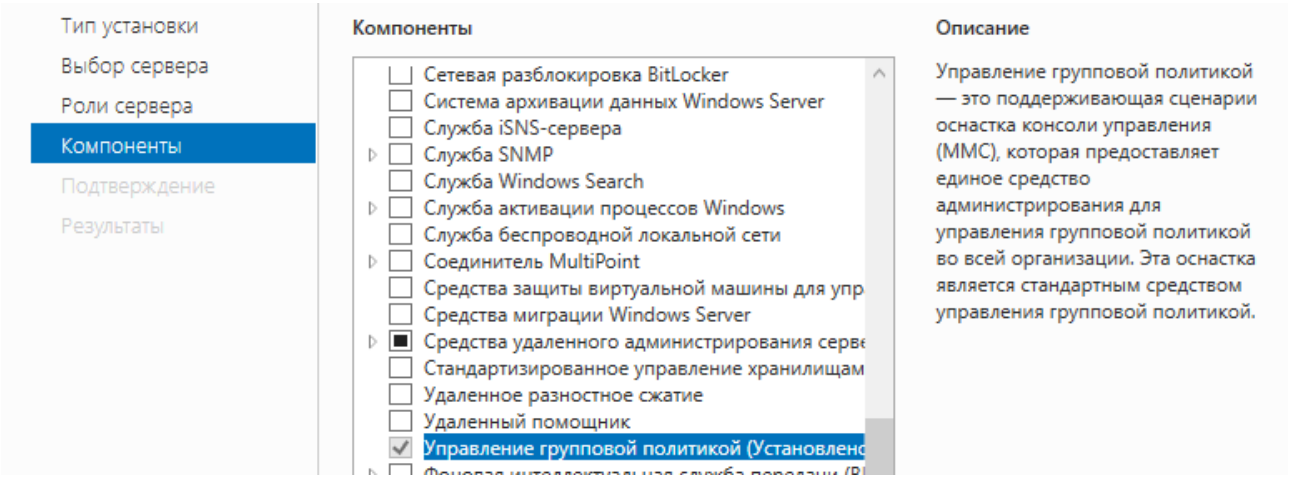


Рис. Г.1. Вибір ролі сервера

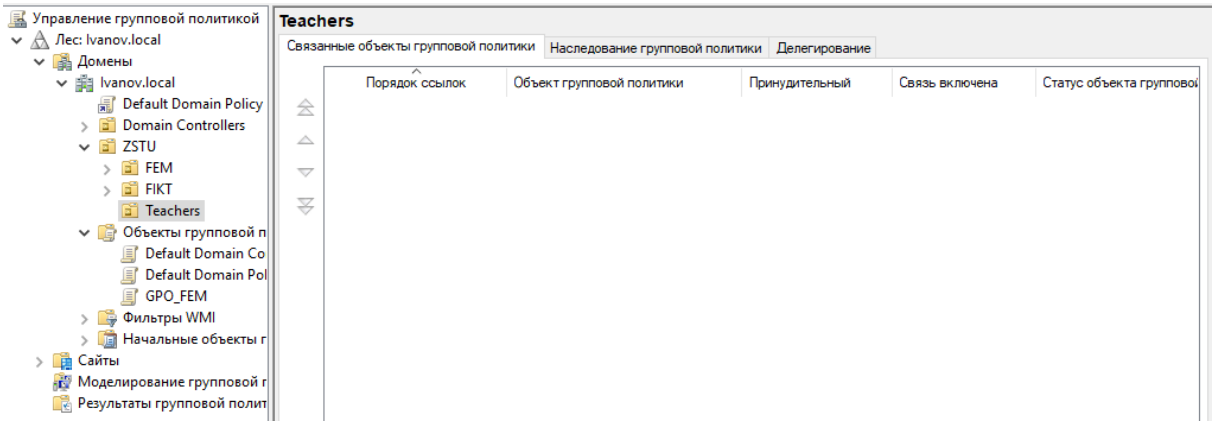


Рис. Г.2. Створений об’єкт групової політики

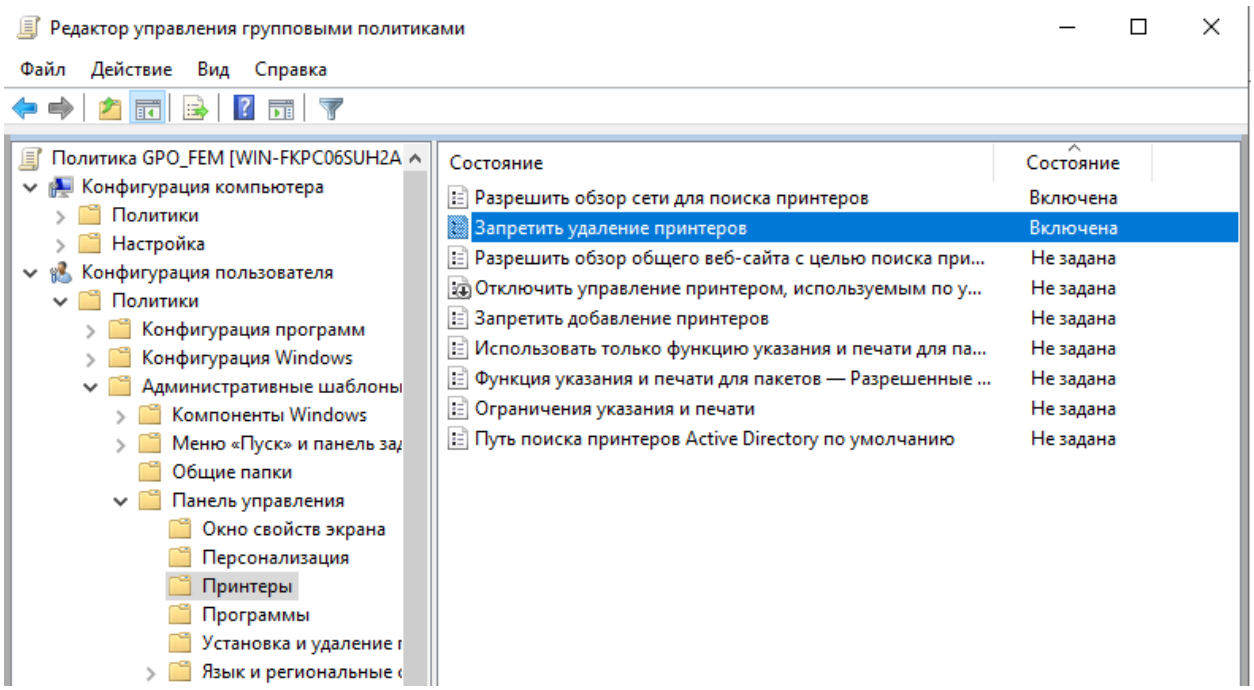


Рис. Г.3. Налаштування об’єкта групової політики

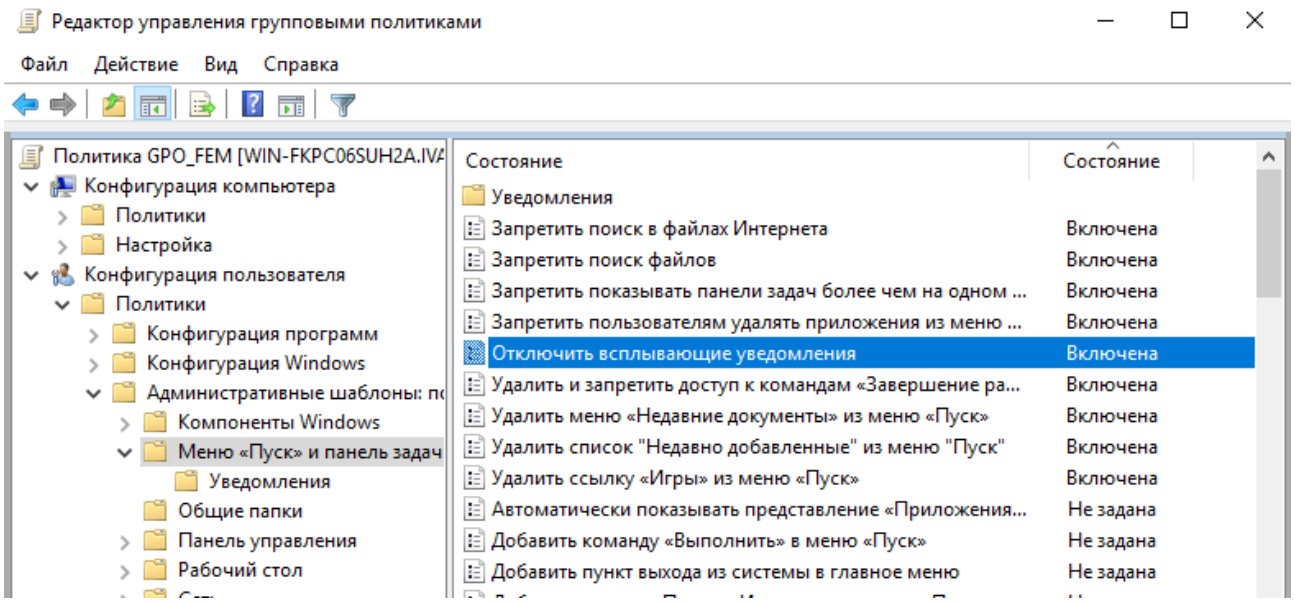


Рис. Г.4. Налаштування об’єкта групової політики

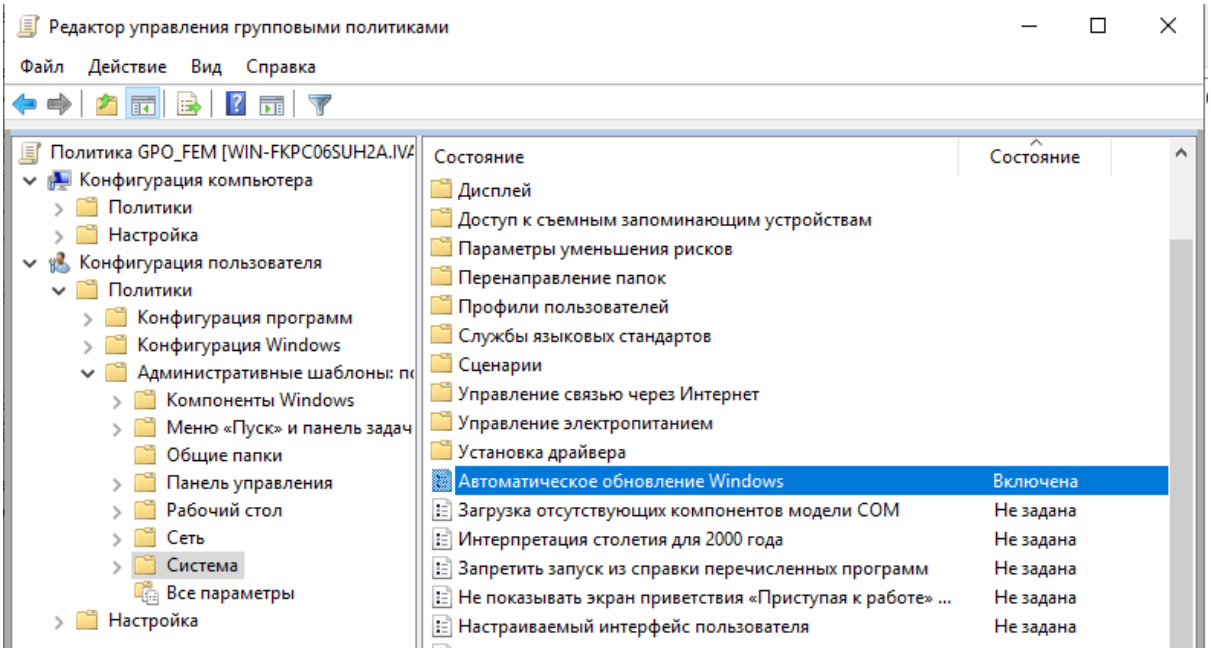


Рис. Г.5. Налаштування об’єкта групової політики

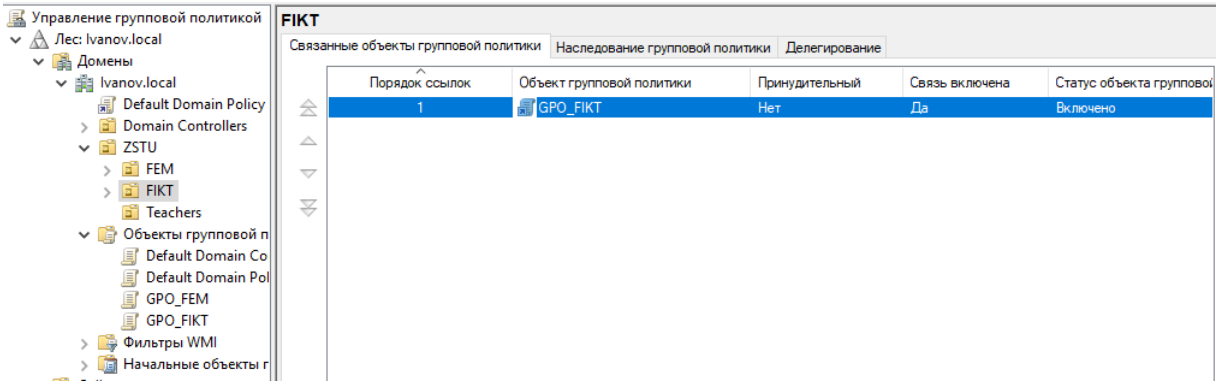


Рис. Г.6. Створений об’єкт групової політики

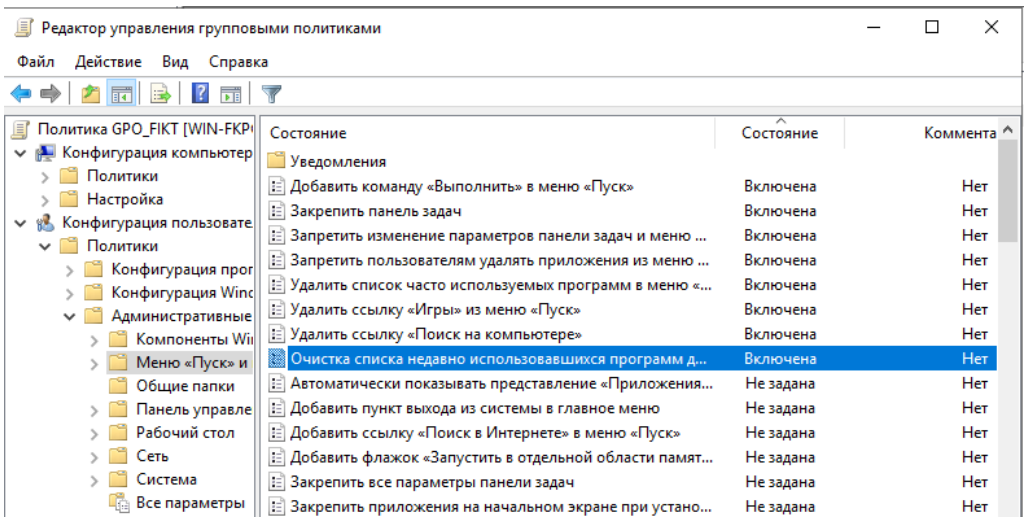


Рис. Г.7. Налаштування об’єкта групової політики

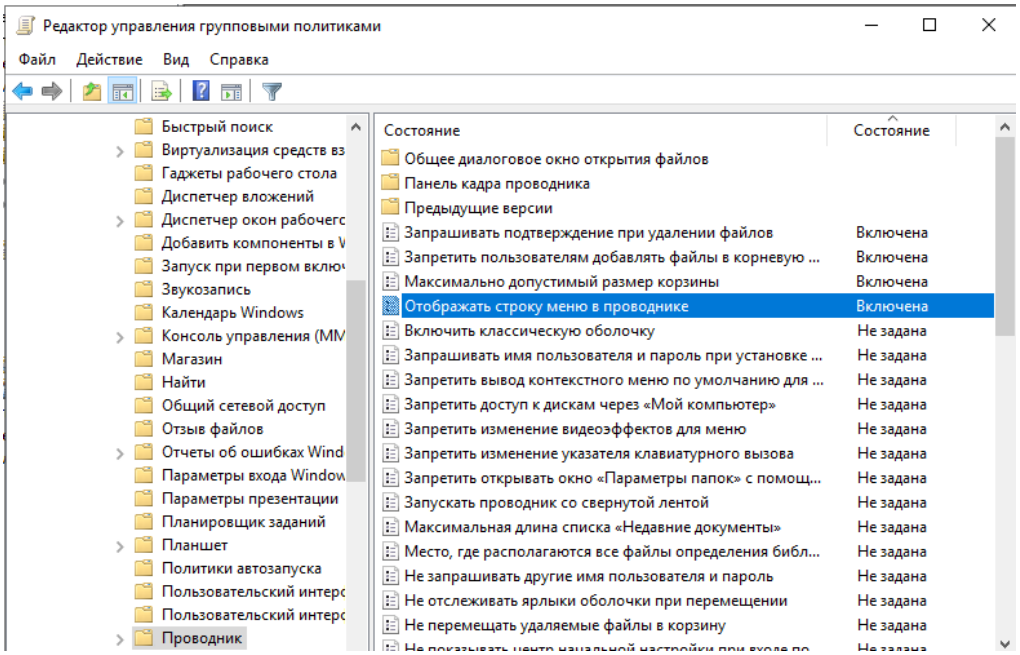


Рис. Г.8. Налаштування об’єкта групової політики

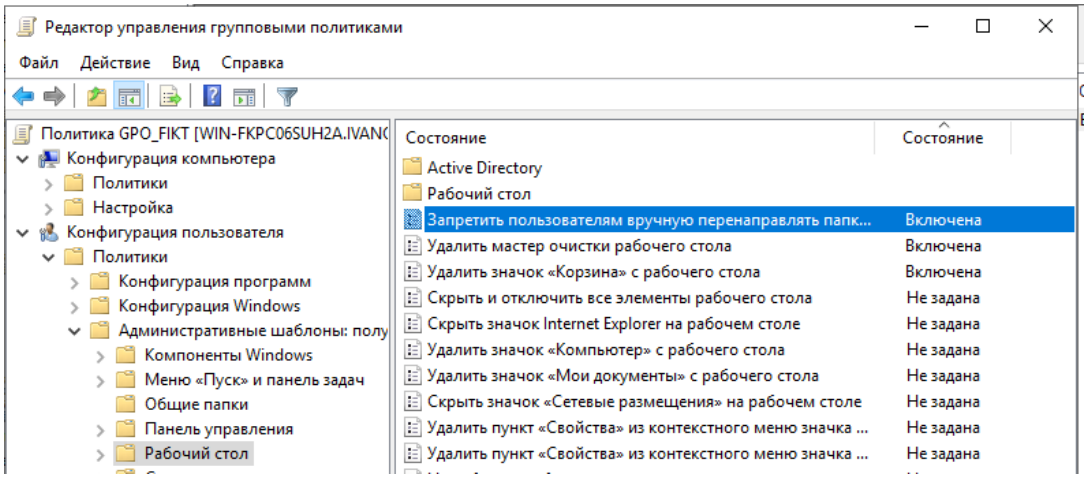


Рис. Г.9. Налаштування об’єкта групової політики

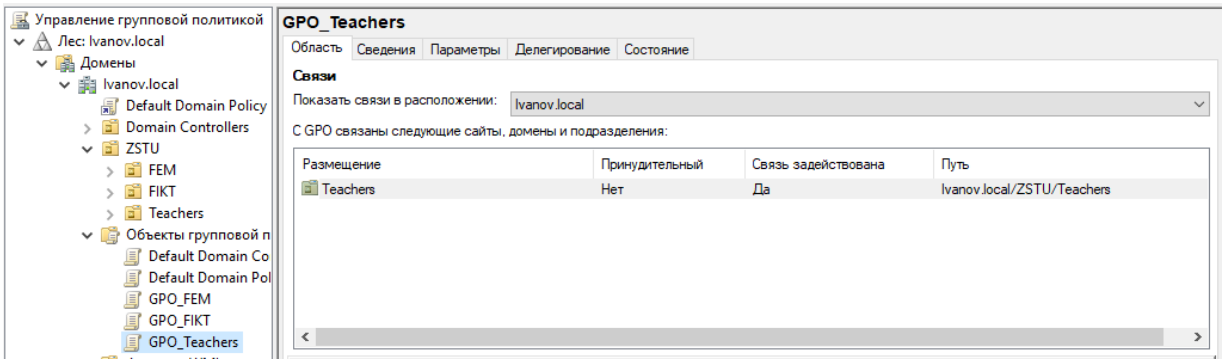


Рис. Г.10. Створений об’єкт групової політики

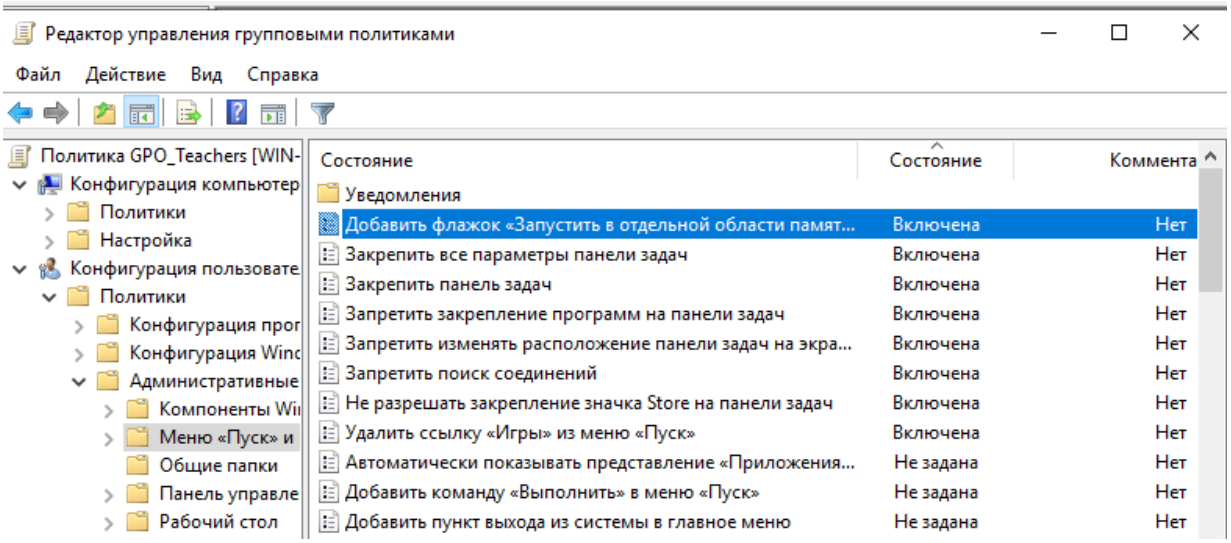


Рис. Г.11. Налаштування об’єкта групової політики

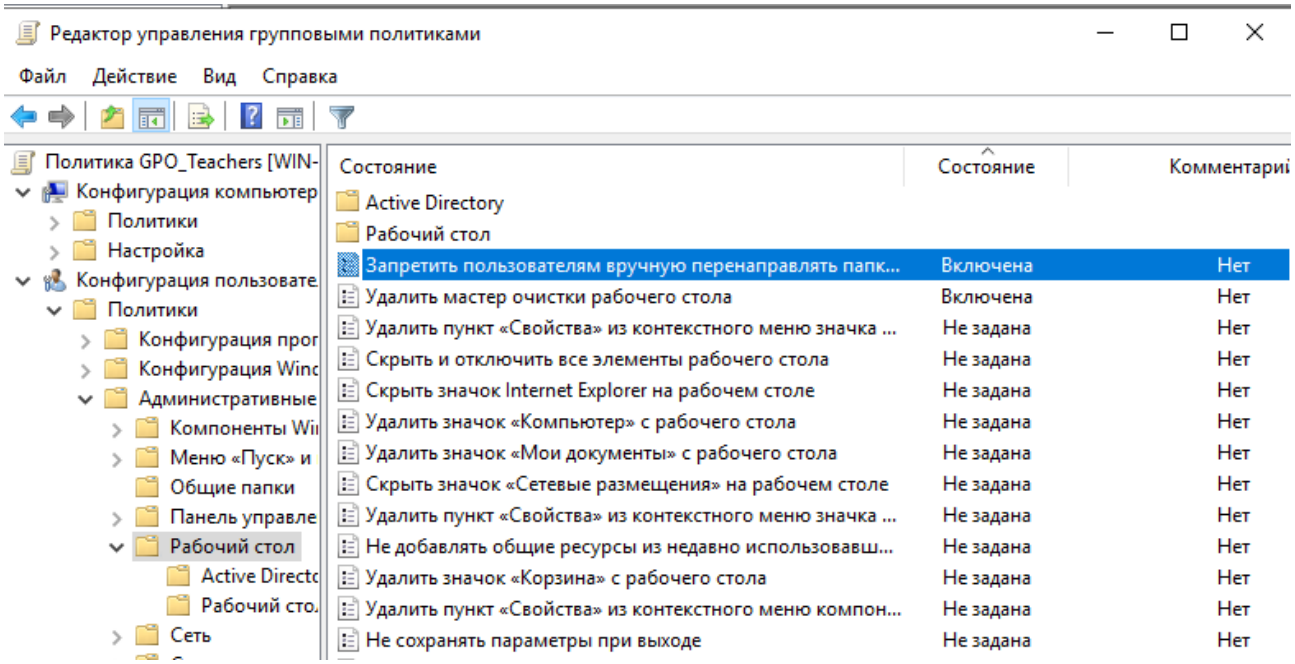


Рис. Г.12. Налаштування об’єкта групової політики

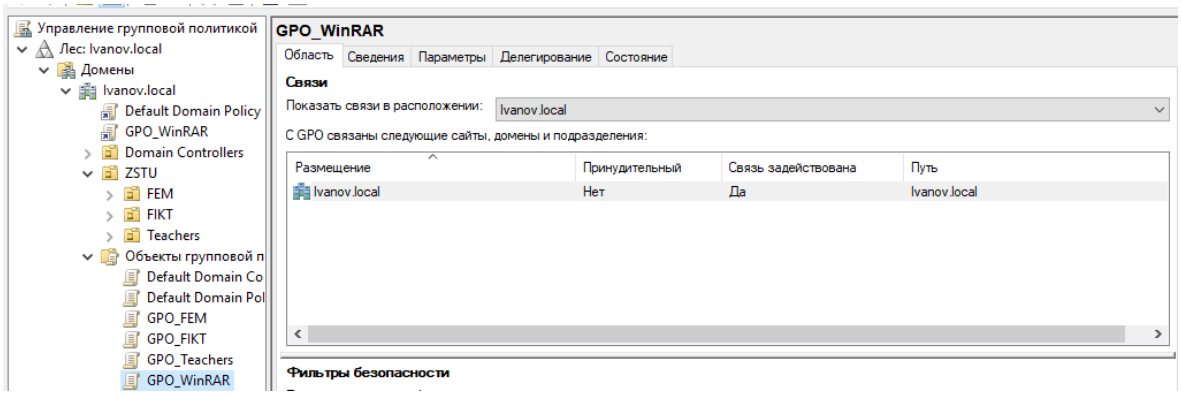


Рис. Г.13. Створений об’єкт групової політики

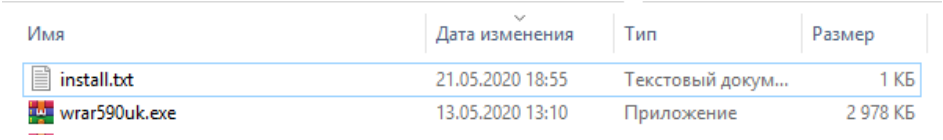


Рис. Г.14. Файли для встановлення ПО

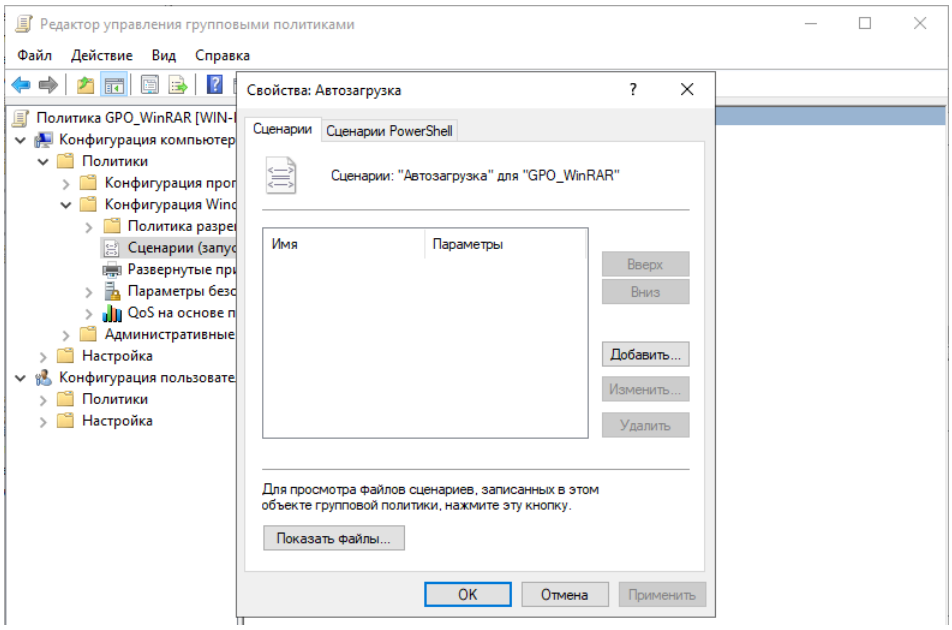


Рис. Г.15. Налаштування об’єкта групової політики

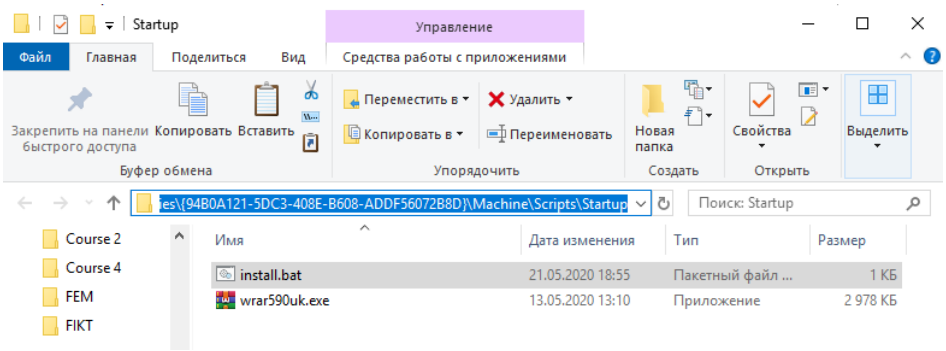


Рис. Г.16. Додання файлів до об’єкта групової політики

