

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

1

ПОЯСНЮВАЛЬНА ЗАПИСКА

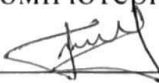
до випускної кваліфікаційної роботи магістра
на тему:

«Проект підсистеми захисту мережної інфраструктури
Коростенського міськрайонного суду»

Виконав студент 2-го курсу, групи КБм-21-1
спеціальності 125 «Кібербезпека»

 Савчук А.В.

Керівник старший викладач кафедри
комп'ютерної інженерії та кібербезпеки

 Покотило О.А.

Рецензент кандидат технічних наук, доцент,
доцент кафедри комп'ютерної інженерії та
кібербезпеки

 Россінський Ю.М.

Житомир 2022

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ

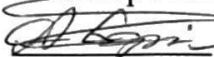
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Сфіменко А. А.

«25» жовтня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Савчука Андрія Васильовича**

Тема роботи: Проект підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду

затверджена Наказом по університету №501/с від «25» жовтня 2022 р.

Термін здачі студентом закінченої роботи – «28» грудня 2022 р.

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Операційна система Windows Server
3. Маршрутизатор Cisco 2900
4. Комутатор Cisco Catalyst 2960
5. Графічний симулятор мереж GNS3
6. Операційна система Windows 7

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	06.11.2022	06.11.2022
2	Покотило О.А.	20.11.2022	20.11.2022
3	Покотило О.А.	11.12.2022	11.12.2022

Керівник  Покотило О.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 жовтня 2022 – 4 жовтня 2022	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо поставленого завдання підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду	5 жовтня 2022 – 7 жовтня 2022	Виконано
3	Розробка загального макету мережі	8 жовтня 2022 – 11 жовтня 2022	Виконано
4	Проектування загального підключення мережа та створення IP-адресації мережі	12 жовтня 2022 – 15 жовтня 2022	Виконано
5	Проектування мережі	16 жовтня 2022 – 21 жовтня 2022	Виконано
6	Проектування та створення сценаріїв тестування функціоналу підсистеми	22 жовтня 2022 – 30 жовтня 2022	Виконано
7	Базове налагодження пристроїв мережі	31 жовтня 2022 – 4 листопада 2022	Виконано
8	Налагодження підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду	31 жовтня 2022 – 8 листопада 2022	Виконано
9	Тестування працездатності мережі	9 листопада 2022 – 15 листопада 2022	Виконано
10	Аналіз результатів тестування	16 листопада 2022 – 23 листопада 2022	Виконано
11	Написання пояснювальної записки	24 листопада 2022 – 18 грудня 2022	Виконано
12	Дата подачі роботи	19 грудня 2022	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	27 грудня 2022	Виконано
14	Підготовка презентації та виступу	28 грудня 2022	Виконано
15	Захист	29 грудня 2022	Виконано

Студент  Савчук А.В.

Керівник  Покотило О.А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду та пояснювальної записки до нього. Пояснювальна записка містить 69 сторінок, 78 ілюстрацій та 2 таблиці.

Метою роботи є розробка проекту підсистеми захисту мережної інфраструктури.

У цій дипломній роботі описана інструкція як налаштувати локальну мережу.

Проект присвячений побудові локальної мережі. Метою проекту буду налаштування працездатності мережі з використанням серверу, щоб мережу була працездатна. Також налаштування захисту який дозволить мережі працювати безперебійно

Пояснювальна записка складається з трьох розділів, в які входять теоретична розробка мережі, вибір програмного забезпечення, базове налаштування мережі, налаштування серверу, налаштування захисту та перевірка працездатності мережі.

КЛЮЧОВІ СЛОВА: ЛОКАЛЬНА МЕРЕЖА, CISCO, WINDOWS SERVER, ПІДПРИЄМСТВО, ЗАХИСТ.

						4

ABSTRACT

The qualification work consists of the project of the network infrastructure protection subsystem of the Korosten City District Court and an explanatory note to it. The explanatory note contains 69 pages, 78 illustrations and 2 tables.

The purpose of the work is to develop a project of the network infrastructure protection subsystem.

This thesis describes instructions on how to set up a local network.

The project is devoted to building a local network. The goal of the project will be to configure the network performance using the server so that the network is operational. Also, security settings that will allow the network to work smoothly

The explanatory note consists of three sections, which include theoretical network design, software selection, basic network setup, server setup, security setup, and network health check.

KEY WORDS: LOCAL NETWORK, CISCO, WINDOWS SERVER, ENTERPRISE, PROTECTION.