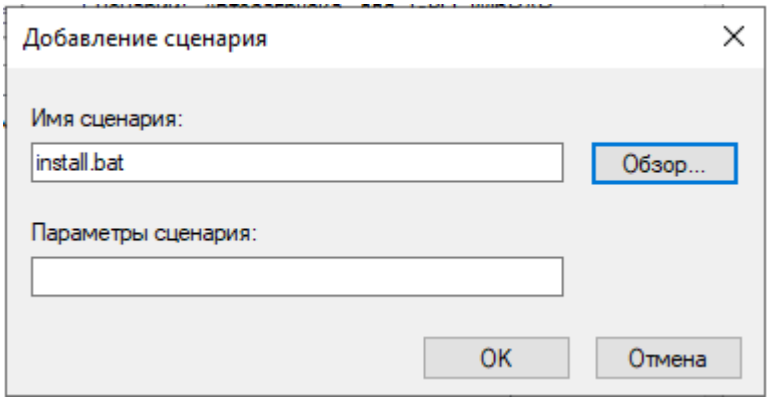


Рис. Г.17. Додання скрипта до об’єкта групової політики

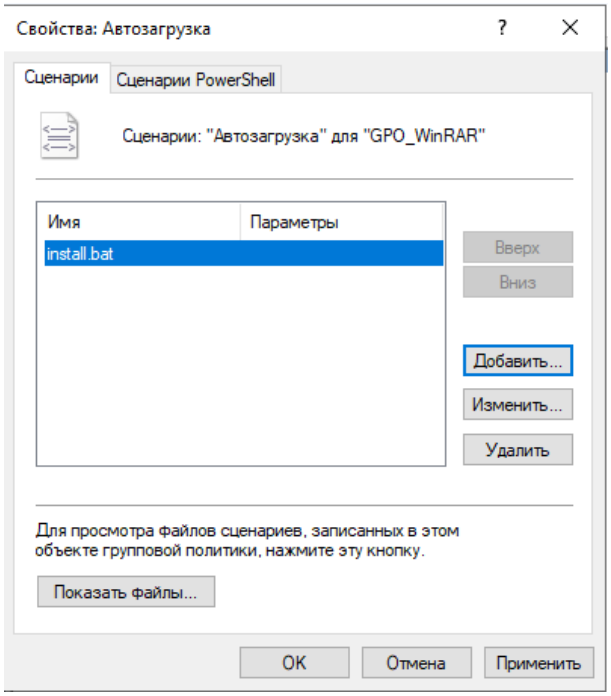


Рис. Г.18. Доданий скрипт до об’єкта групової політики

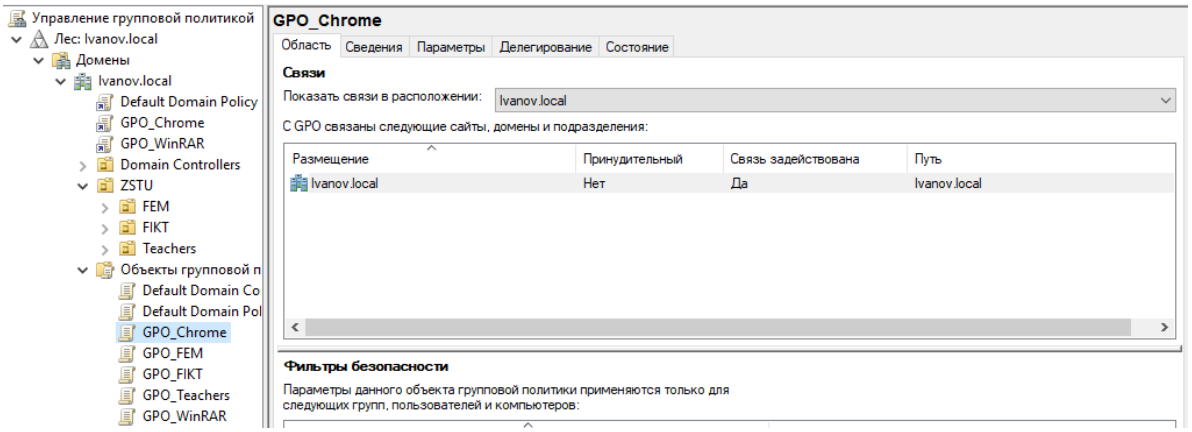


Рис. Г.19. Створений об’єкт групової політики

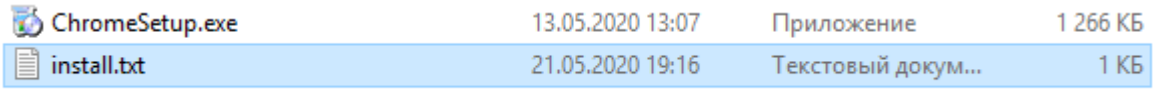


Рис. Г.20. Файли для встановлення ПО

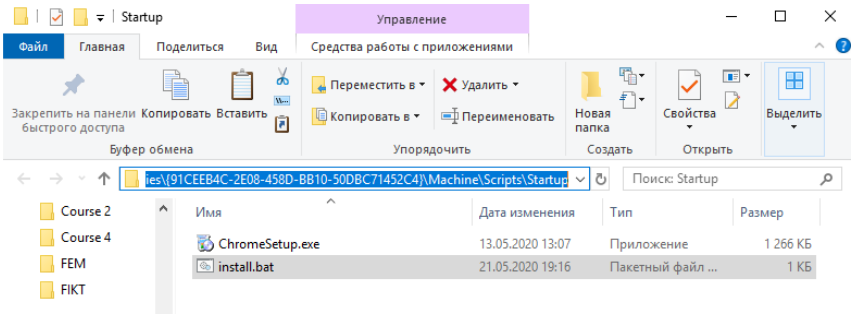


Рис. Г.21. Додання файлів до об’єкта групової політики

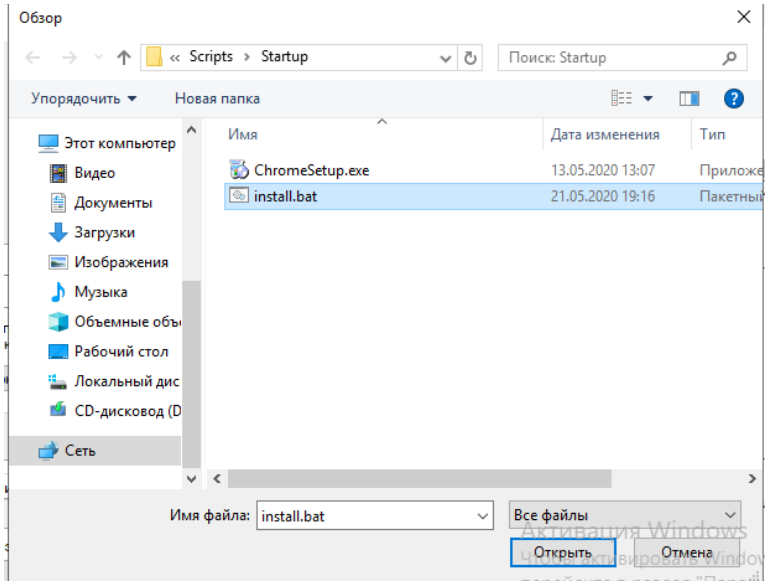


Рис. Г.22. Доданий скрипт до об’єкта групової політики

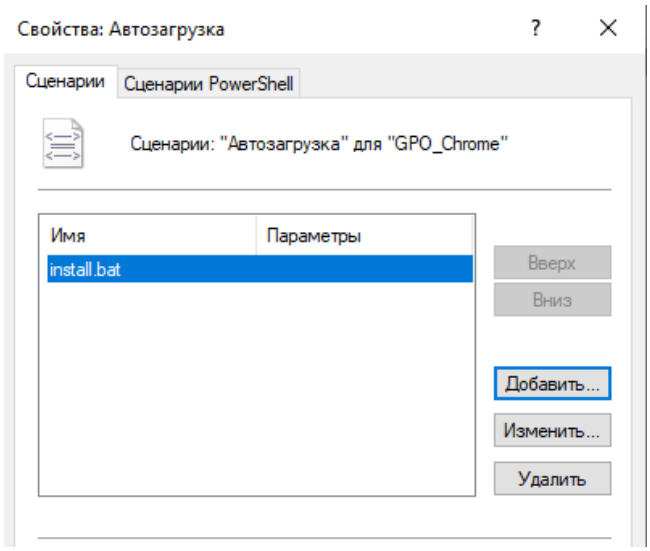


Рис. Г.23. Доданий скрипт до об’єкта групової політики

ДОДАТОК Д

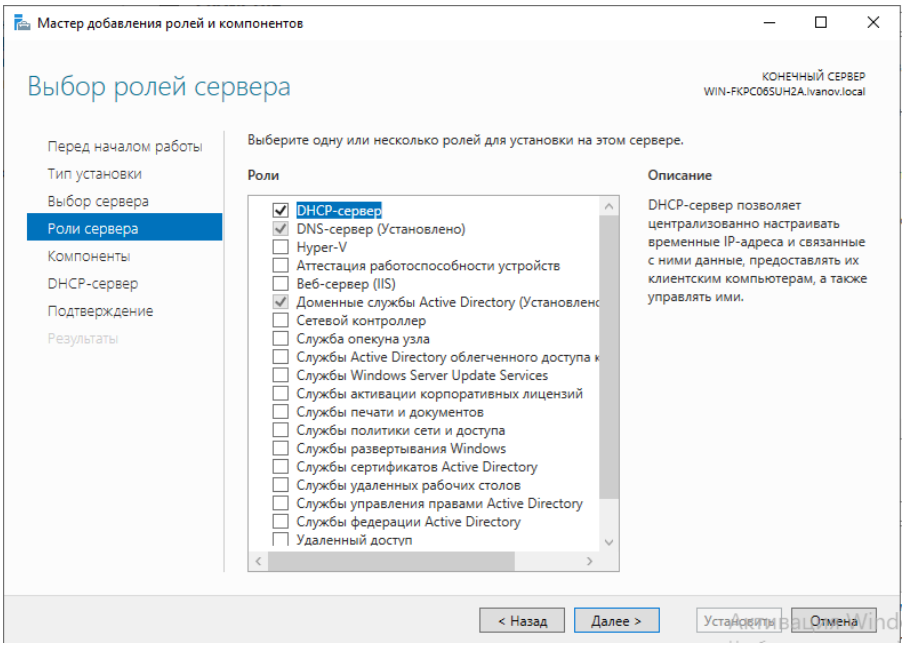


Рис. Д.1. Вибір ролі сервера

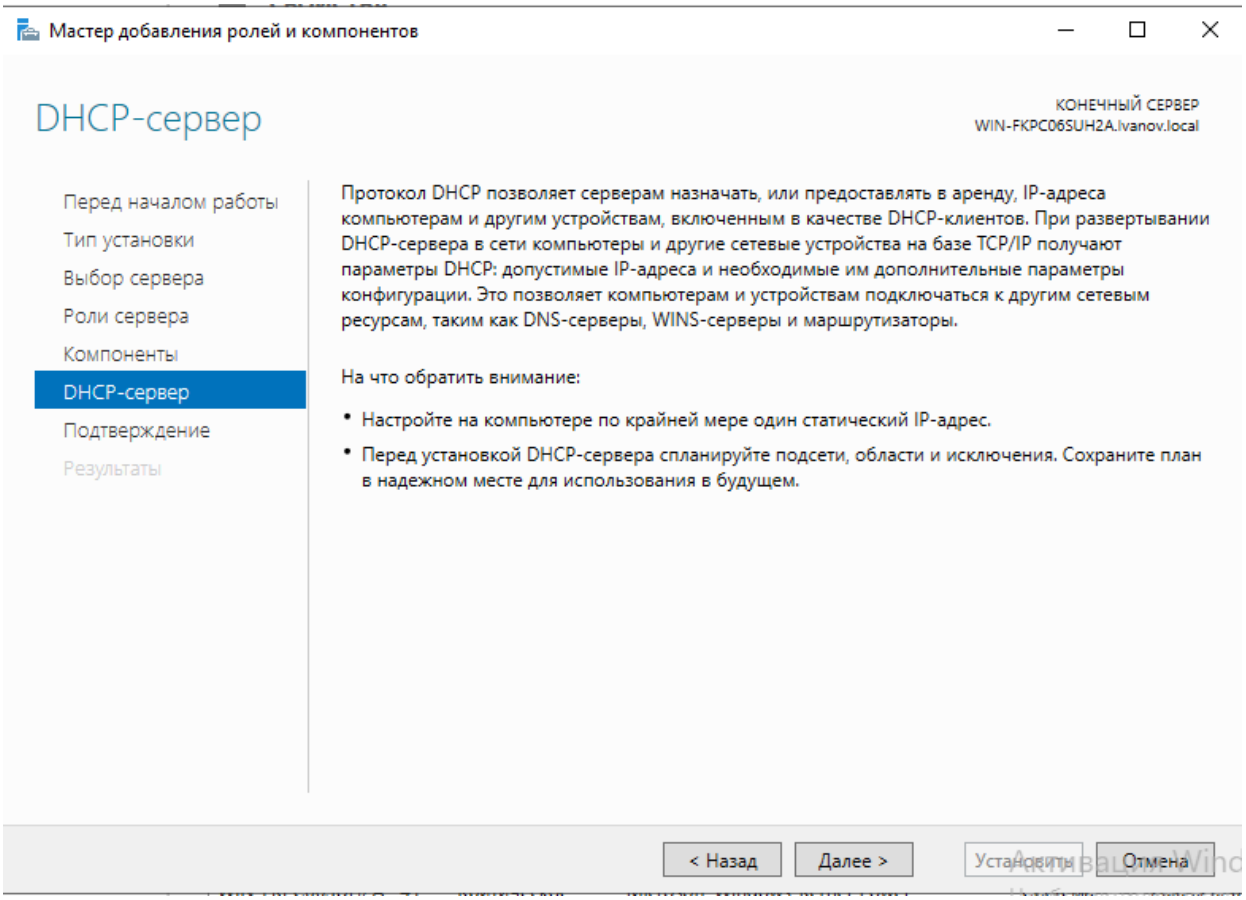


Рис. Д.2. Налаштування ролі сервера

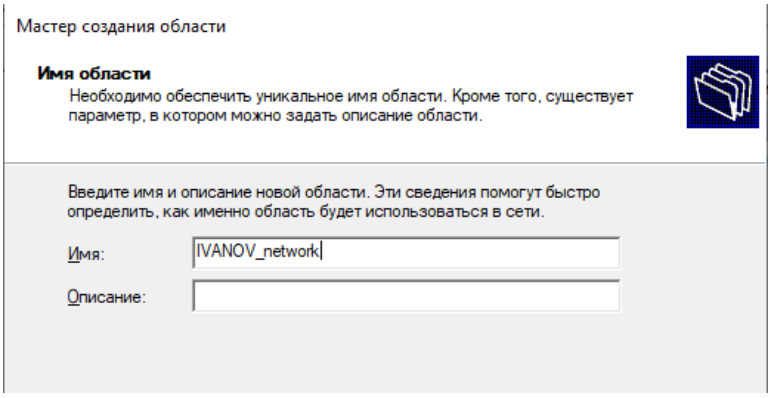


Рис. Д.3. Налаштування DHCP-області

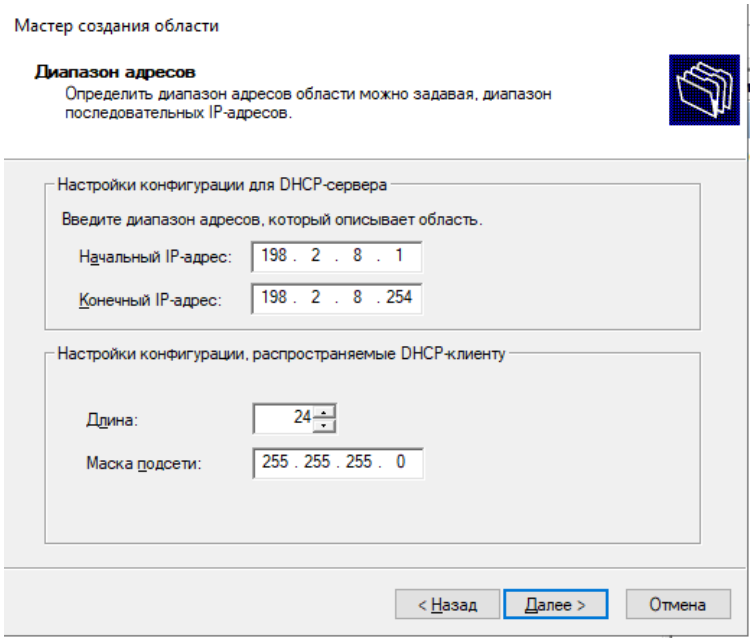


Рис. Д.4. Налаштування діапазона DHCP-області

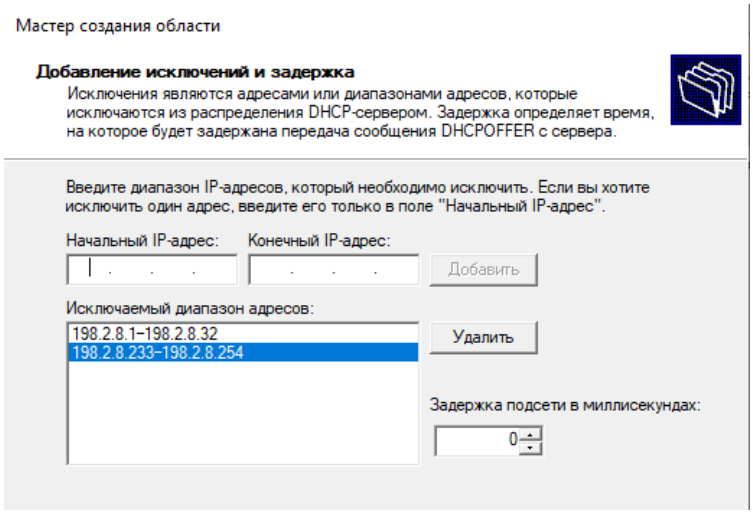


Рис. Д.5. Налаштування адрес DHCP-області

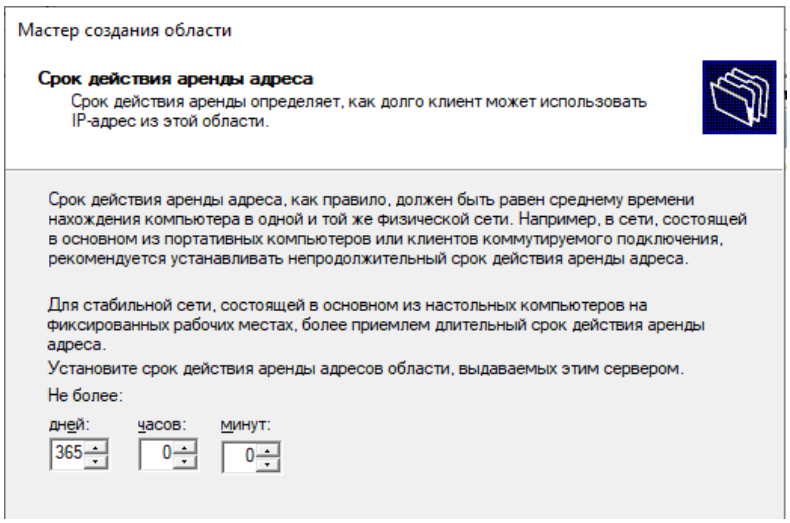


Рис. Д.6. Налаштування DHCP-області

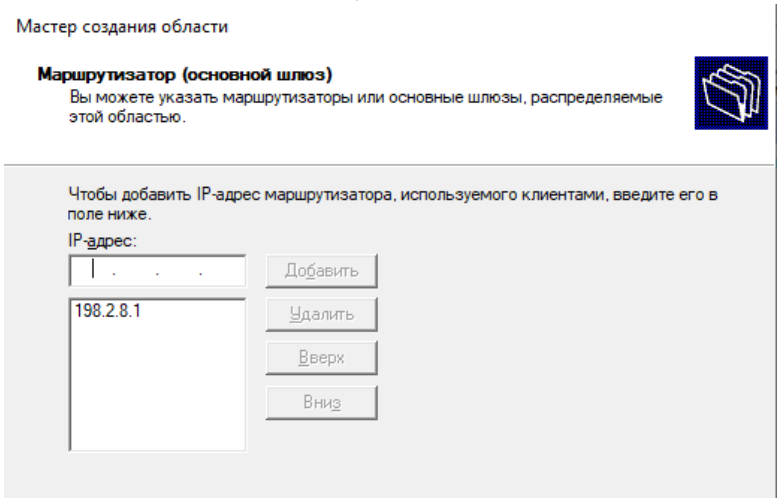


Рис. Д.7. Налаштування основного шлюза DHCP-області

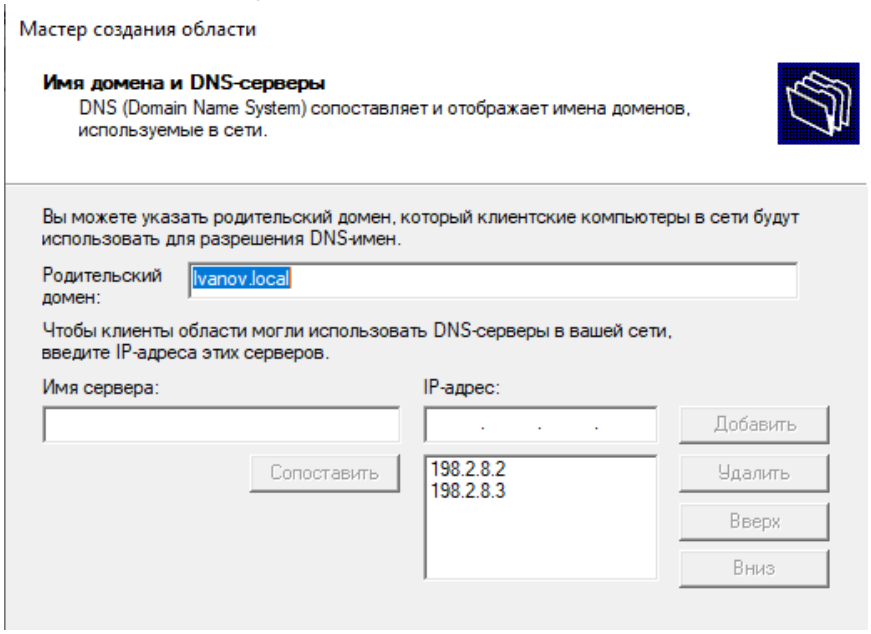


Рис. Д.8. Налаштування DNS DHCP-області

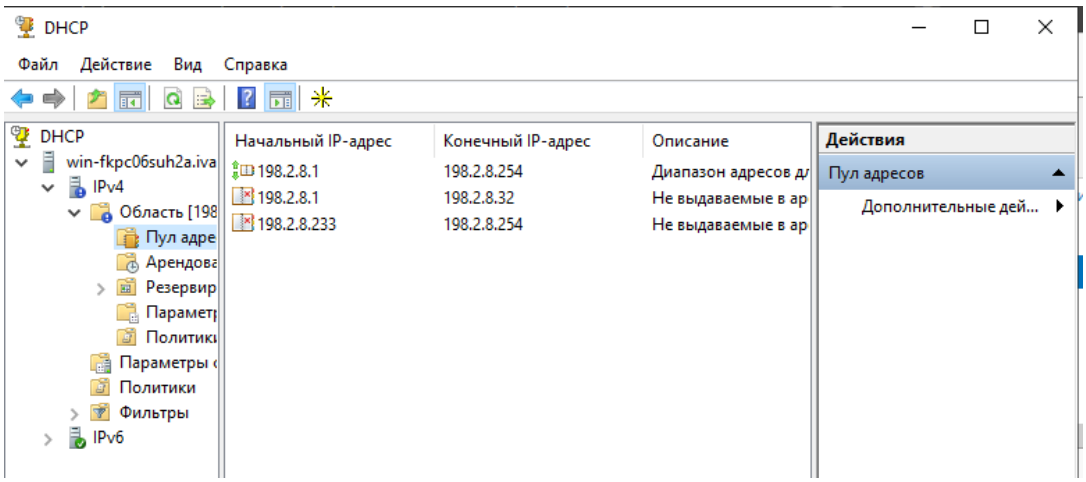


Рис. Д.9. Створена DHCP-області

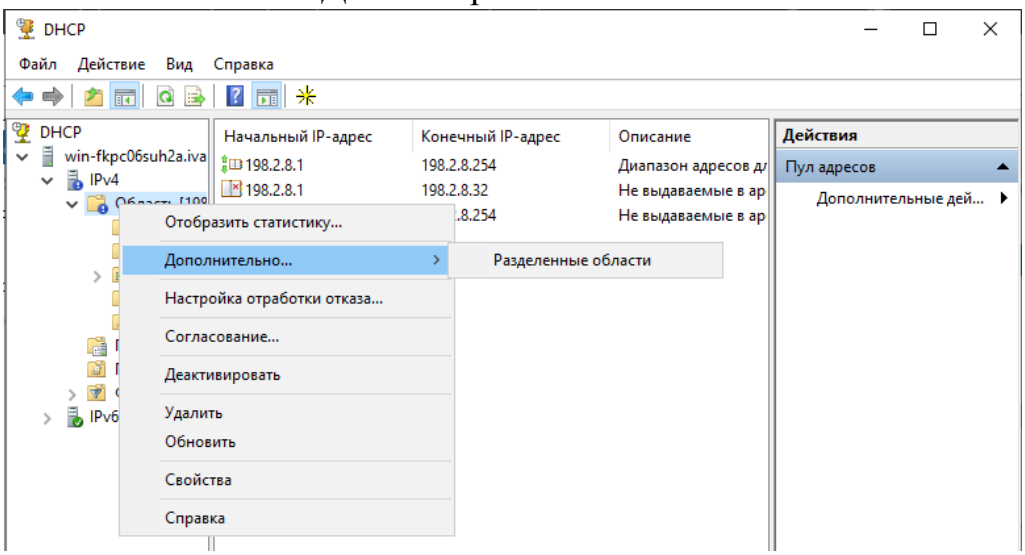


Рис. Д.10. Додаткові налаштування DHCP-області

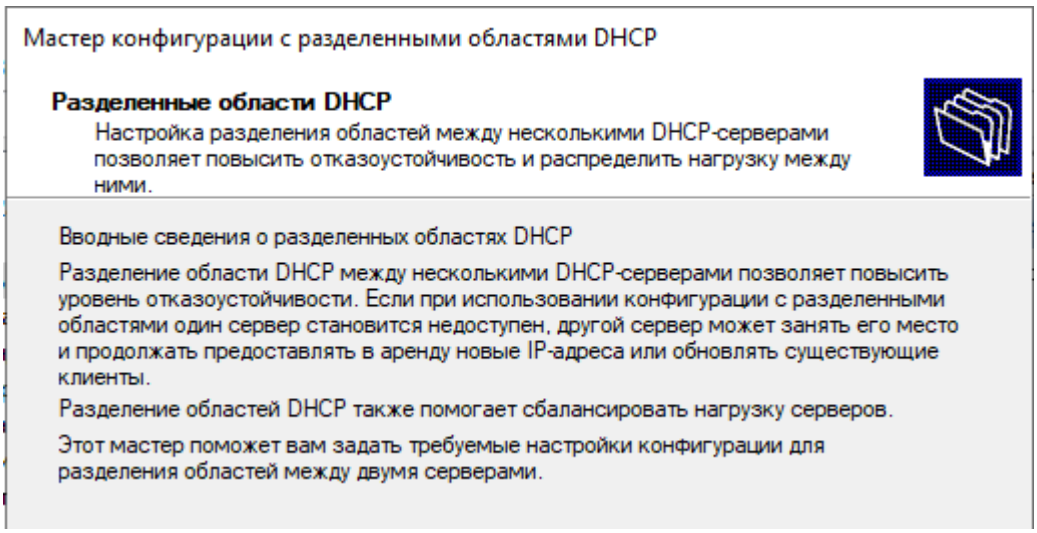


Рис. Д.11. Розділення DHCP-області

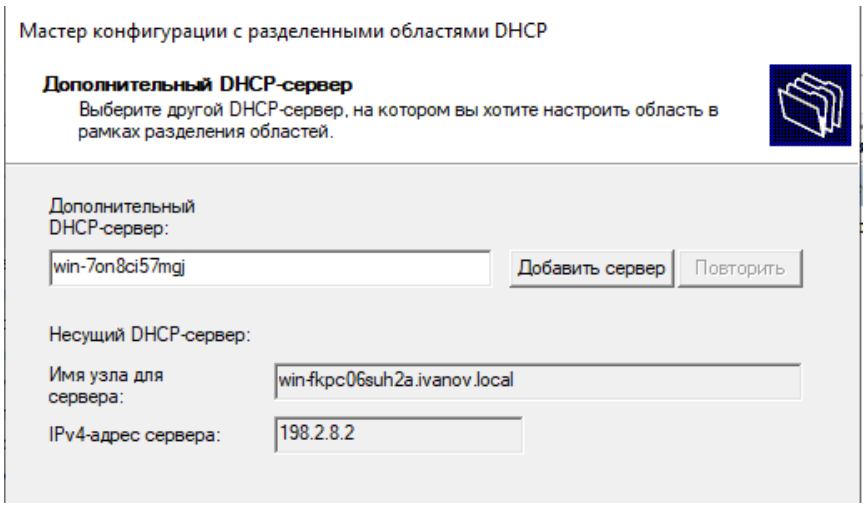


Рис. Д.12. Вибір сервера для розділення DHCP-області

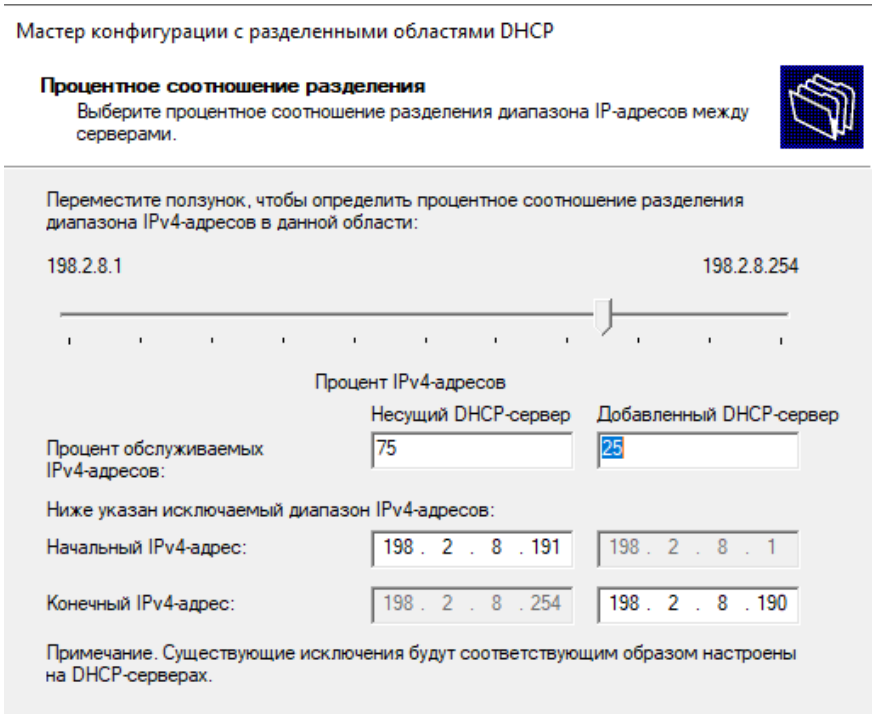


Рис. Д.13. Відсоткове відношення розділення DHCP-області

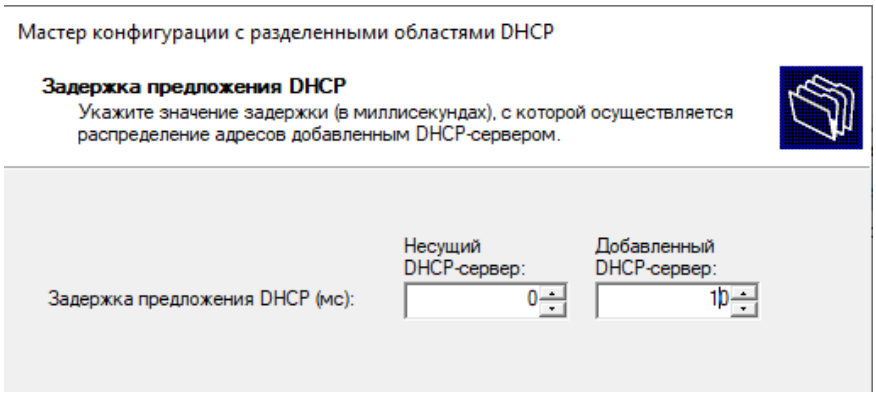


Рис. Д.14. Затримка DHCP-області



Рис. Д.15. Налаштоване розділення DHCP-області

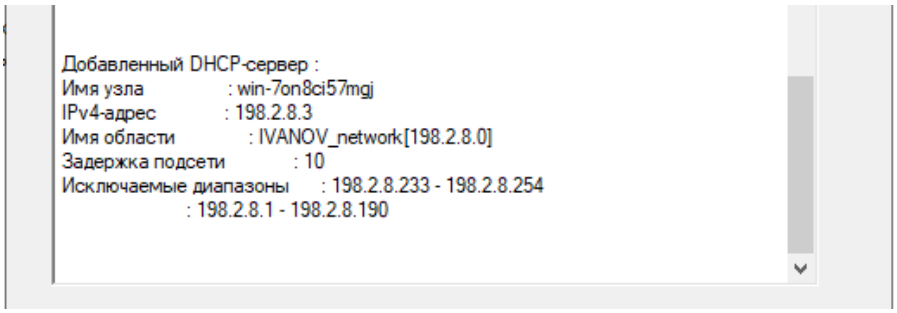


Рис. Д.16. Налаштоване розділення DHCP-області

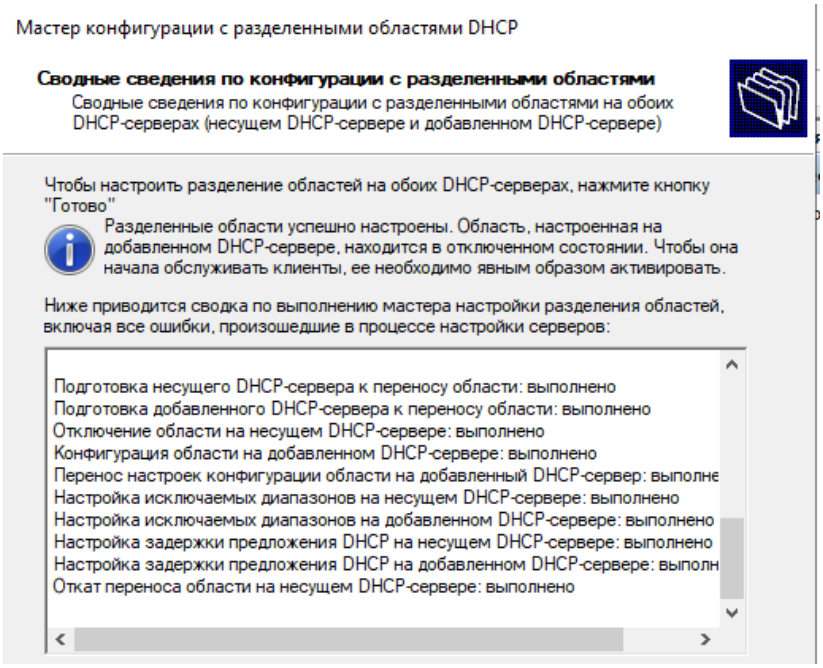


Рис. Д.17. Налаштоване розділення DHCP-області

ДОДАТОК Е

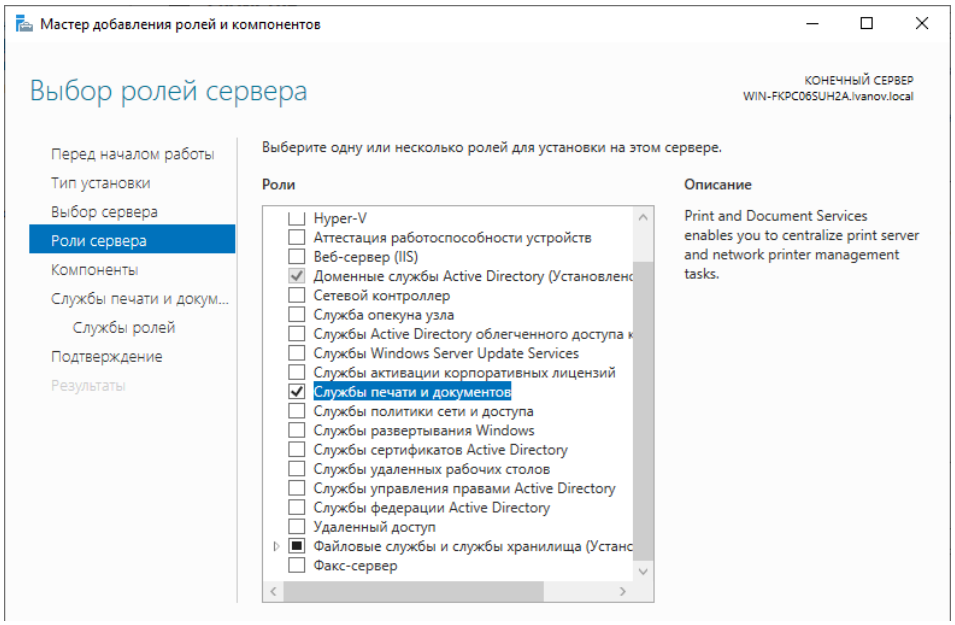


Рис. Е.1. Вибір ролі сервера

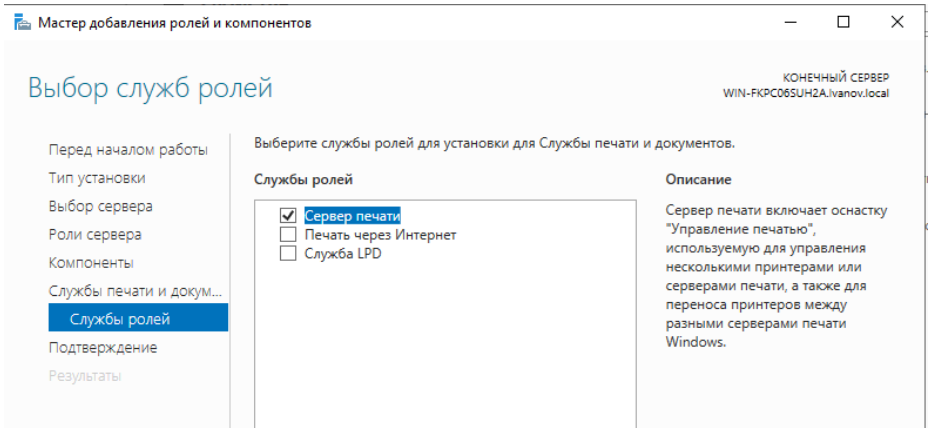


Рис. Е.2. Вибір служб ролей сервера

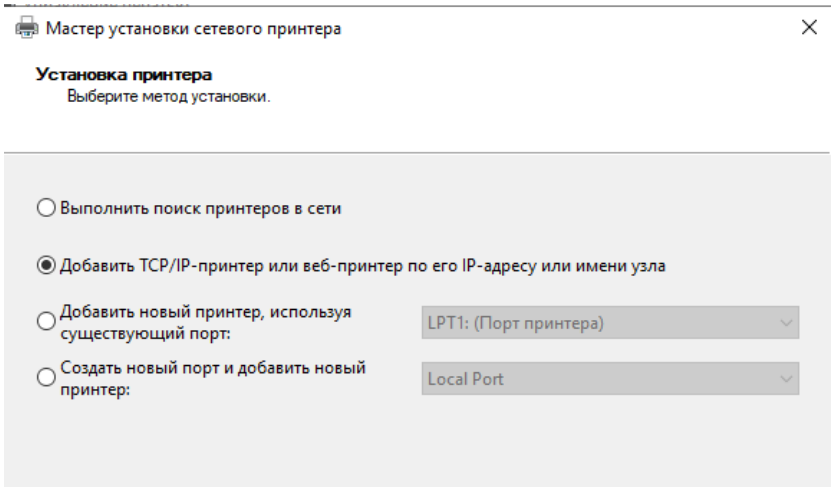


Рис. Е.3. Налаштування принтера

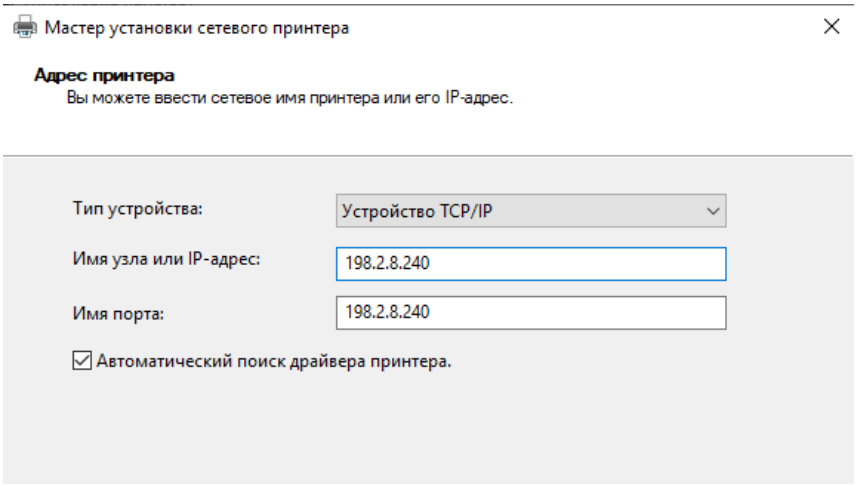


Рис. Е.4. Налаштування IP-адреси принтера

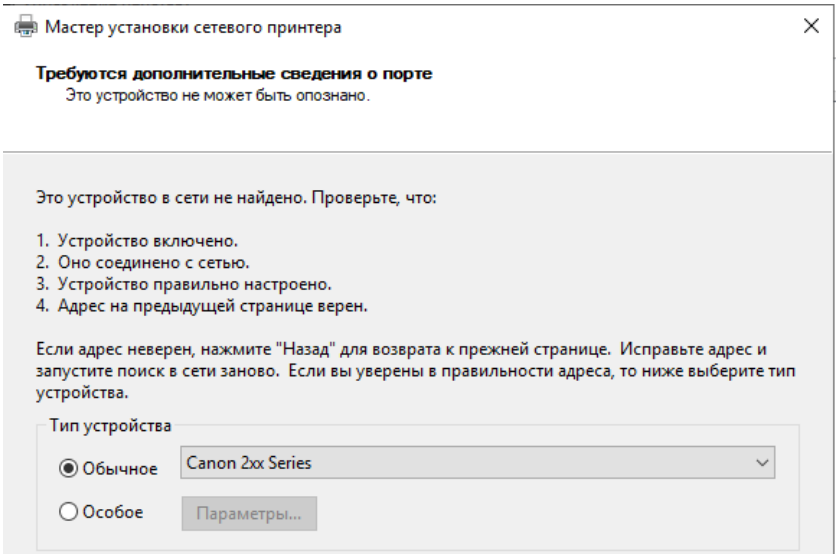


Рис. Е.5. Налаштування порта принтера

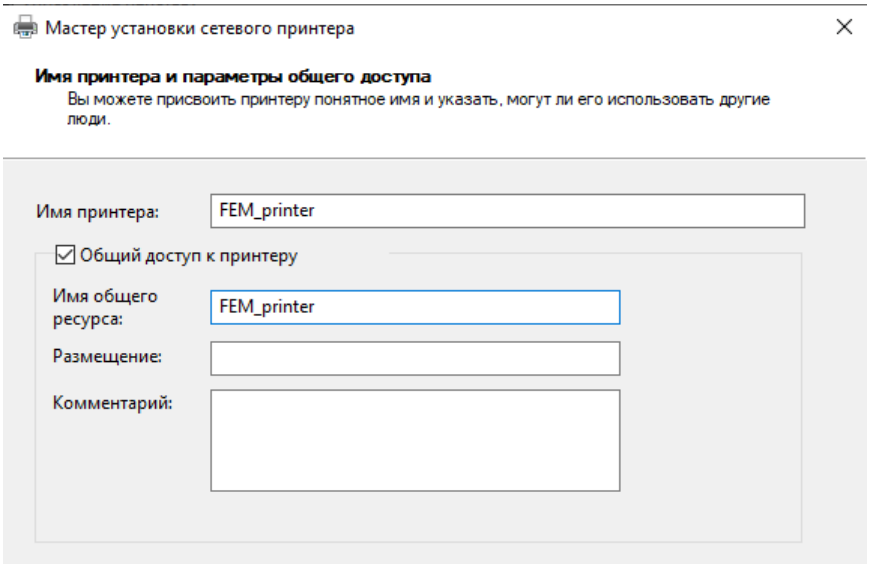


Рис. Е.6. Налаштування назви принтера

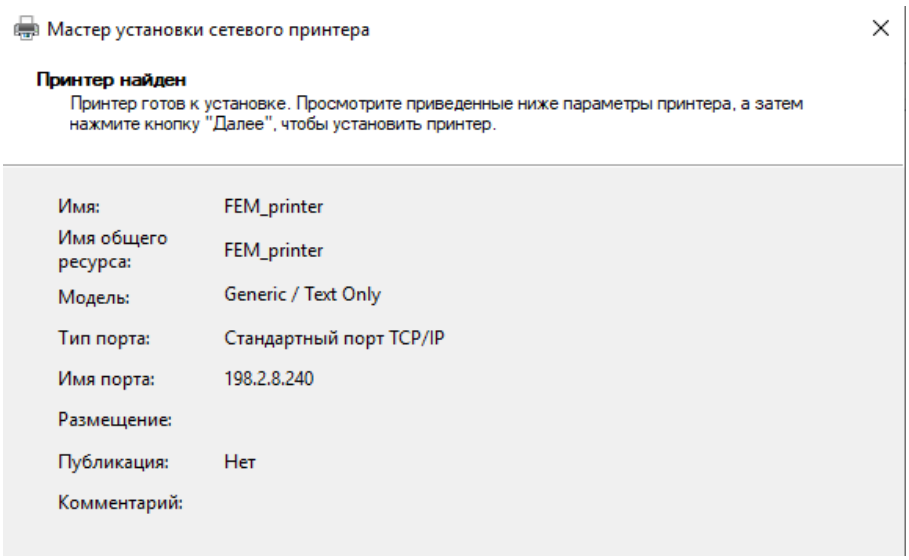


Рис. Е.7. Налаштований принтера

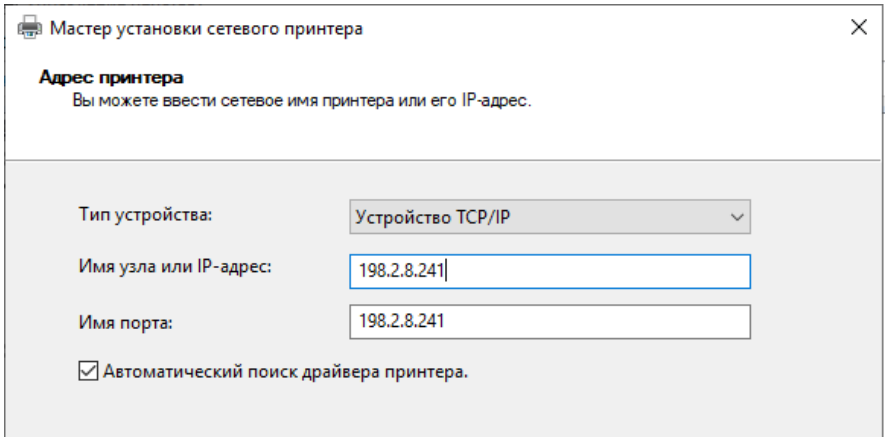


Рис. Е.8. Налаштування IP-адреси принтера

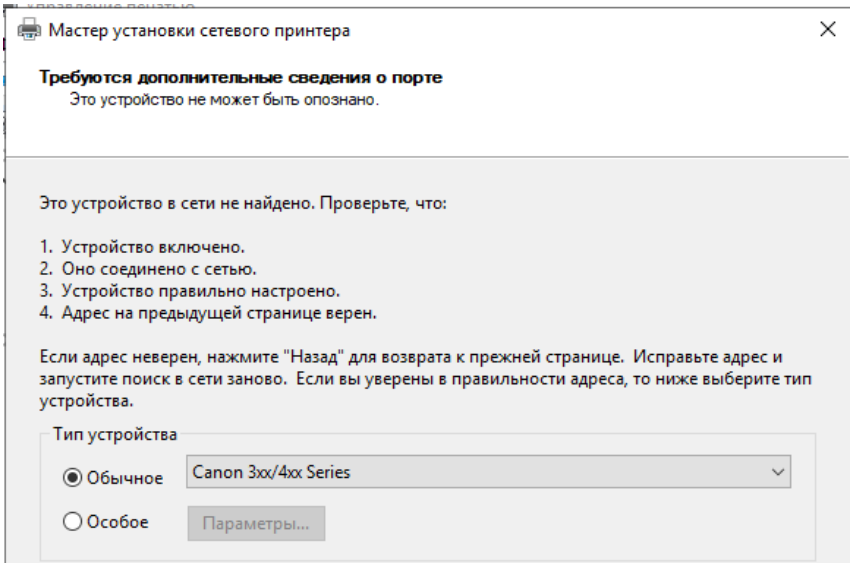


Рис. Е.9. Налаштування порта принтера

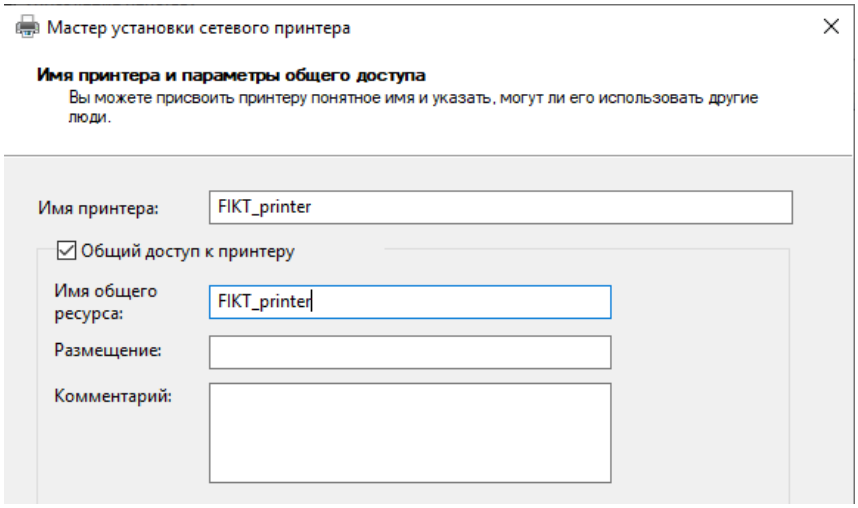


Рис. Е.10. Налаштування назви принтера

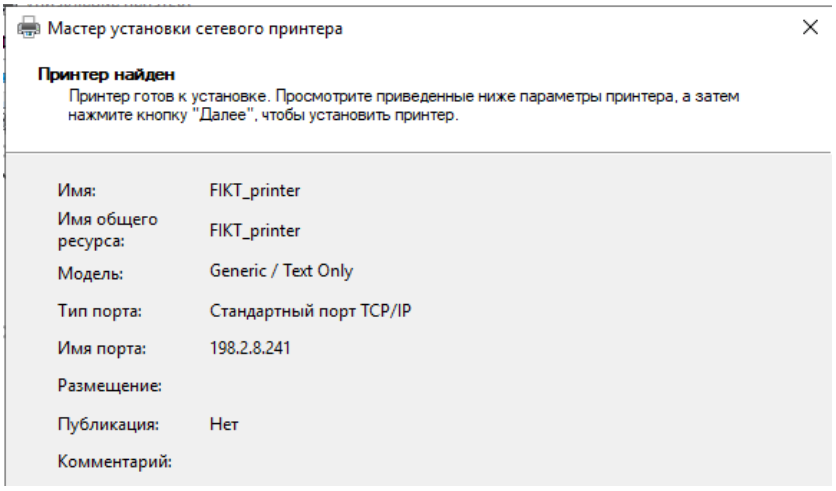


Рис. Е.11. Налаштований принтера

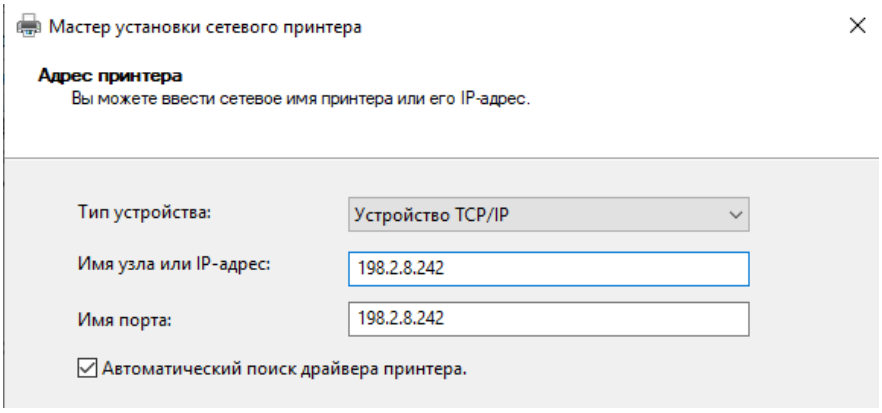


Рис. Е.12. Налаштування IP-адреси принтера

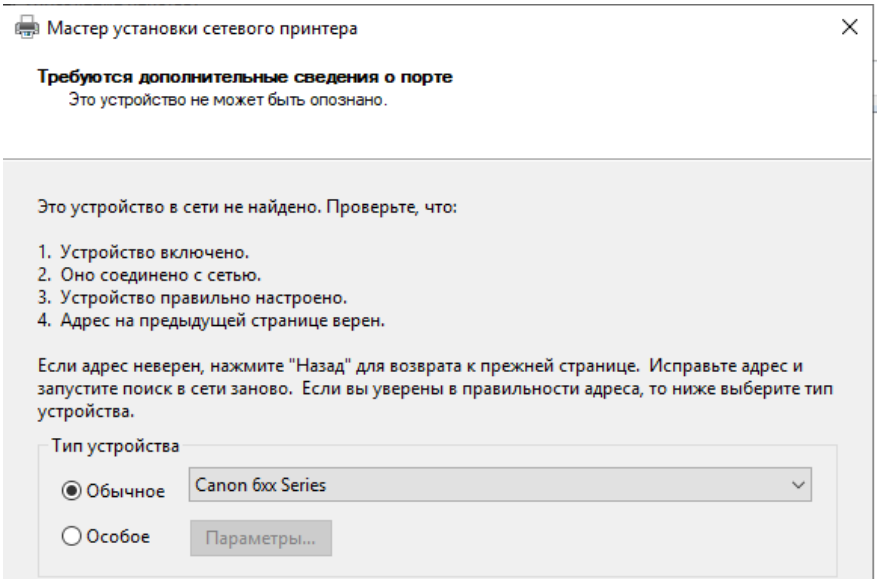


Рис. Е.13. Налаштування порта принтера

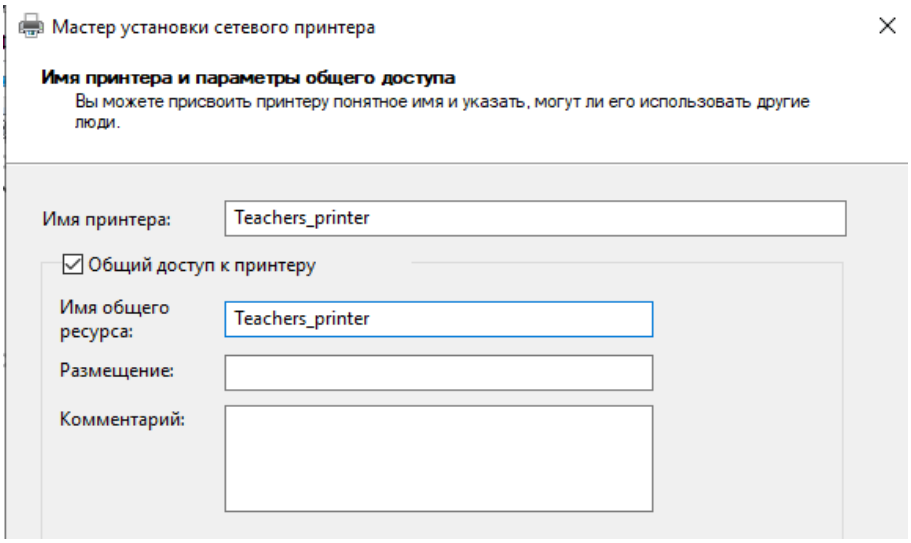


Рис. Е.14. Налаштування назви принтера

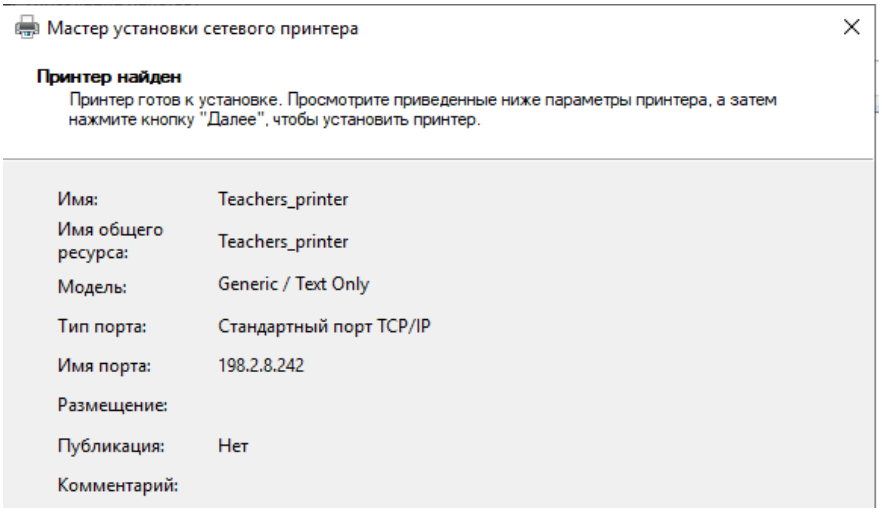


Рис. Е.15. Налаштований принтера

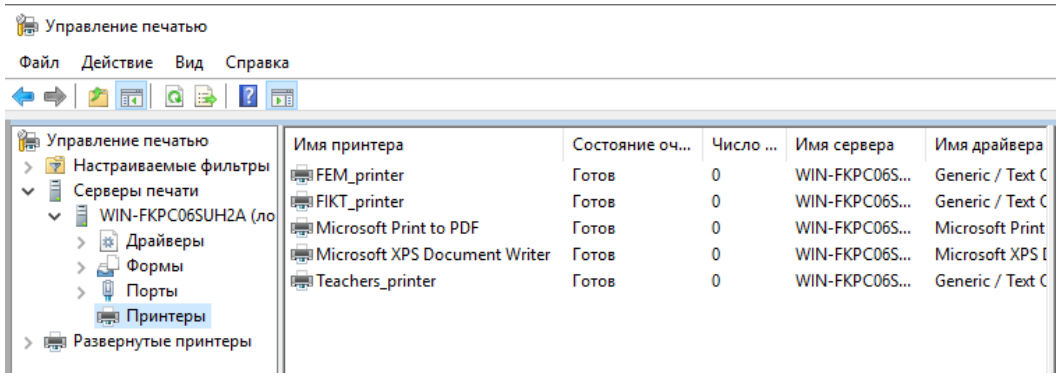


Рис. Е.16. Налаштовані принтери

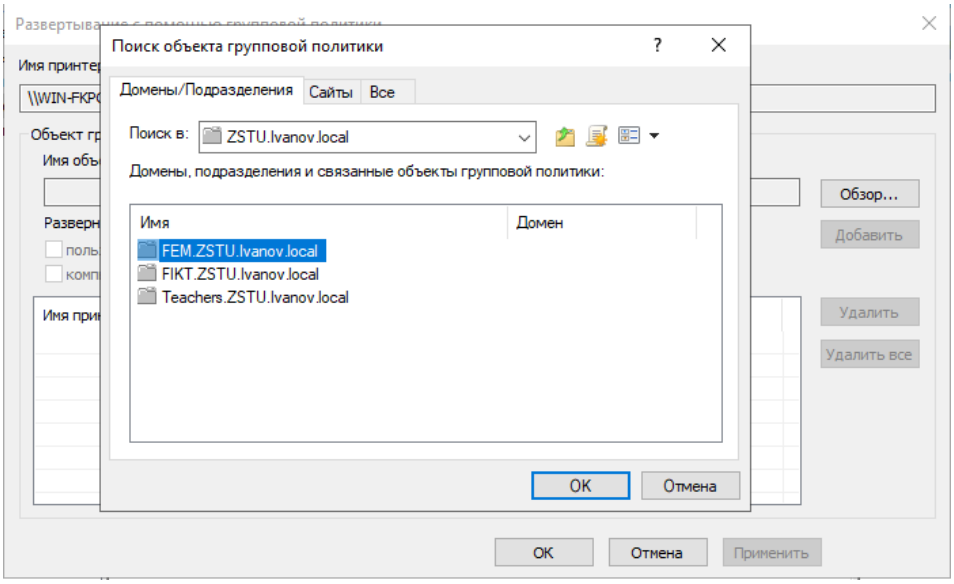


Рис. Е.17. Налаштування групової політики принтера

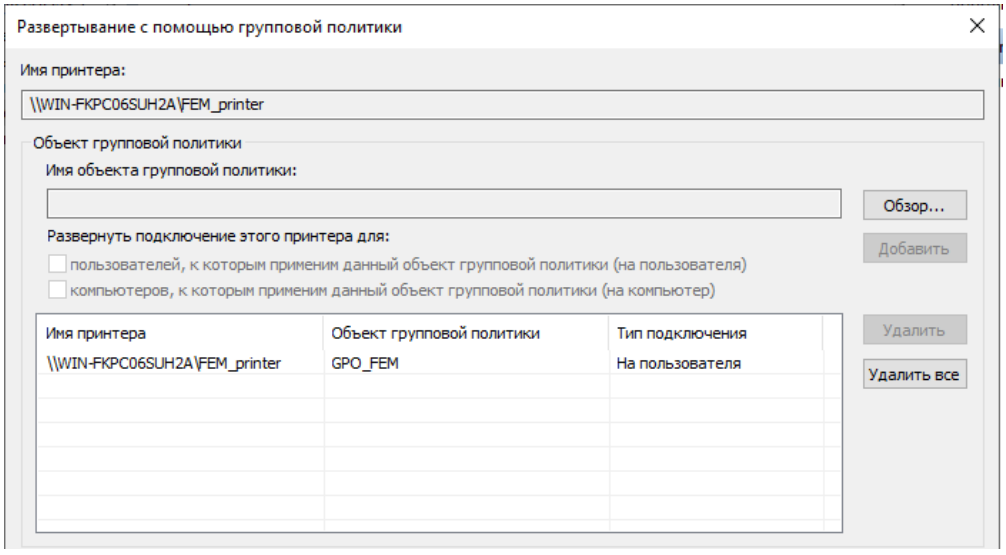


Рис. Е.18. Налаштована групова політика принтера

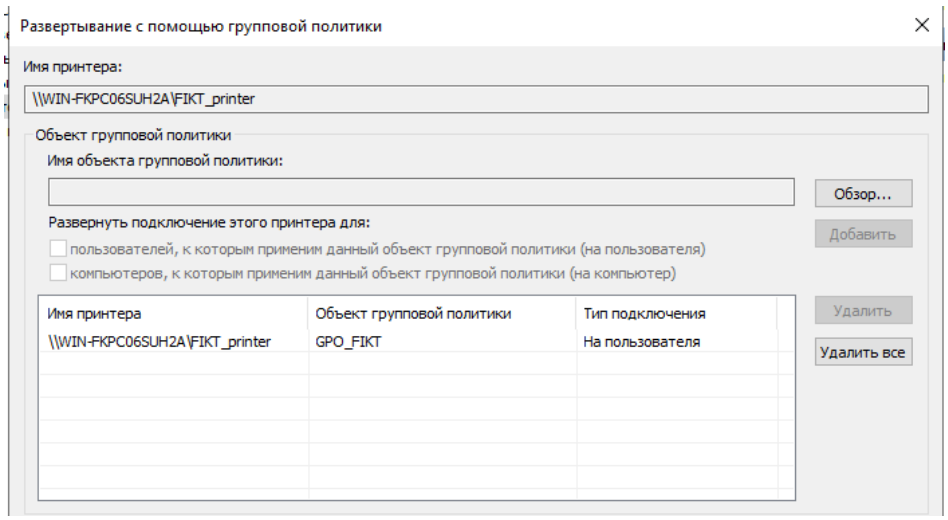


Рис. Е.19. Налаштована групова політика принтера

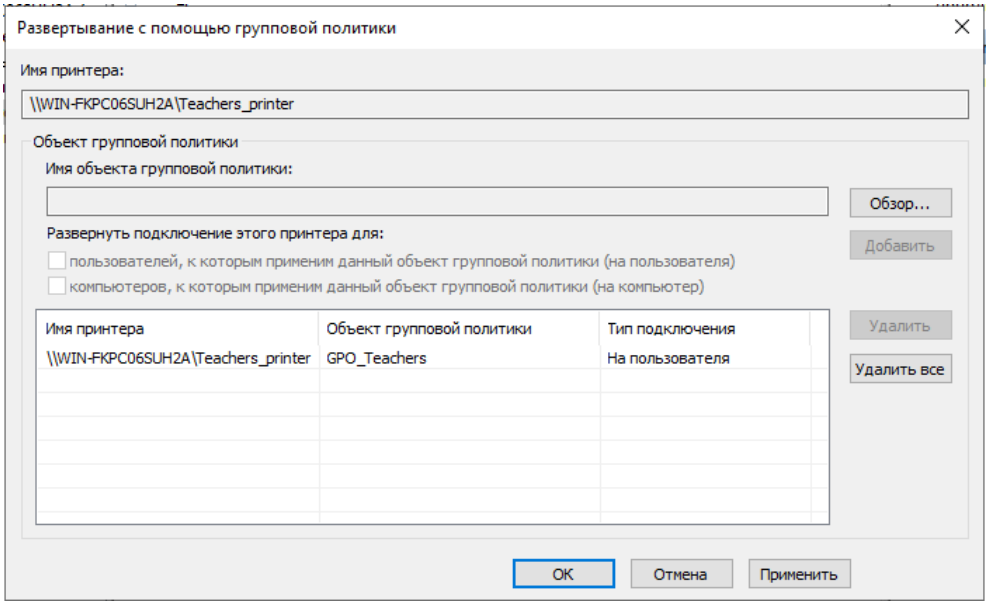


Рис. Е.20. Налаштована групова політика принтера

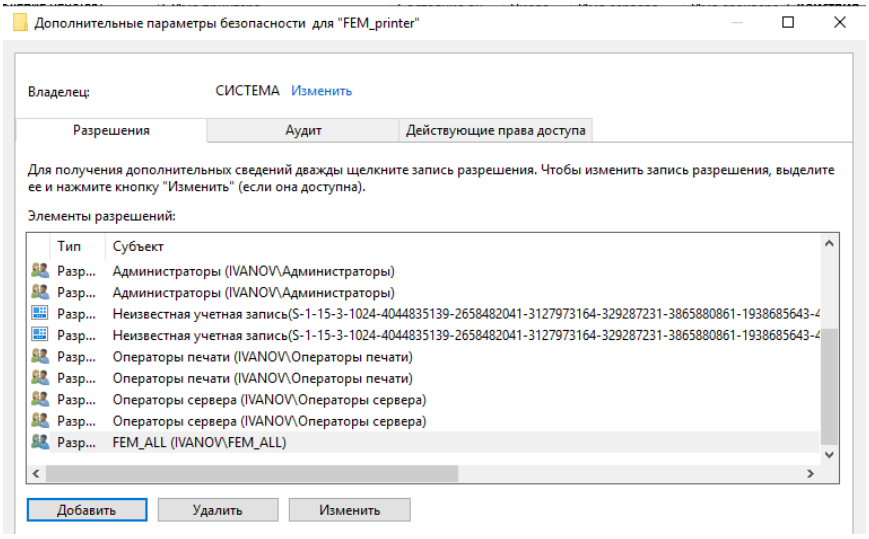


Рис. Е.21. Поширення принтера на певну групу користувачів

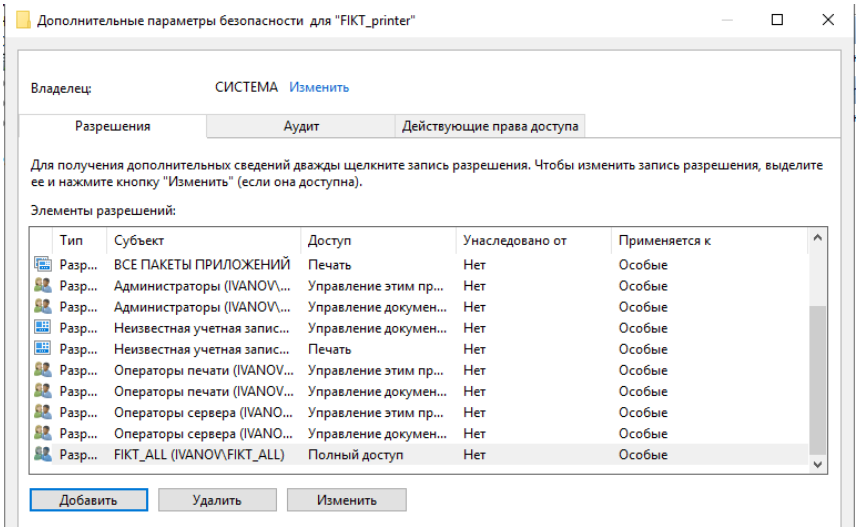


Рис. Е.22. Поширення принтера на певну групу користувачів

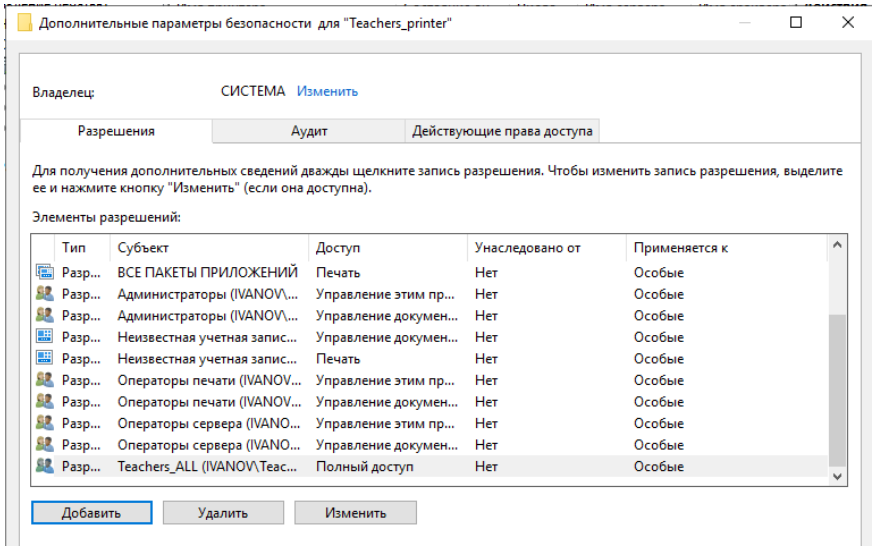


Рис. Е.23. Поширення принтера на певну групу користувачів

ДОДАТОК Є

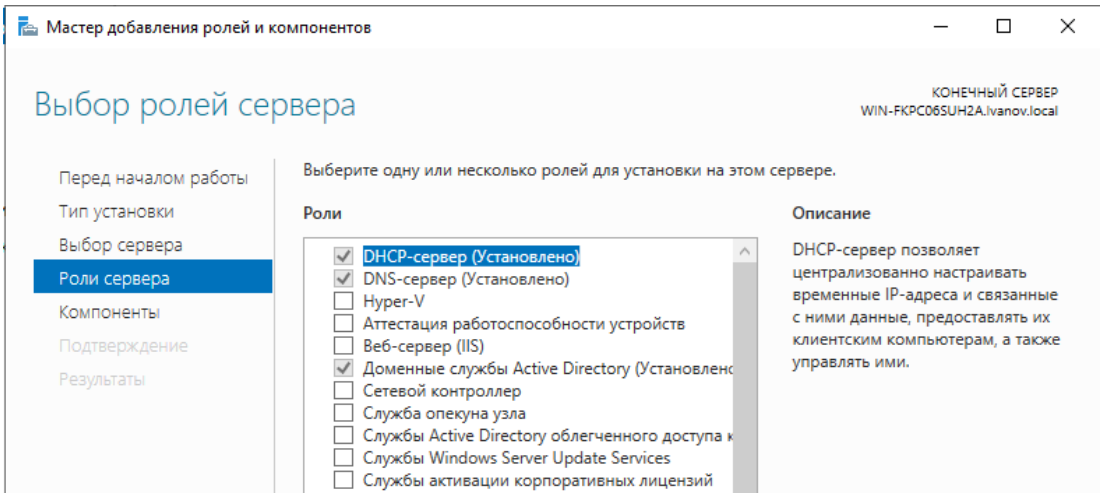


Рис. Є.1. Вибір ролі сервера

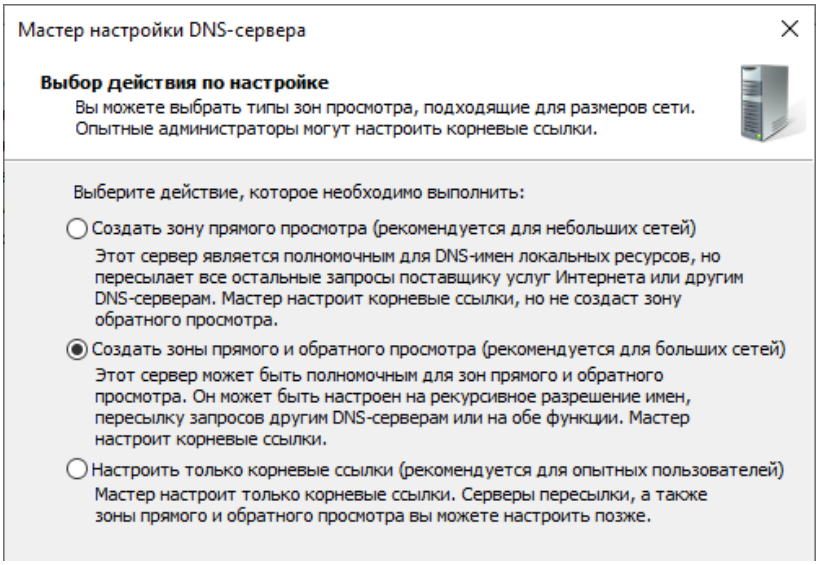


Рис. Є.2. Налаштування DNS

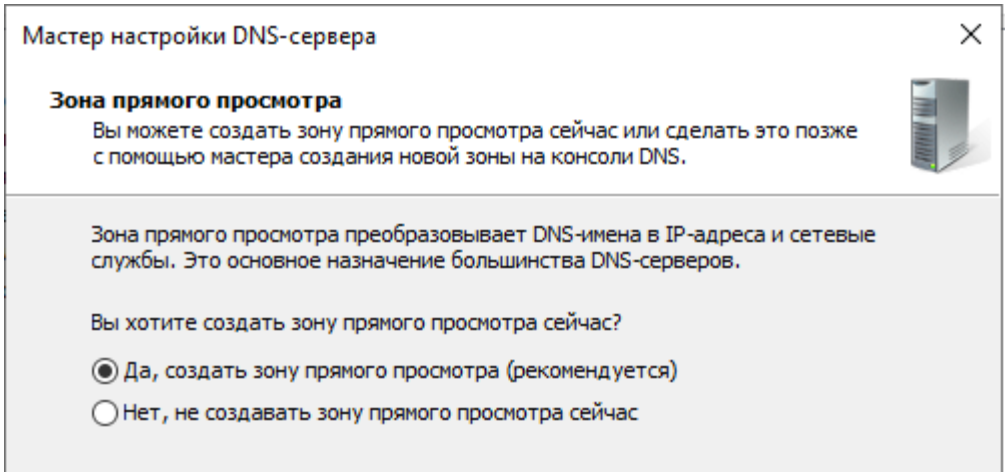


Рис. Є.3. Створення прямої зони перегляду

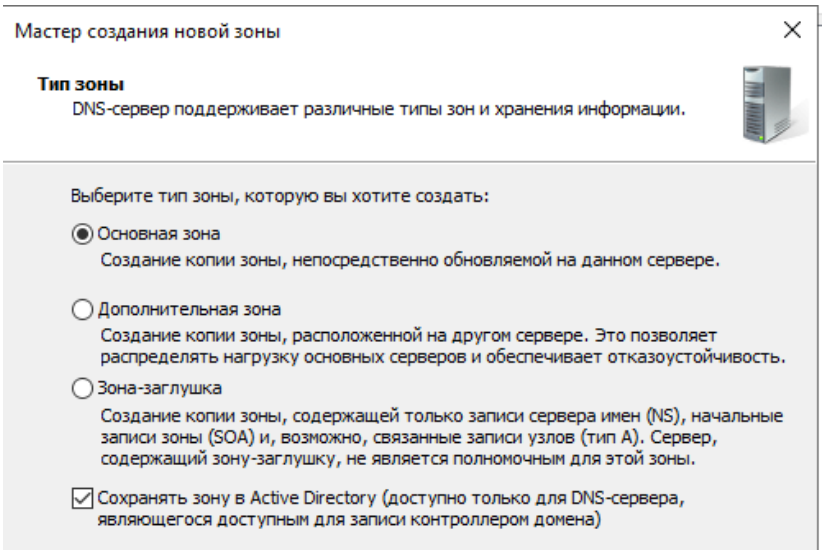


Рис. Є.4. Налаштування прямої зони перегляду

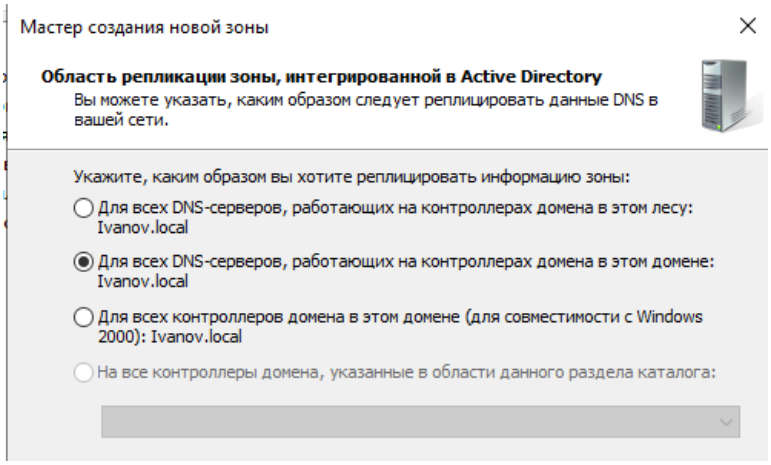


Рис. Є.5. Налаштування прямої зони перегляду

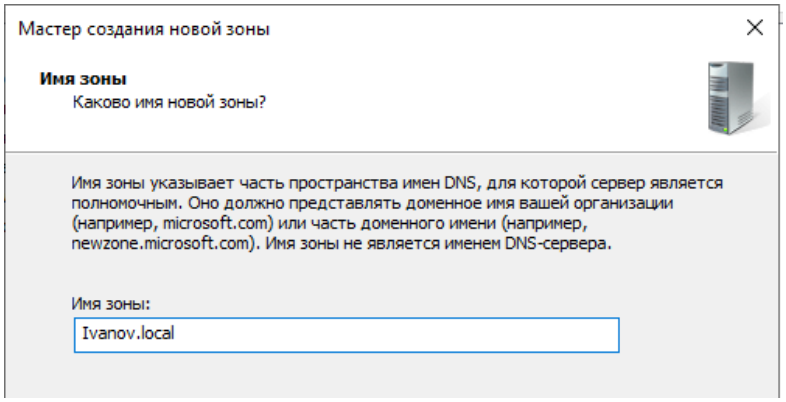


Рис. Є.6. Налаштування імені прямої зони перегляду

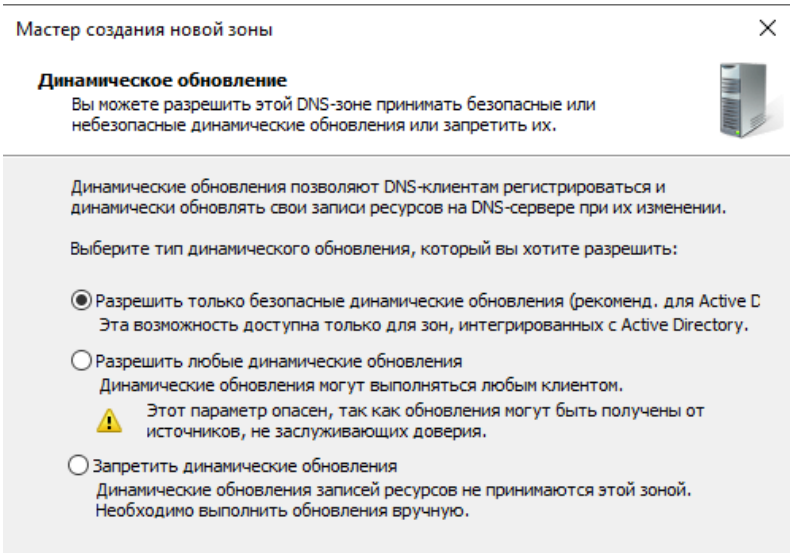


Рис. Є.7. Налаштування прямої зони перегляду

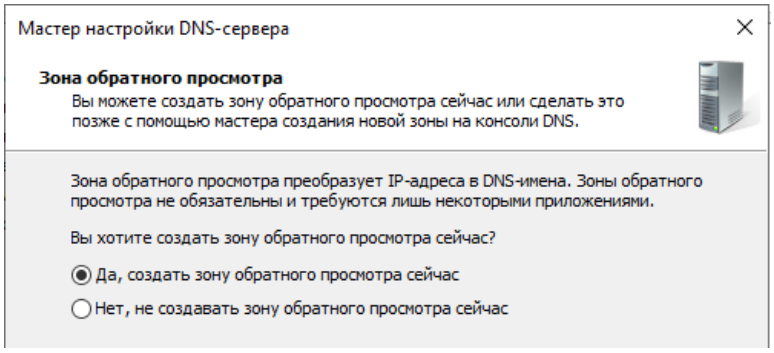


Рис. Є.8. Налаштування зворотньої зони перегляду

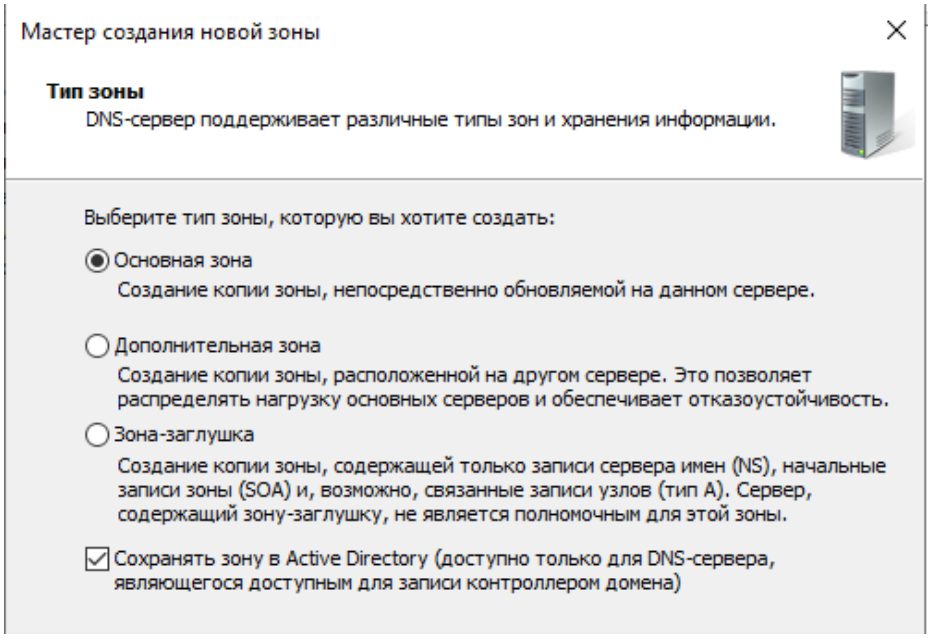


Рис. Є.9. Налаштування зворотньої зони перегляду

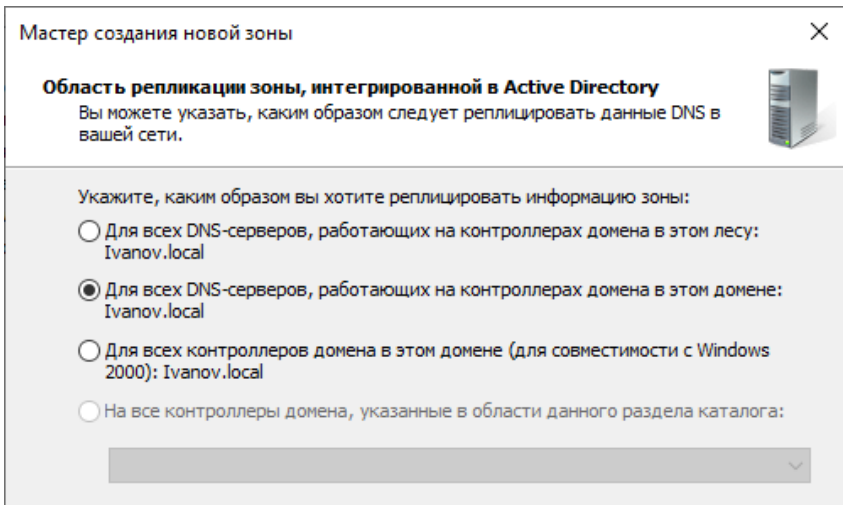


Рис. Є.10. Налаштування зворотньої зони перегляду

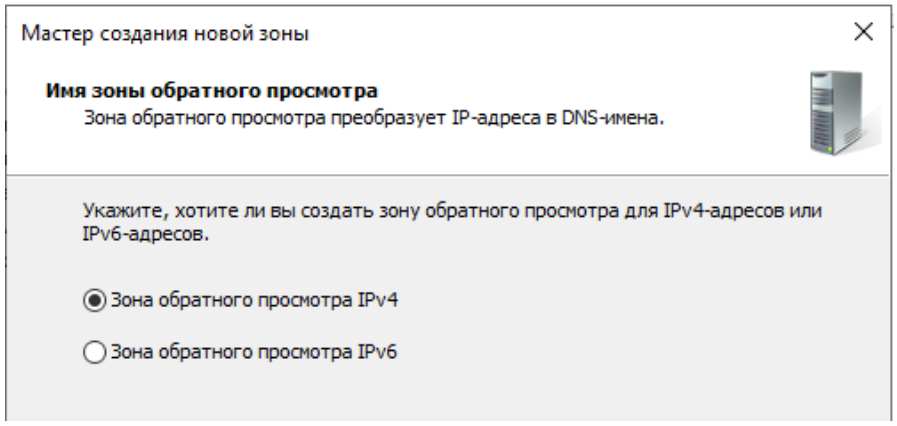


Рис. Є.11. Налаштування зворотньої зони перегляду

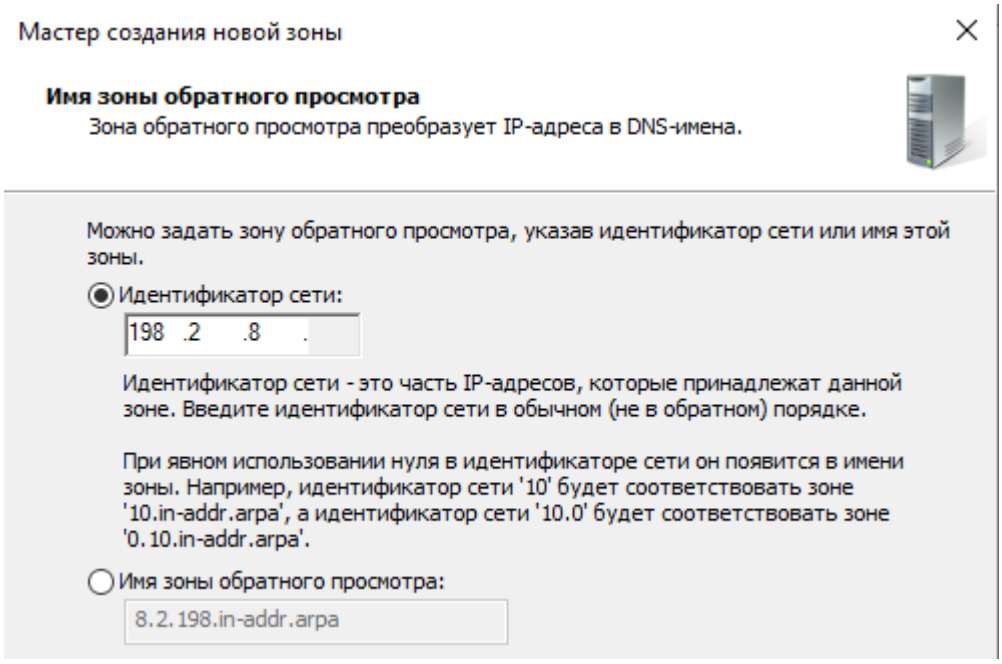


Рис. Є.12. Налаштування зворотньої зони перегляду

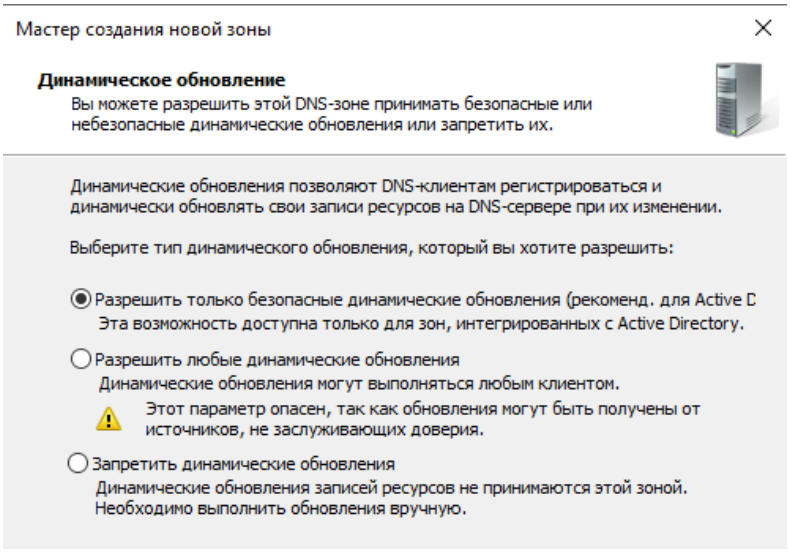


Рис. Є.13. Налаштування зворотньої зони перегляду

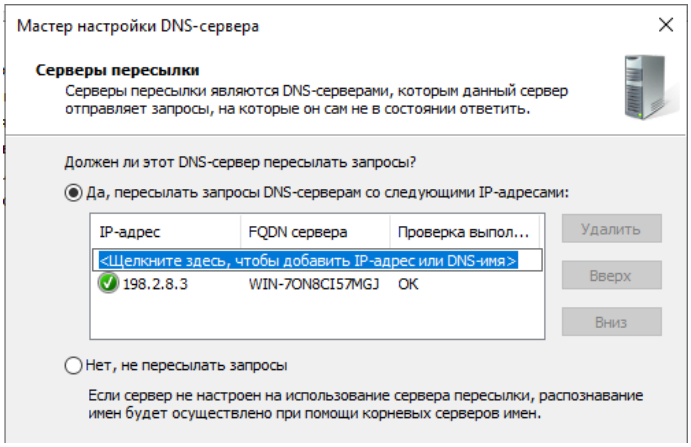


Рис. Є.14. Налаштування зворотньої зони перегляду

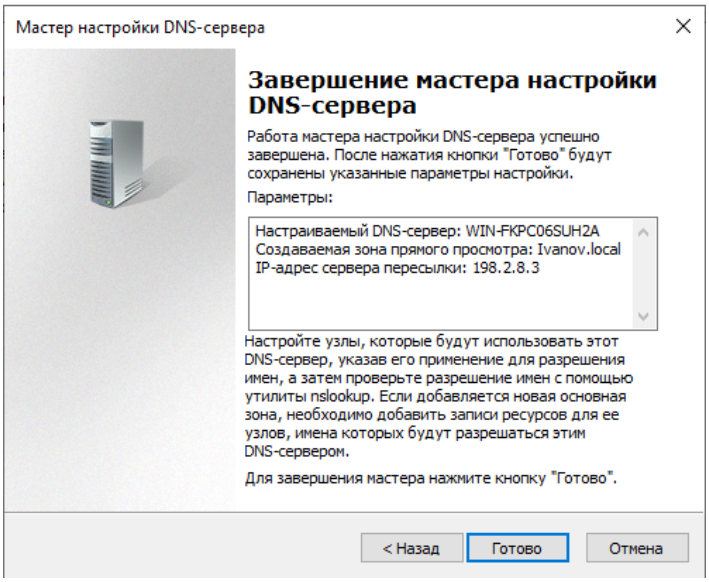


Рис. Є.15. Налаштований DNS

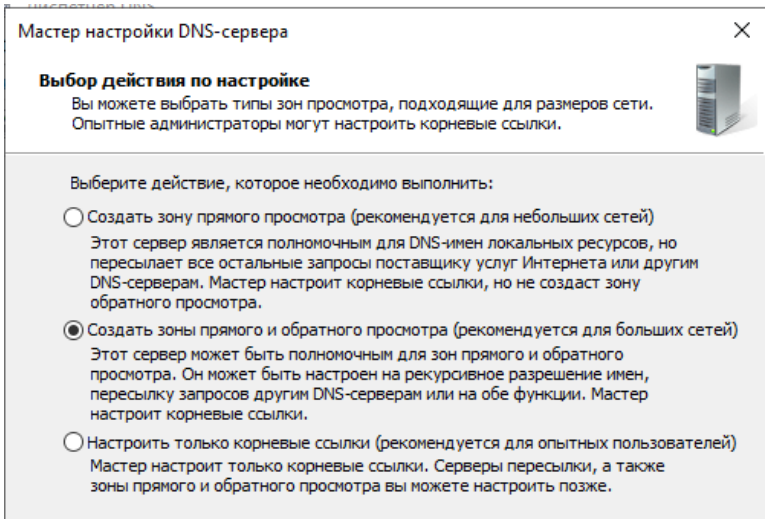


Рис. Є.16. Налаштування DNS на альтернативному сервері

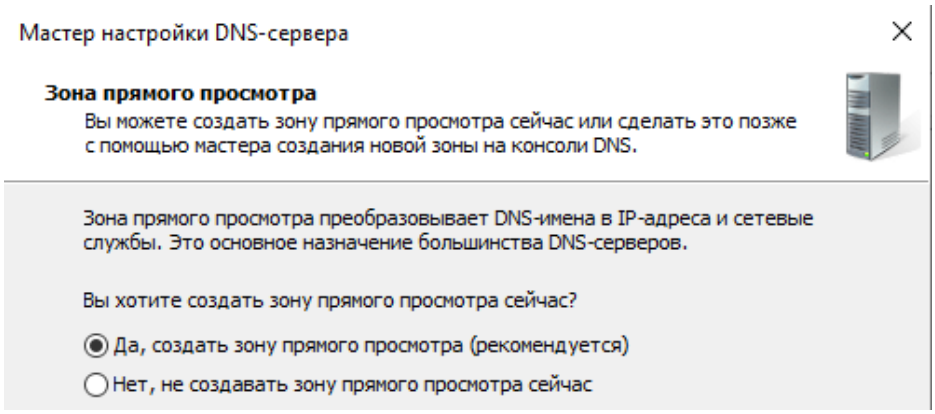


Рис. Є.17. Налаштування DNS на альтернативному сервері

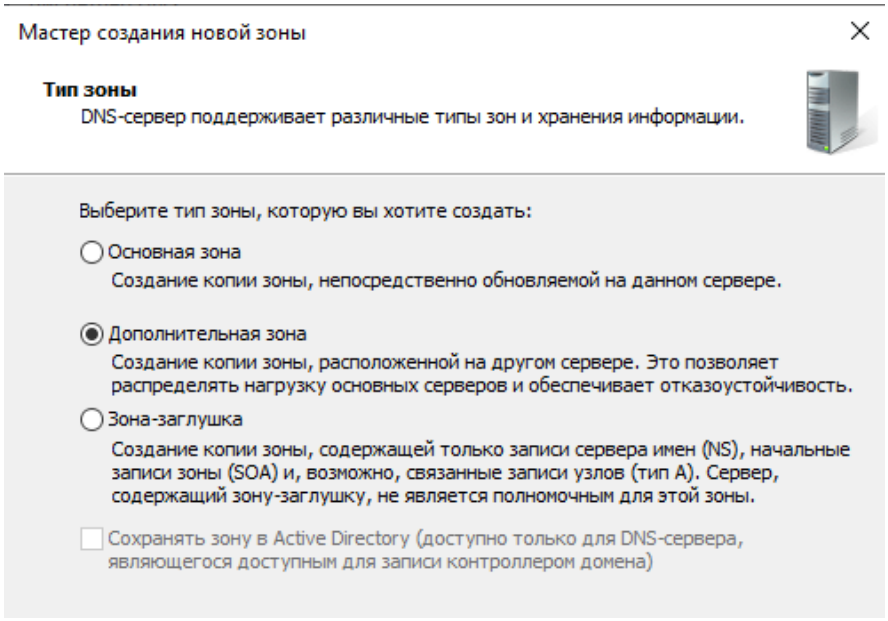


Рис. Є.18. Налаштування DNS на альтернативному сервері

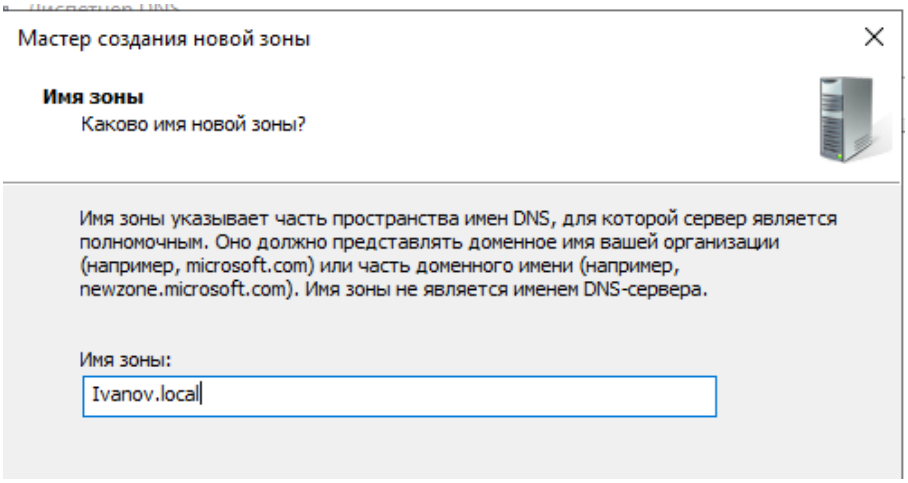


Рис. Є.19. Налаштування DNS на альтернативному сервері

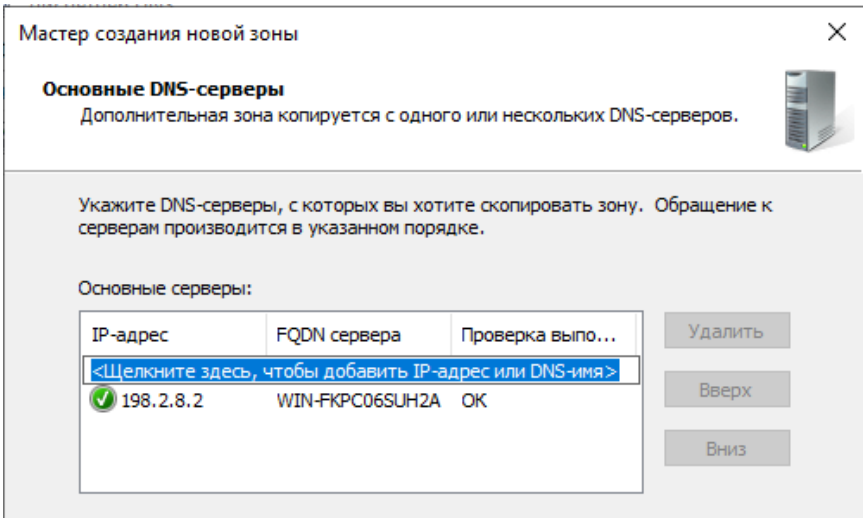


Рис. Є.20. Налаштування DNS на альтернативному сервері

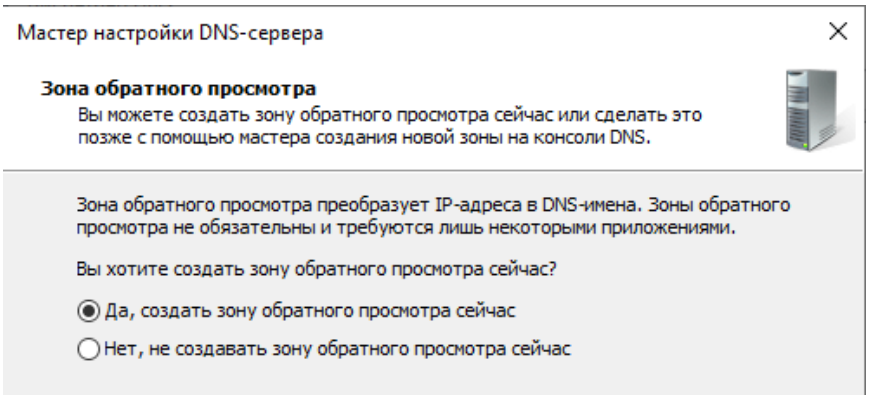


Рис. Є.21. Налаштування DNS на альтернативному сервері

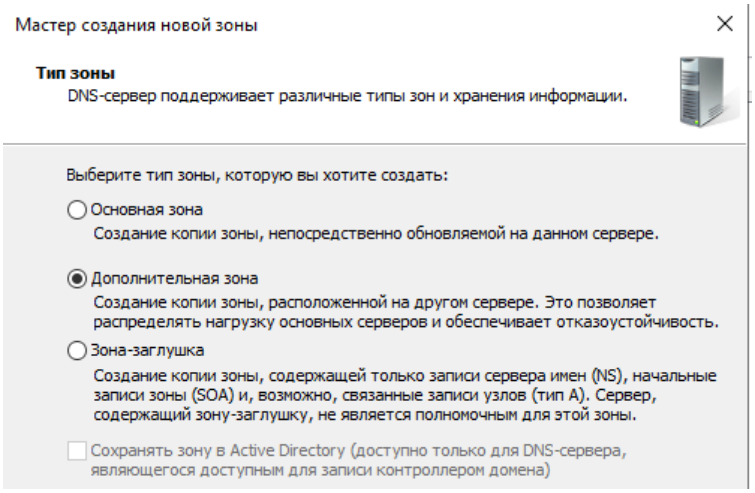


Рис. Є.22. Налаштування DNS на альтернативному сервері

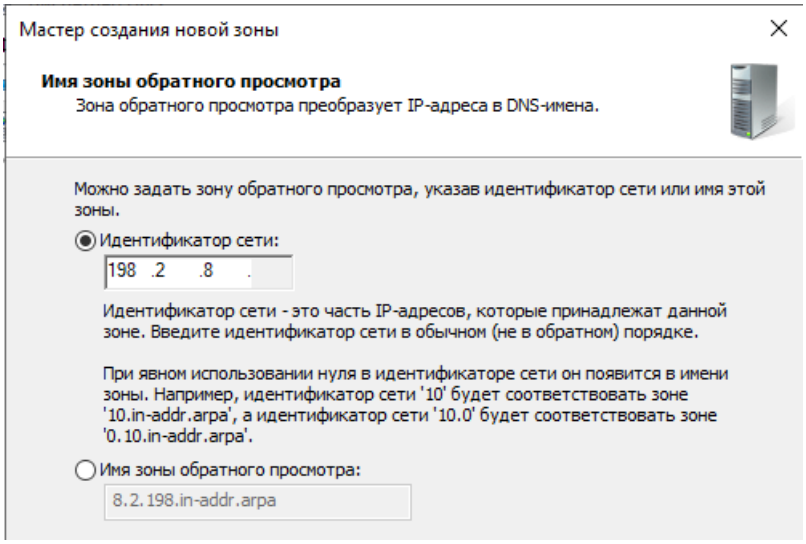


Рис. Є.23. Налаштування DNS на альтернативному сервері

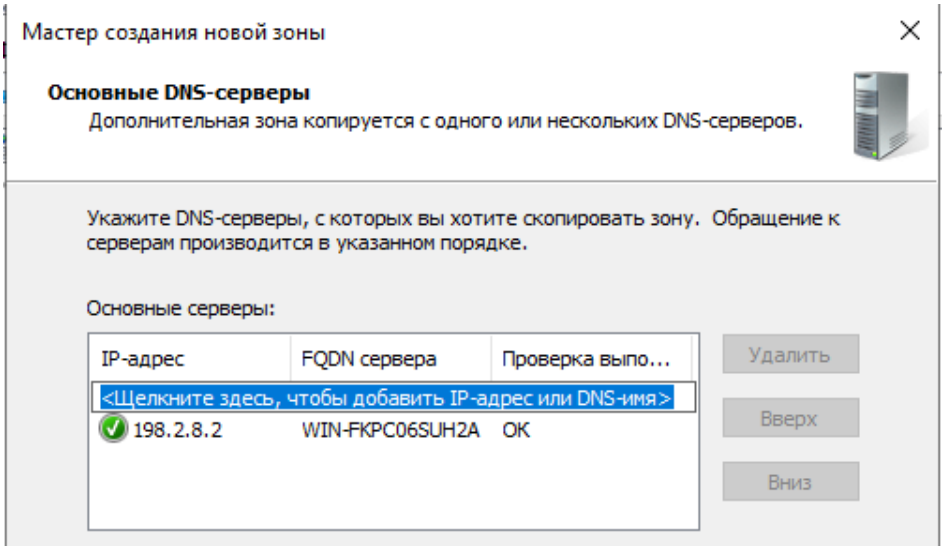


Рис. Є.24. Налаштування DNS на альтернативному сервері

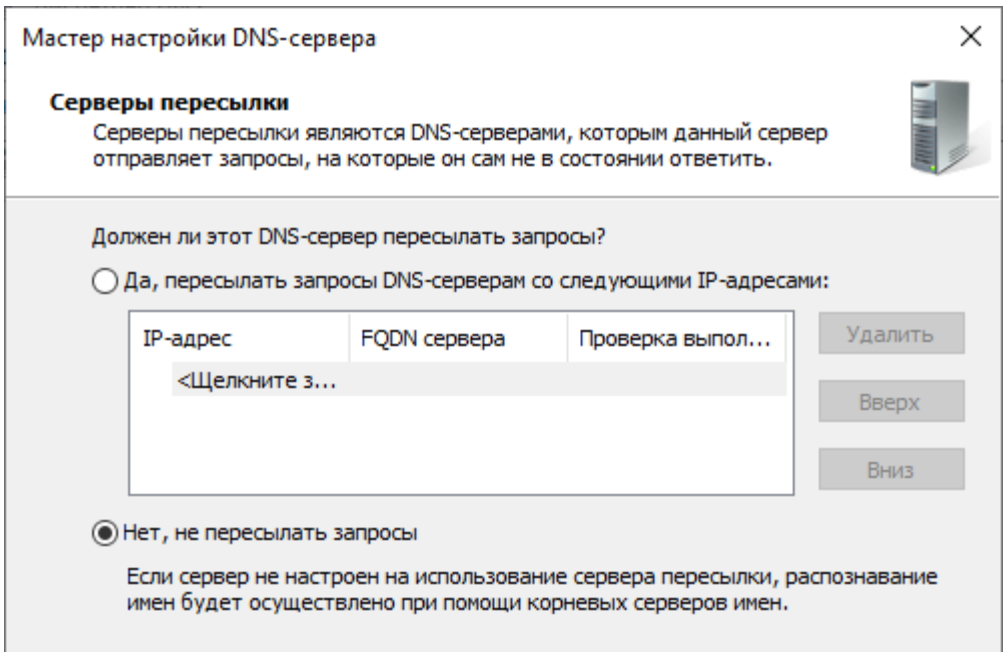


Рис. Є.25. Налаштування DNS на альтернативному сервері

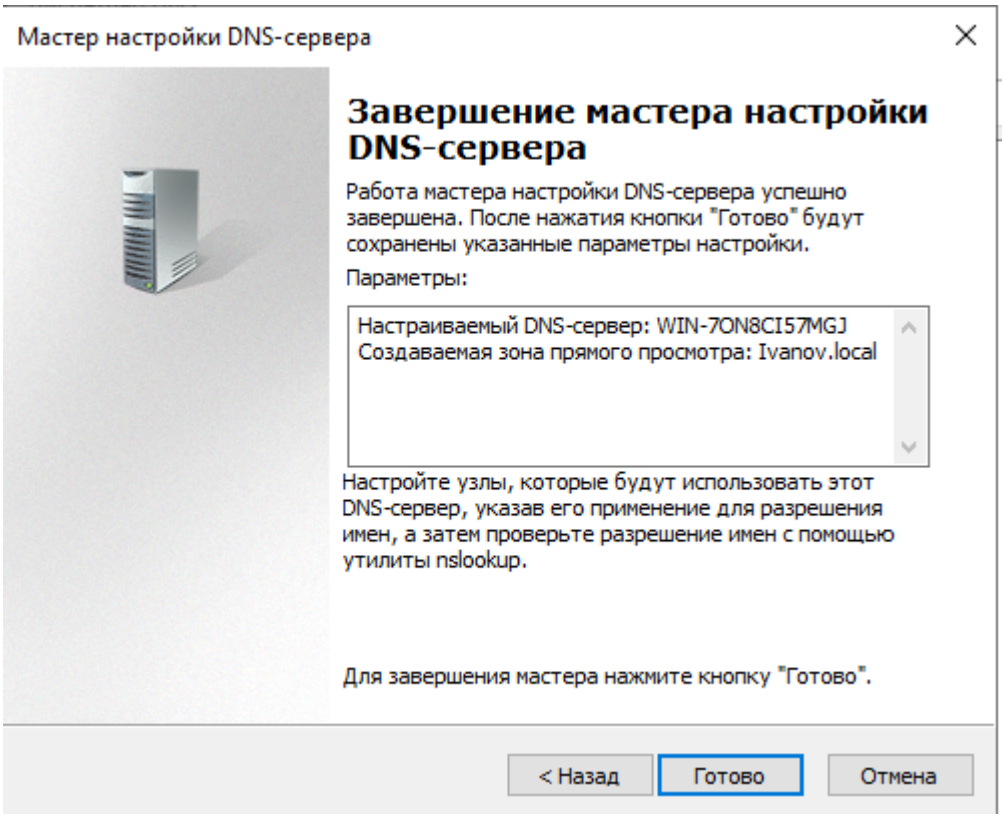


Рис. Є.26. Налаштований DNS на альтернативному сервері

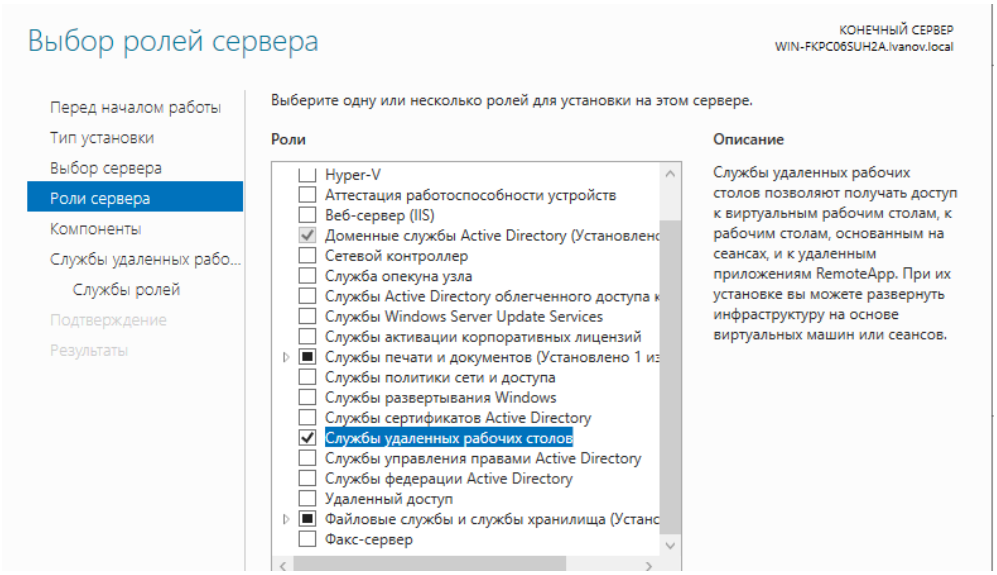


Рис. Ж.1. Вибір ролі сервера

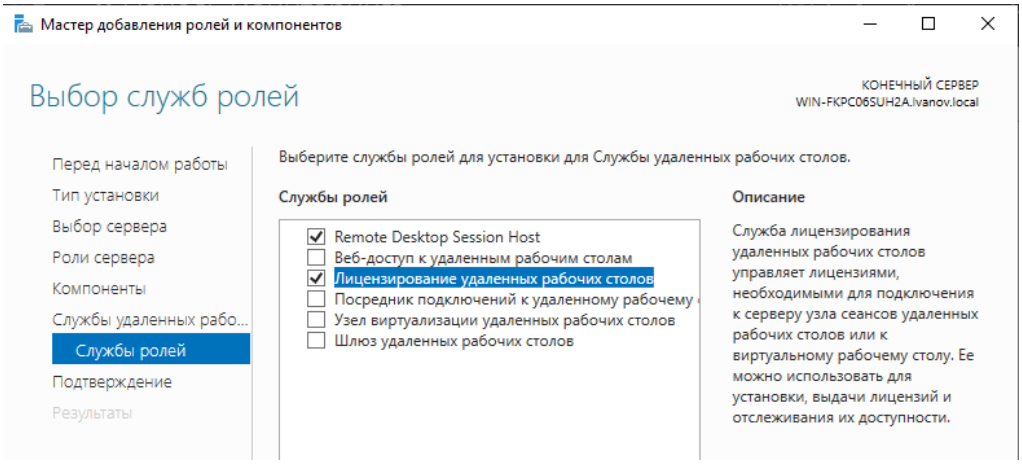


Рис. Ж.2. Вибір служби ролей сервера

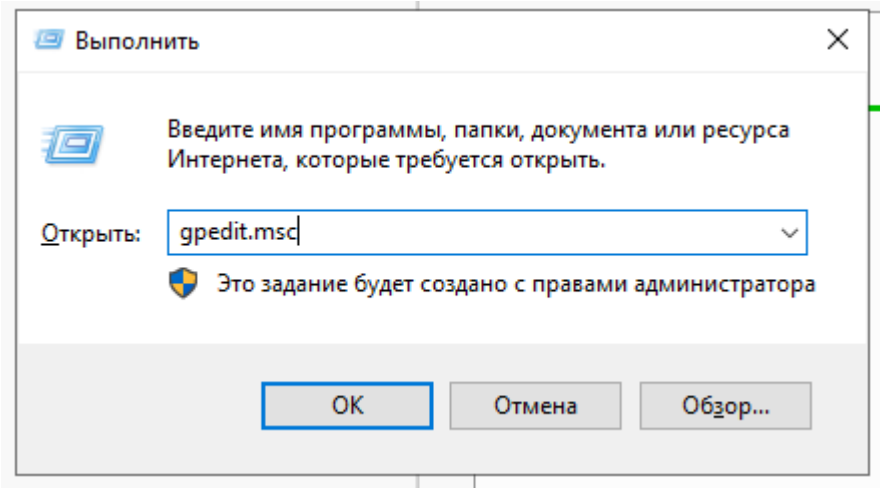


Рис. Ж.3. Виклик локалькоїгрупової політки сервера

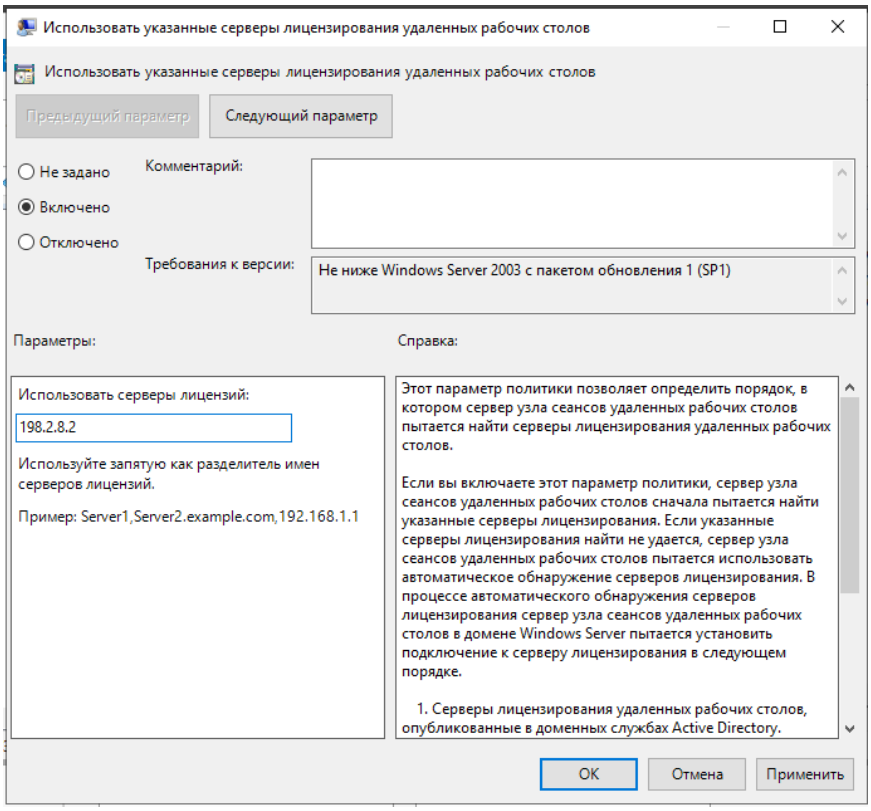


Рис. Ж.4. Налаштування локальної групової політики

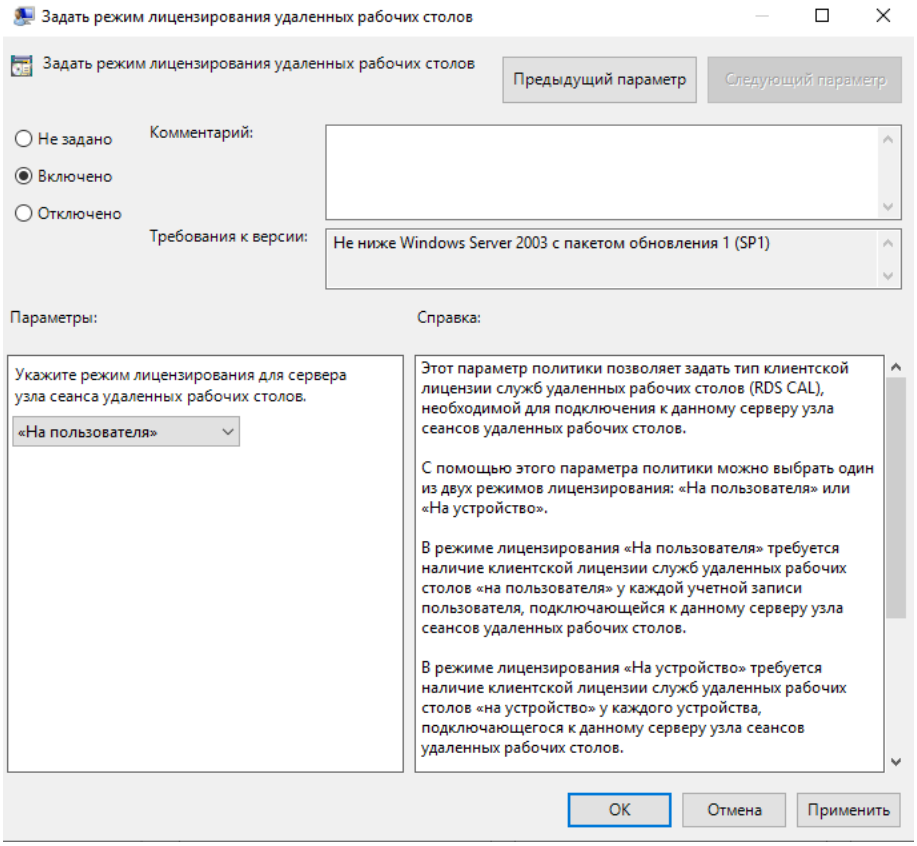


Рис. Ж.5. Налаштування локальної групової політики

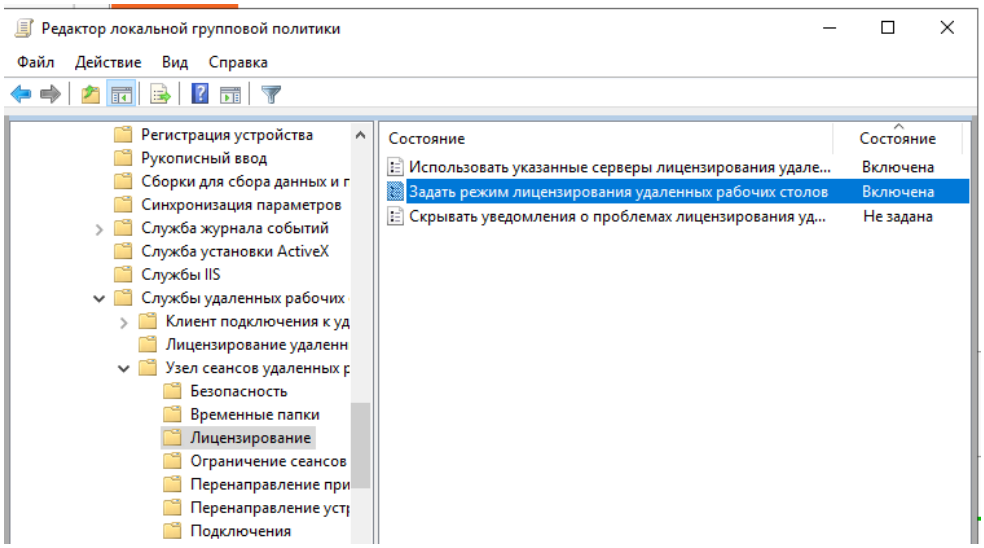


Рис. Ж.6. Налаштована локальна групова політика

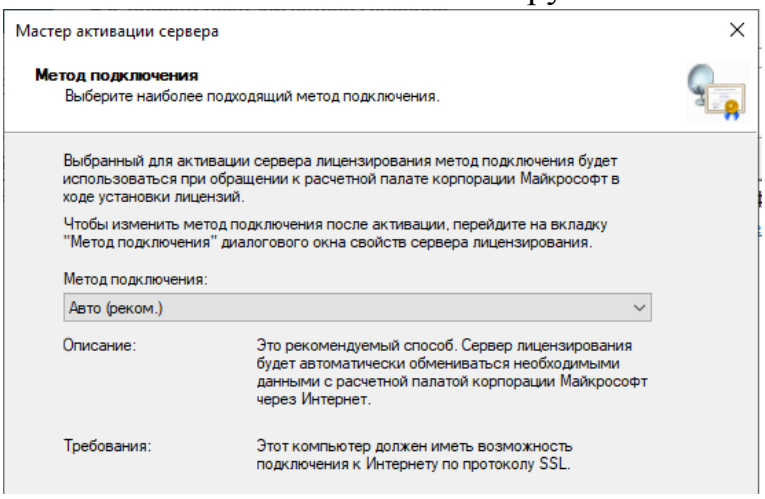


Рис. Ж.7. Активація сервера

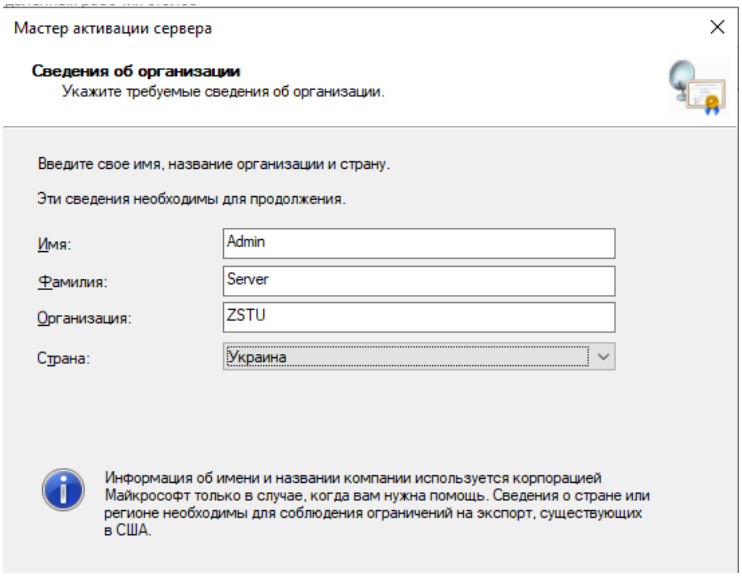


Рис. Ж.8. Активація сервера

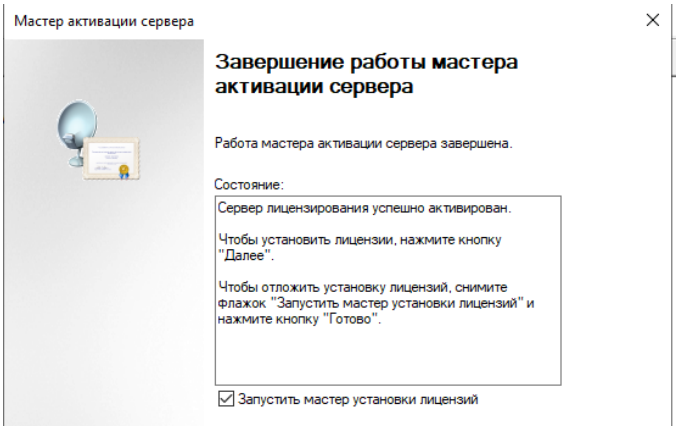


Рис. Ж.9. Завершення активації сервера

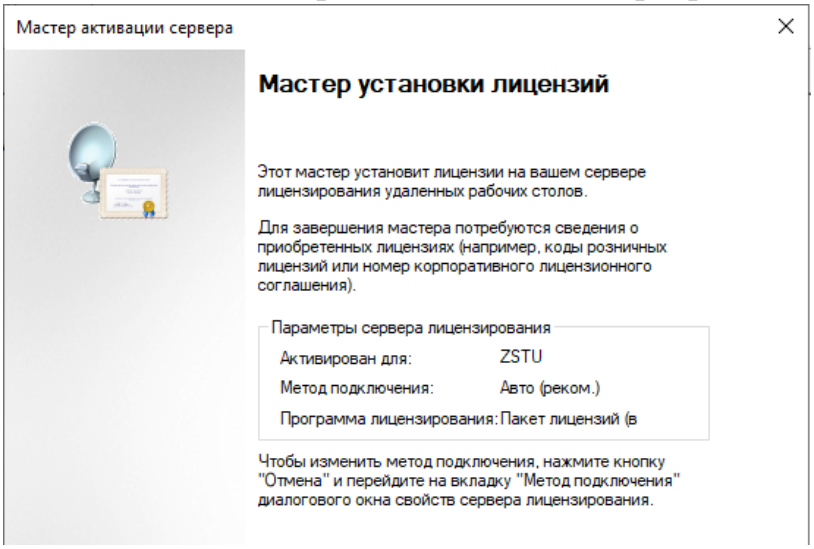


Рис. Ж.10. Установка ліцензії сервера

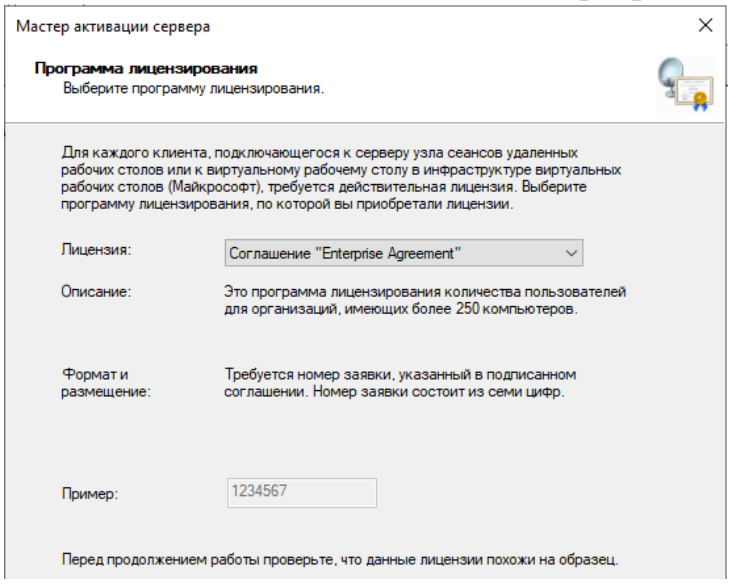


Рис. Ж.11. Установка ліцензії сервера

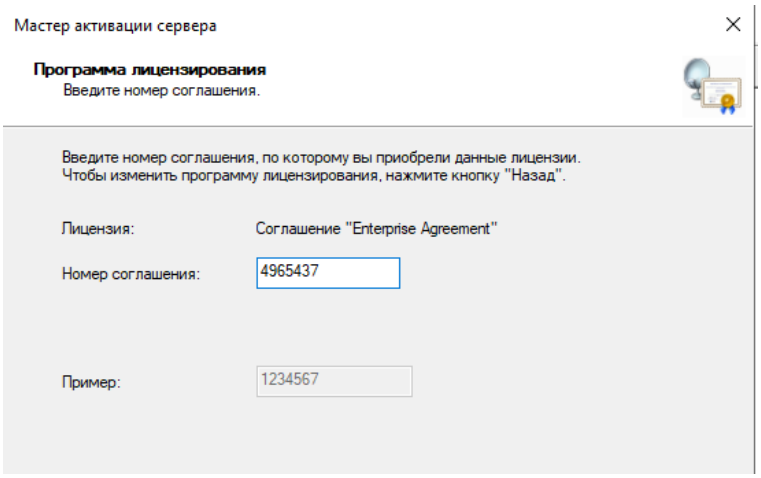


Рис. Ж.12. Установка ліцензії сервера

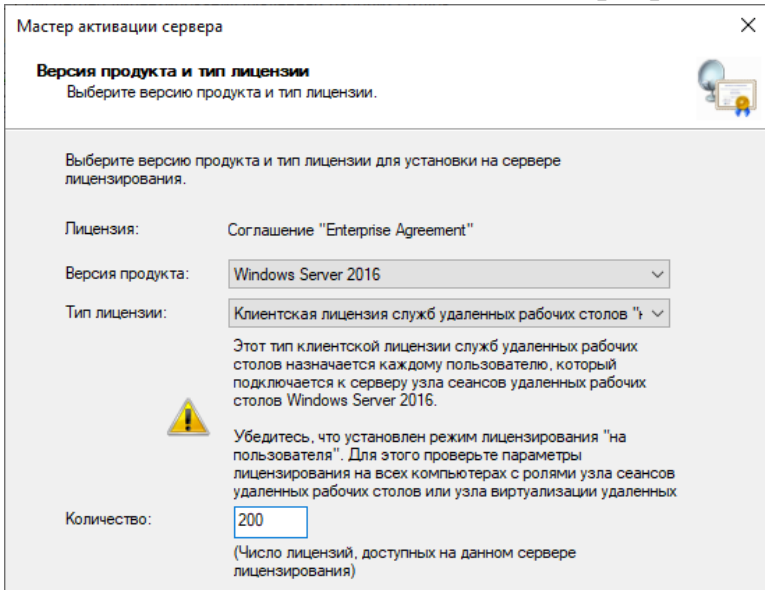


Рис. Ж.13. Установка ліцензії сервера

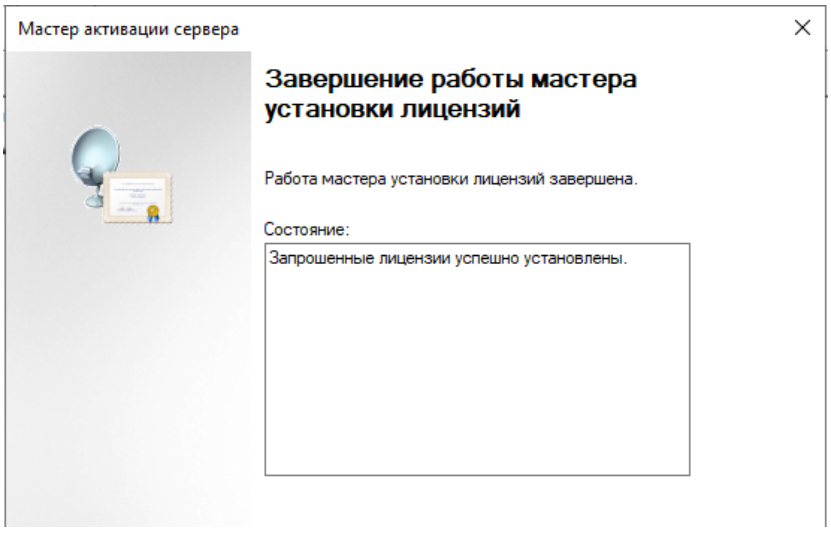


Рис. Ж.14. Заверешння установки ліцензії сервера

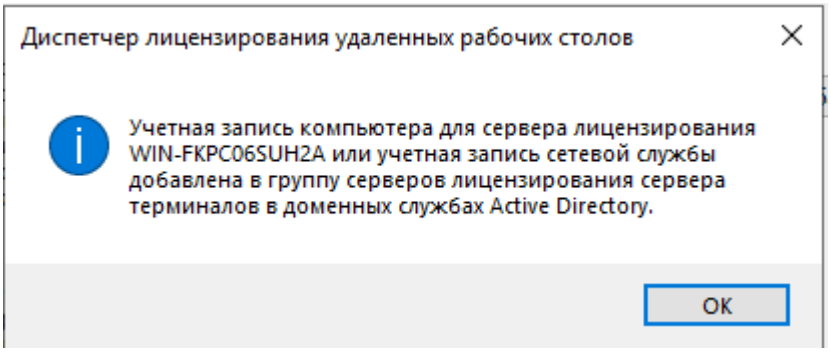


Рис. Ж.15. Додання сервера в групу серверів

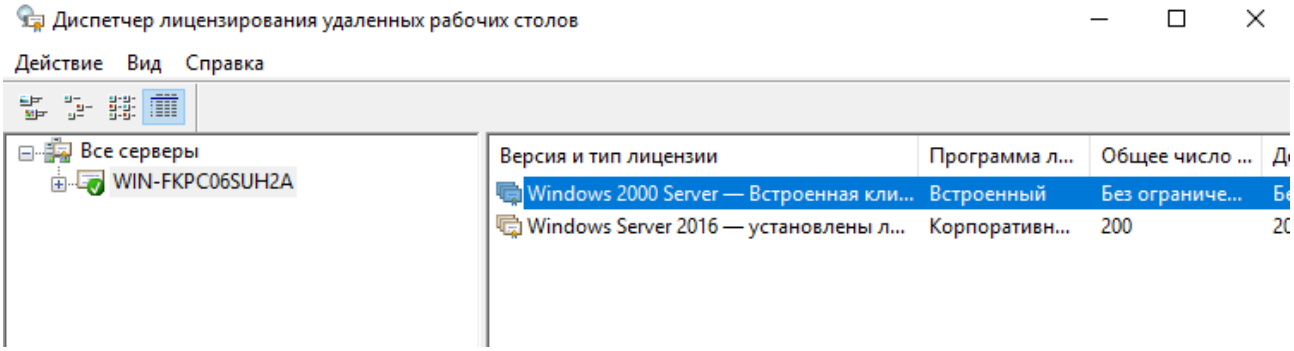


Рис. Ж.16. Налаштований сервер

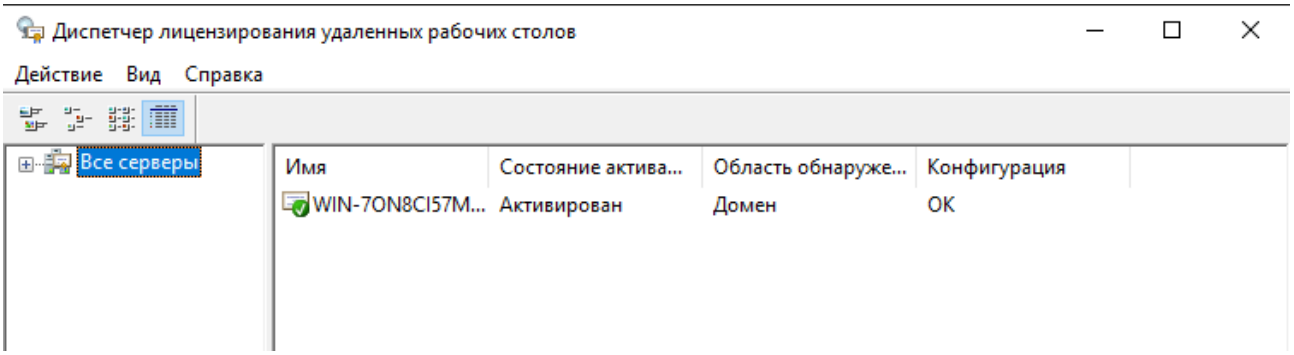


Рис. Ж.17. Налаштований сервер

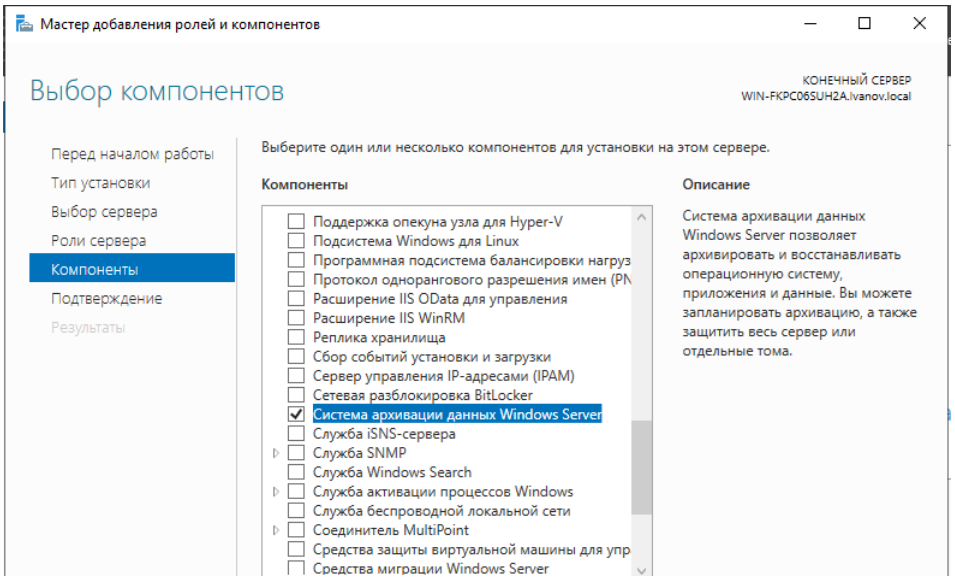


Рис. 3.1. Вибір ролі сервера

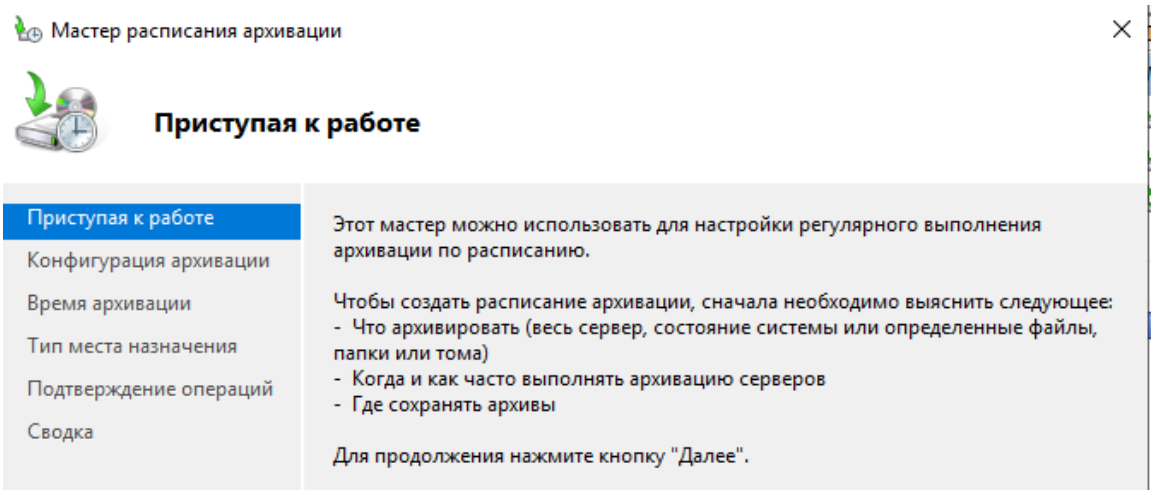


Рис. 3.2. Налаштування архівації сервера

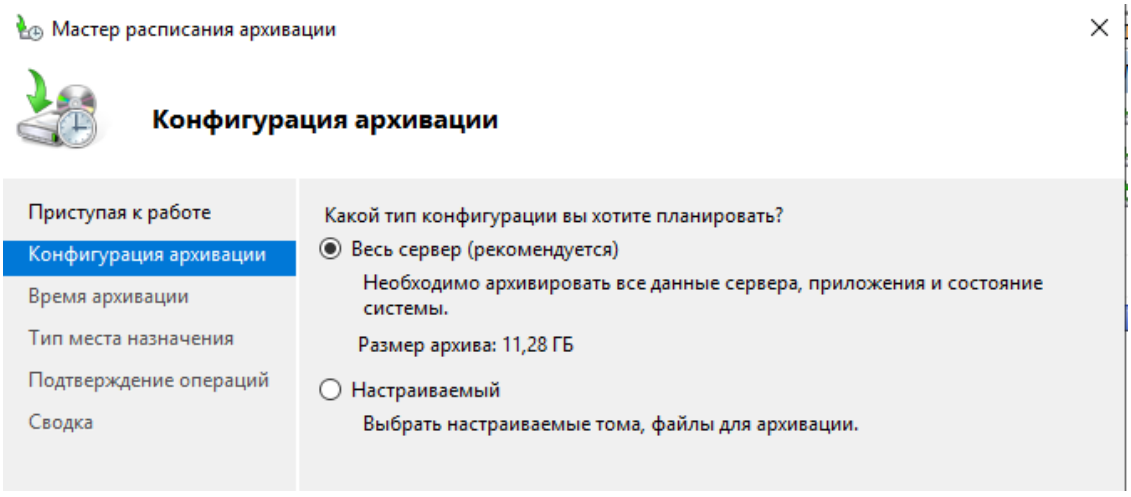


Рис. 3.3. Вибір типу архівації сервера

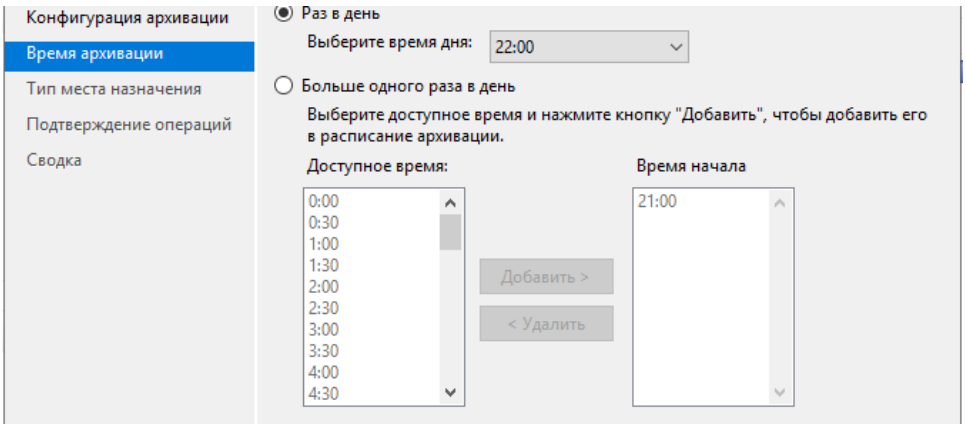


Рис. 3.4. Вибір часу архівації сервера

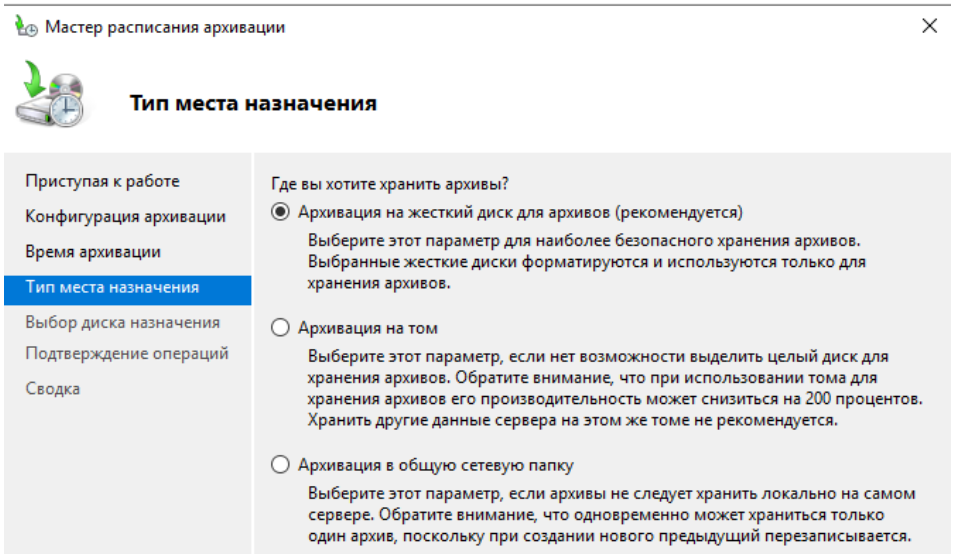


Рис. 3.5. Вибір місця для зберігання архіва сервера

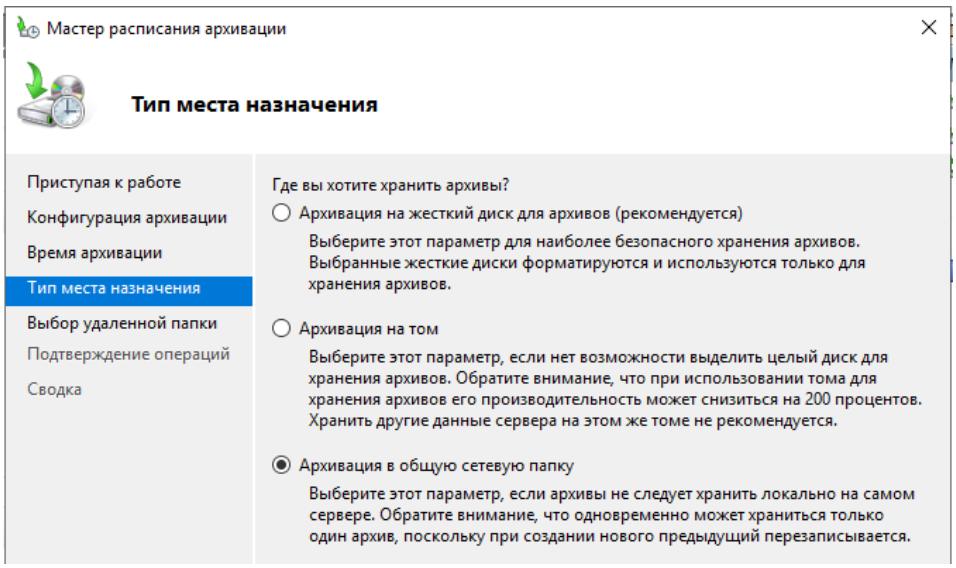


Рис. 3.6. Вибір місця для зберігання архіва сервера

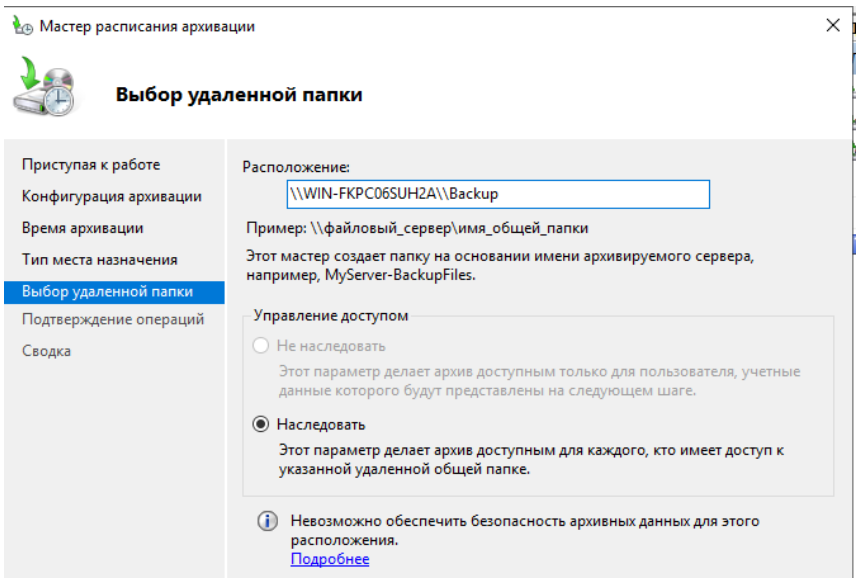


Рис. 3.7. Вибір папки для зберігання архіва сервера

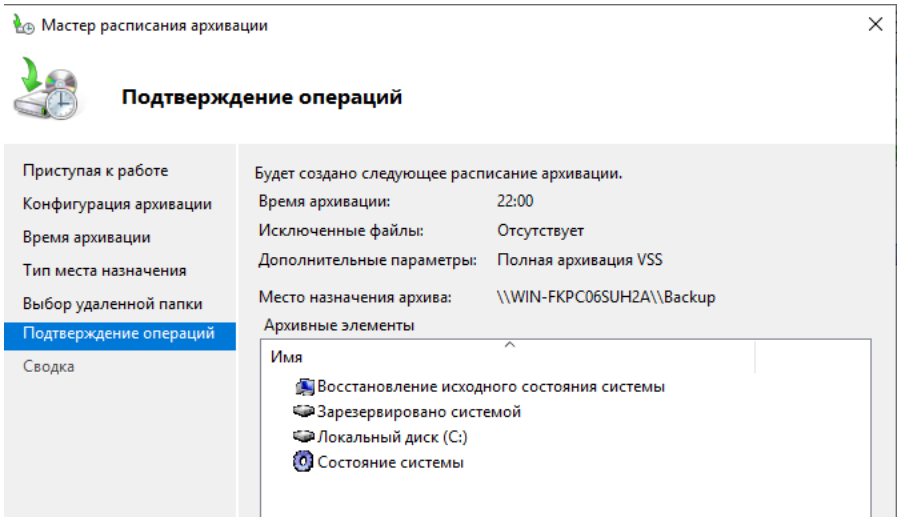


Рис. 3.8. Завершення налаштування архівації сервера

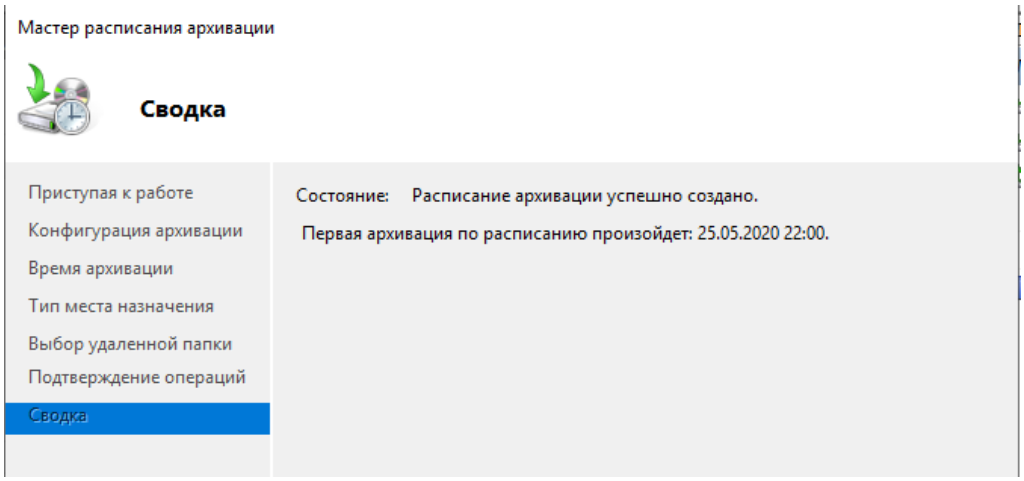


Рис. 3.9. Налаштована архівація сервера

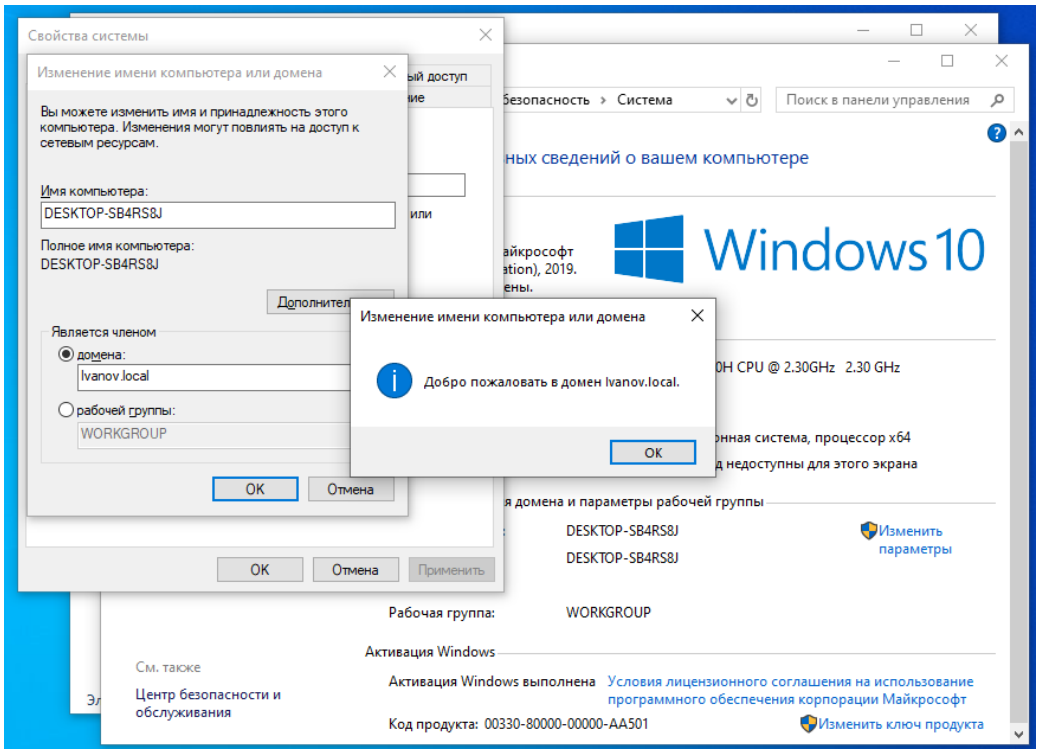


Рис. І.1. Додання робочої станції в домен

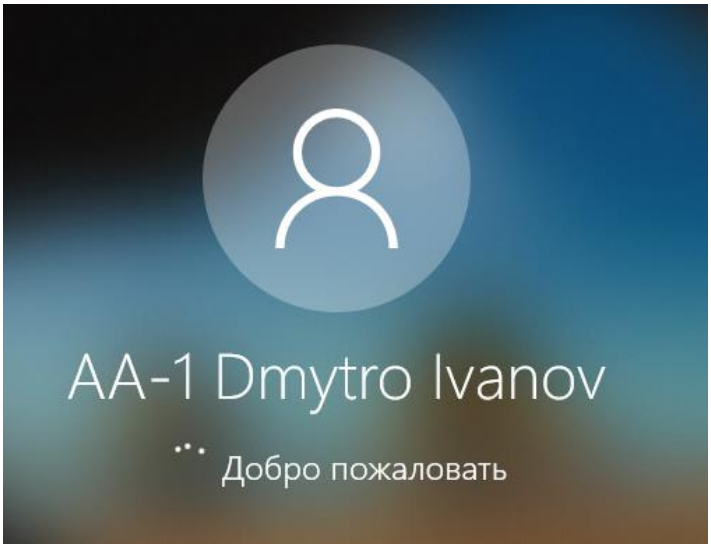


Рис. І.2. Вхід в обліковий запис

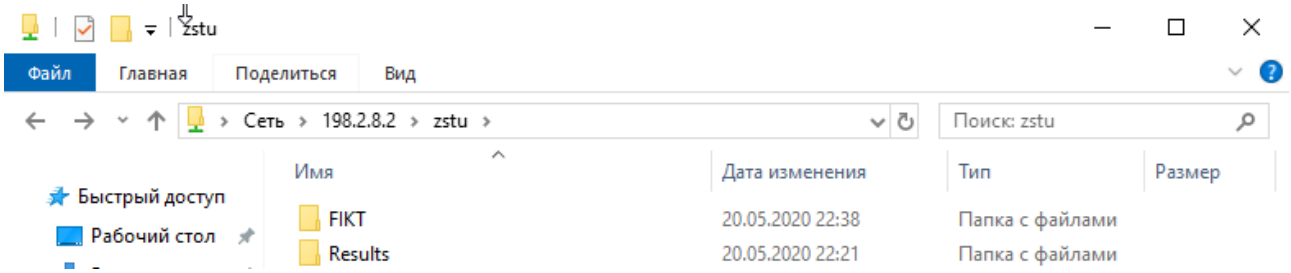


Рис. І.3. Доступний мережевий каталог

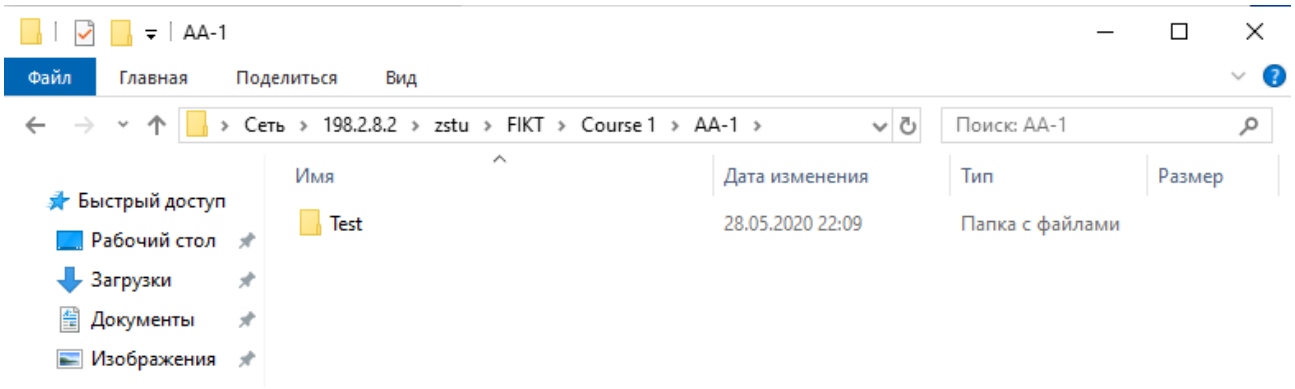


Рис. I.4. Додання в мережеву папку

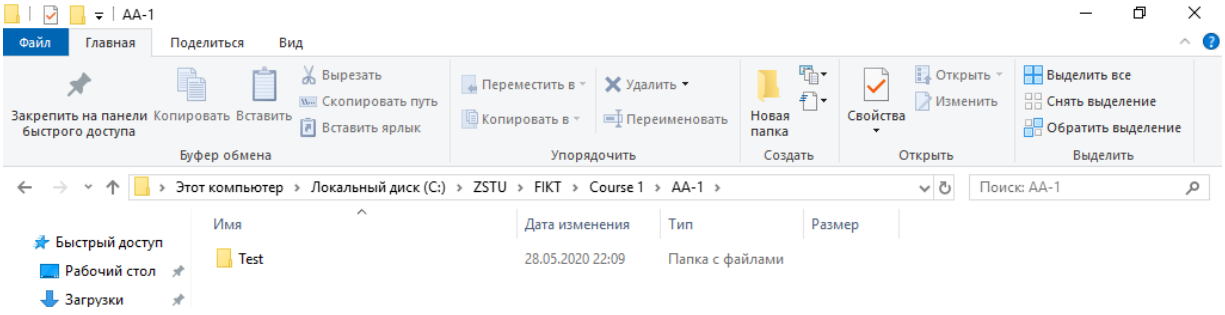


Рис. I.5. Вид з сервера

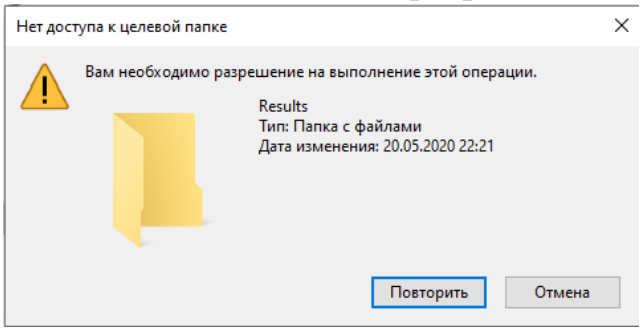


Рис. I.6. Відмова у доступі у не свою папку

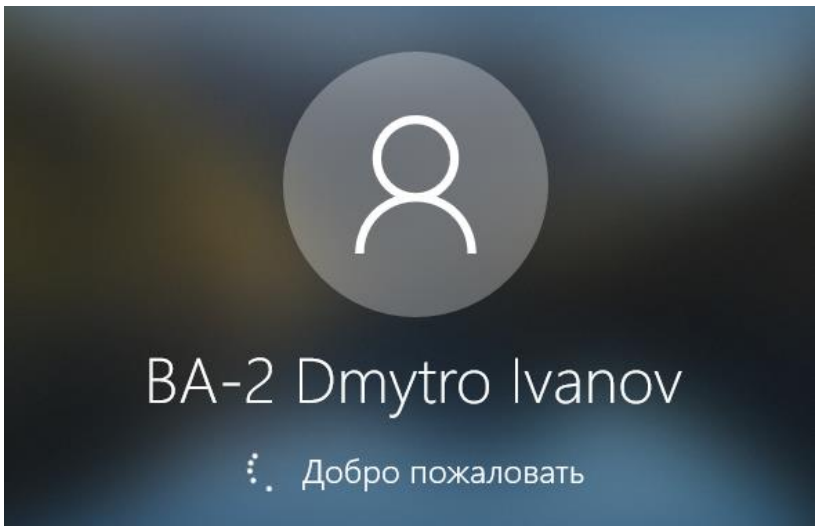


Рис. I.7. Вхід в обліковий запис

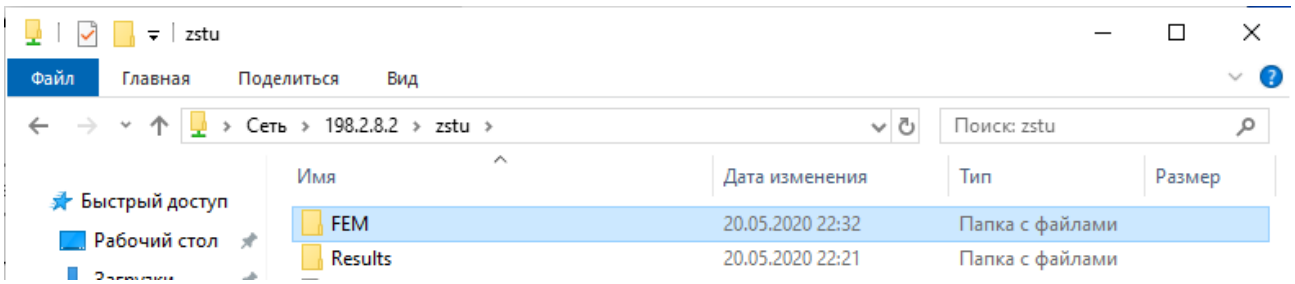


Рис. I.8. Доступний мережевий каталог

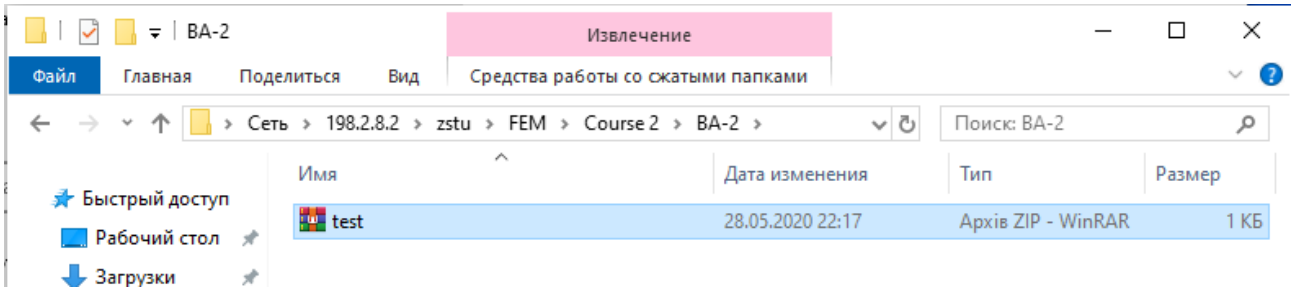


Рис. I.9. Додання в мережеву папку

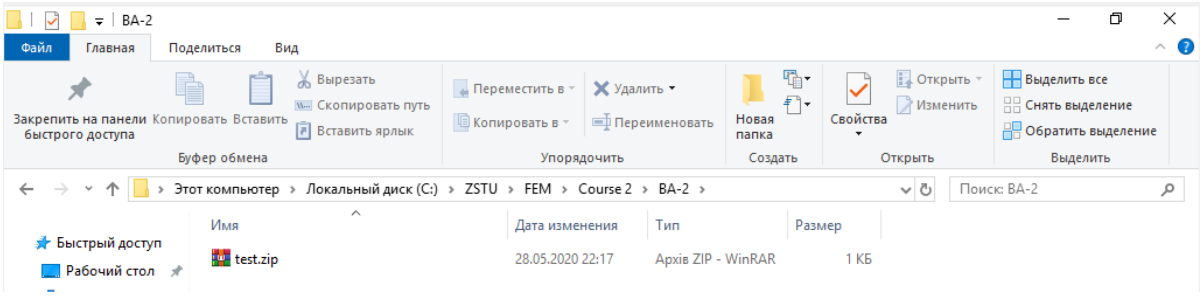


Рис. I.10. Вид з сервера

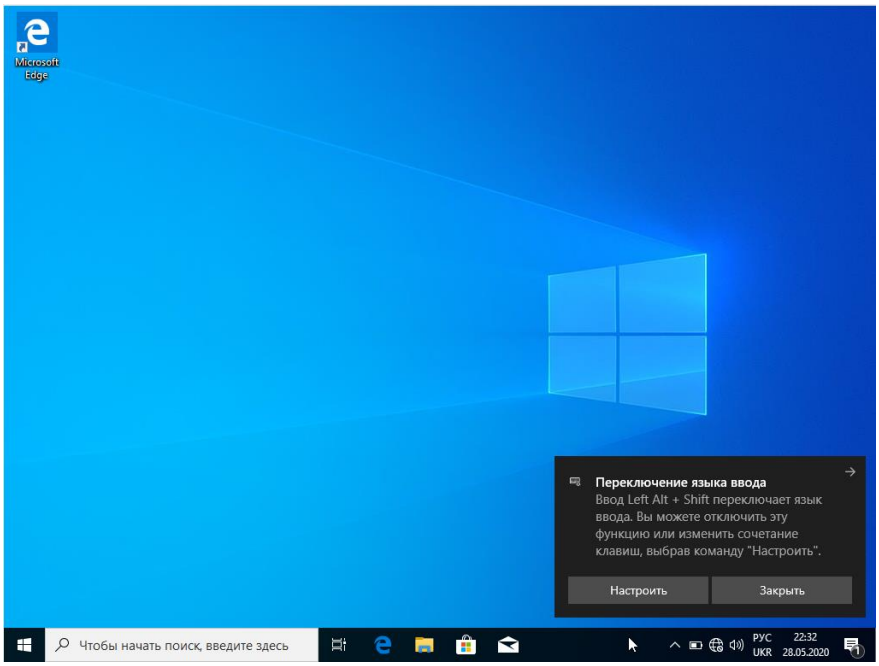


Рис. I.11. Відсутність «Кошика»

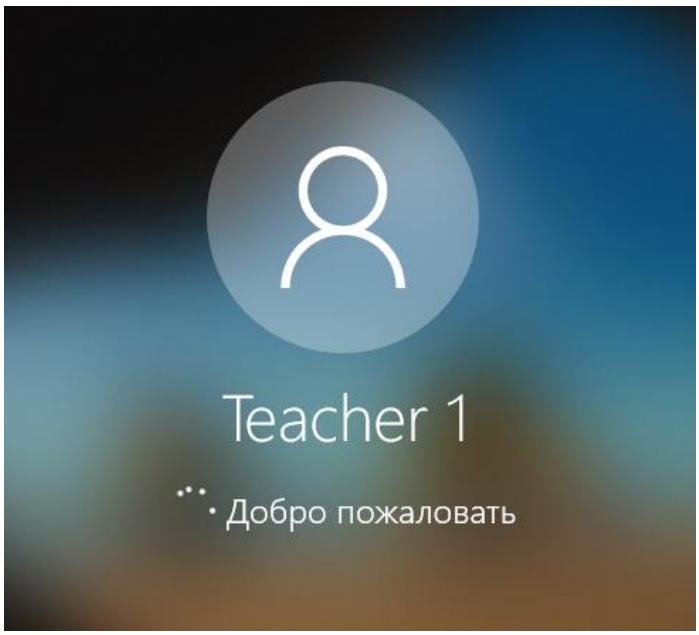


Рис. I.12. Вхід в обліковий запис

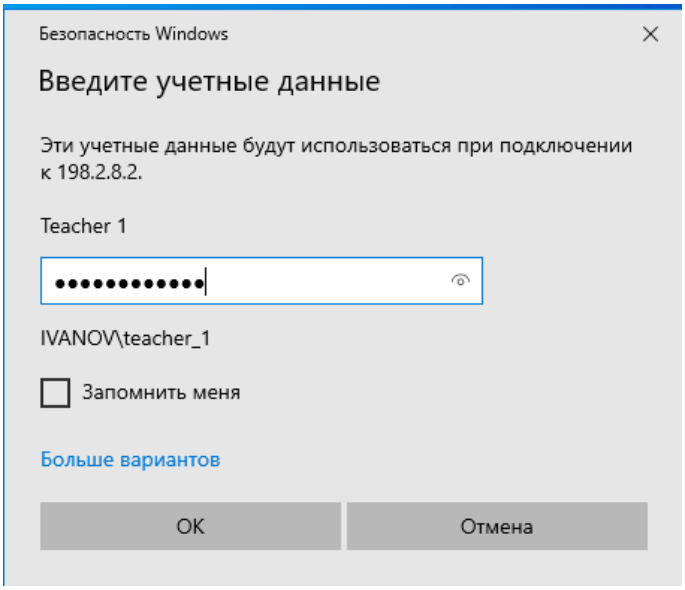


Рис. I.13. Віддалене підключення до сервера

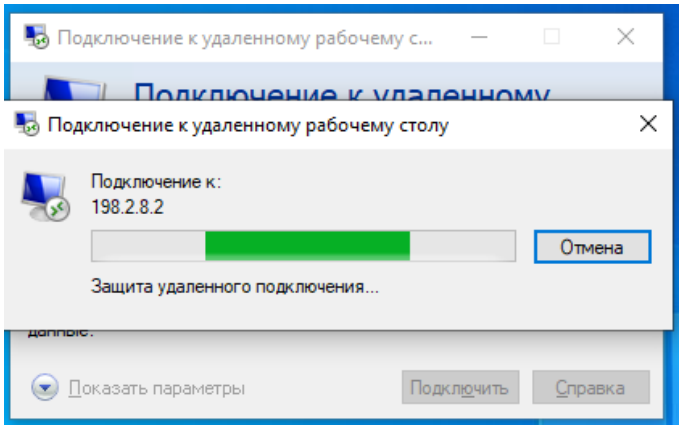


Рис. I.14. Віддалене підключення до сервера

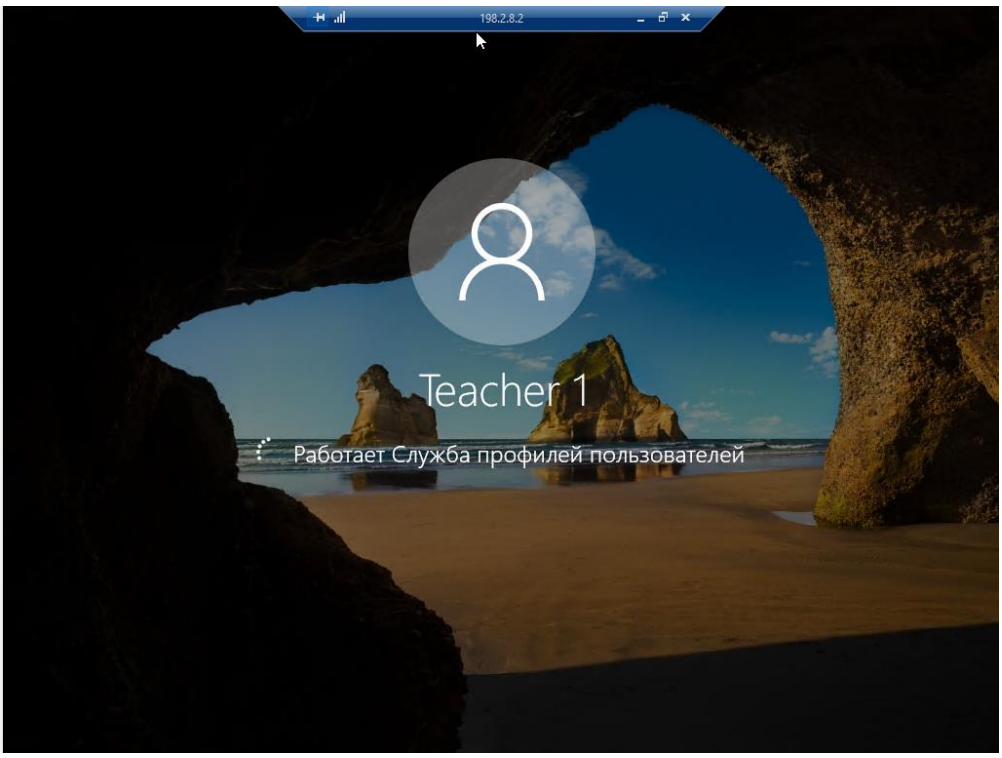


Рис. І.15. Віддалене підключення до сервера

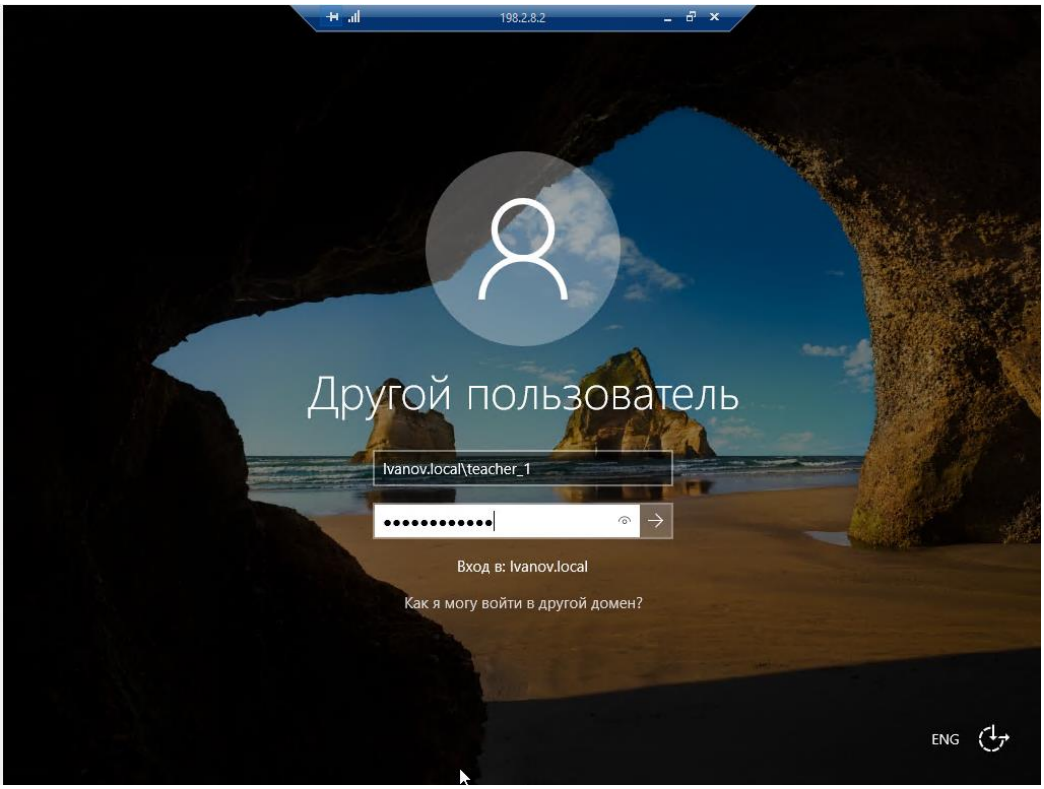


Рис. І.16. Віддалене підключення до сервера



Рис. I.17. Віддалене підключення до сервера

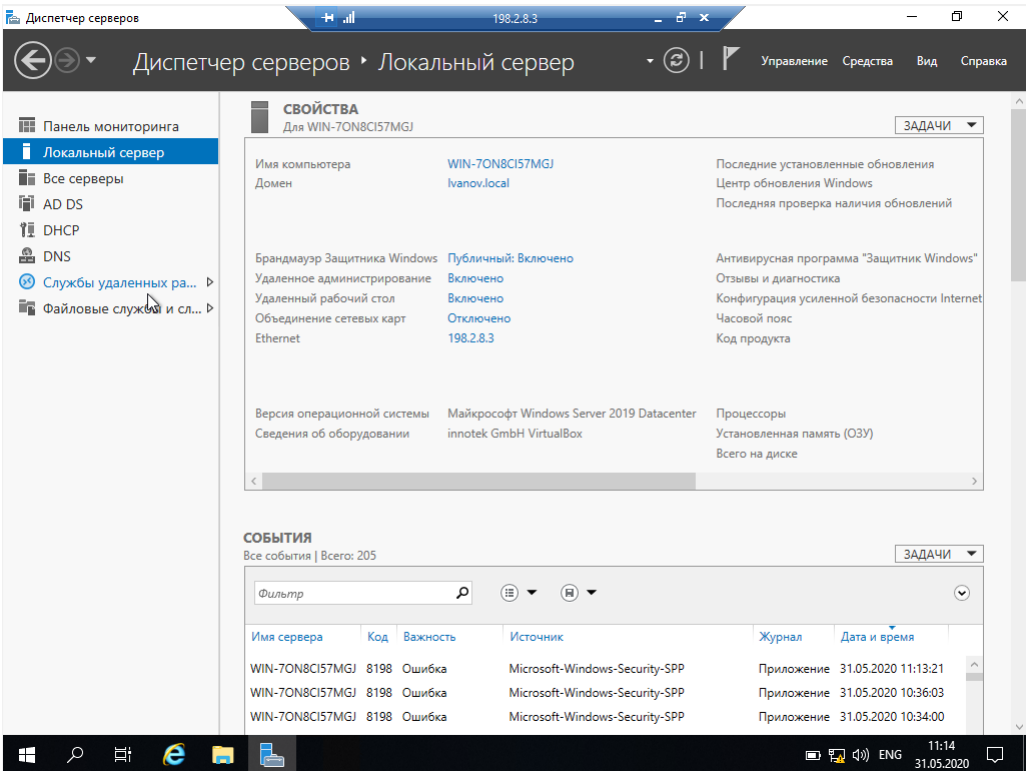


Рис. I.18. Віддалене підключення до сервера