						4

3MICT

ПЕРЕЛІК УМОНІХ СКОРОЧЕНЬ	8
ВСТУП	9
РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ ПІДПРИЄМСТВА. ПРИНЦИП ПОБУДОВИ МЕРЕЖІ ТА СПОСОБИ ЗАХИСТУ	12
1.1 ОСОБЛИВОСТІ ПОБУДОВИ МЕРЕЖІ ПІДПРИЄМСТВА	12
1.2 ЛОКАЛЬНА МЕРЕЖА ПІДПРИЄМСТВА	14
1.3 ЗАХИСТ МЕРЕЖІ	17
1.4 ЗАГАЛЬНІ ТЕХНІЧНІ ВІДОМОСТІ ТА ВИМОГИ ДО ПРОГРАМНОГО ТА АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ МЕРЕЖІ.	22
РОЗДІЛ 2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ІНФАСТРУКТУРИ КОРОСЕТНСЬКОГО МІСЬРАЙОННОГО СУДУ	24
2.1 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ.....	24
2.2 РОЗРОБКА СТРУКТУРИ МЕРЕЖІ.....	26
2.3 ВИБІР ОБЛАДНАННЯ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	28
РОЗДІЛ 3 НАЛАШТУВАННЯ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ КОРОСТЕНСЬКОГО МІСЬКРАЙОНОГО СУДУ	34
3.1 БАЗОВЕ НАЛАШТУВАННЯ МЕРЕЖІ	34
3.2 ПЕРЕВІРКА БАЗОВИХ НАЛАШТУВАНЬ МЕРЕЖІ ТА НАЛАШТУВАННЯ WINDOWS SERVER.....	39
3.3 НАЛАШТУВАННЯ ДОДАТКОВОГО ЗАХИСТУ ТА ПЕРЕВІРКА РОБОТИ МЕРЕЖІ	60
3.4 АНАЛІЗ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ	64
ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	68
ДОДАТКИ.....	70

						4

ПЕРЕЛІК УМОНІХ СКОРОЧЕНЬ

ОС – Операційна система

DHCP - Dynamic Host Configuration Protocol

NAT – Network Address Translation

NTP – Network Time Protocol

RDP – Remote Desktop Protocol

IP – Internet Protocol

DNS – Domain Name System

						4

ВСТУП

Актуальність теми. Інформаційна технологія – це сукупність методів, виробничих процесів, програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує реалізацію інформаційних процесів з метою підвищення їх надійності та ефективності та скорочення трудомісткості процесу використання інформації. Ресурс.

Інформаційні технології є одним із найважливіших досягнень людської діяльності. Застосування інформаційних технологій дає змогу створити сприятливі умови для розвитку економіки, стимулювати зростання продуктивності праці та підвищення заробітної плати, полегшити організацію зв'язку на всіх рівнях управління та швидко знизити матеріало та енергомісткість населення. виробництва і народного господарства в цілому.

Розвиток новітніх технологій значною мірою сприяв створенню інформаційних систем. Для України дуже важливо, щоб використання інформаційних технологій покращувало якість підготовки та прийняття важливих рішень виконавчої влади. З 2000 року Україна бере активну участь у формуванні інформаційного суспільства. У 2007 році був прийнятий Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки».

Основне завдання розвитку інформаційного суспільства в Україні – допомогти кожній людині на основі широкого використання можливостей сучасних ІКТ створювати інформацію та знання, використовувати та обмінюватися ними, виробляти товари та надавати послуги, реалізуючи свої повний потенціал, покращуючи якість свого життя. Розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя та діяльність органів державної влади та органів місцевого самоврядування визначаються одним із пріоритетних напрямів державної політики.

Національна політика розвитку інформаційного суспільства в Україні базується на принципах: пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих та сприятливих економічних умов; комплексний розвиток загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення загального доступу до

						4

телекомунікаційних та ІКТ-послуг; сприяти збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; підвищення кадрового потенціалу; посилення мотивації щодо використання ІКТ; масштабне впровадження ІКТ у науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечити інформаційну безпеку.

Але на шляху досягнення цих цілей постають труднощі, пов'язані з недостатньою технологічною базою, складним фінансовим забезпеченням цього процесу, відсутністю достатньої кількості наукових досліджень процесу становлення інформаційного суспільства та його складових.

Сучасна інформаційна система забезпечує:

1) прямий і швидкий доступ до інформаційного продукту;

2) ефективна координація внутрішньої діяльності;

3) використання якісно кращих технологій системного аналізу та оперативного проектування менеджменту в різних сферах діяльності підприємства тощо.

Україна накопичила значний потенціал в інформаційних технологіях. Її національною конкурентною перевагою є її розвиток. Але Україна, як виробник товарів, може бути витіснена з найперспективніших світових ринків через відсутність обґрунтованої державної політики. Розвиток інформаційного суспільства в Україні має базуватися на узгодженості дій усіх гілок влади. Вирішення проблем ІТ-відставання в Україні потребує національного підходу, а саме:

1) формування національної стратегії, міжнародної та національної політики, сприятливого законодавчого, соціально-економічного клімату у сфері використання інформаційних технологій;

2) забезпечити потенційну можливість технологічного доступу населення до комп'ютерних інформаційних технологій шляхом об'єднання зусиль державного та приватного секторів економіки у розвитку інформаційної інфраструктури;

3) сприяти збільшенню та поширенню кількості послуг населенню та суб'єктам господарювання, що надаються з використанням комп'ютерних інформаційних технологій;

4) концентрація зусиль держави і суспільства на створенні загальнодоступних

						4

електронних ресурсів на основі національних, політичних та економічних міркувань.
Мовно-культурні та релігійні аспекти розвитку України;

5) забезпечення можливості набуття знань, умінь та компетентностей щодо використання інформаційно-комп'ютерних технологій у процесі здобуття освіти.

Наша держава потребує певної політики у сфері інформатизації, оскільки в Україні ще існують певні перешкоди, які необхідно усунути, а саме:

- 1) гостра нестача кваліфікованих кадрів;
- 2) неадекватність існуючої моделі відносин з інформаційними технологіями з боку влади для впевненого збереження здобутих позицій на світовому ринку;
- 3) недійсність захисту прав інтелектуальної власності;
- 4) завищена вартість і неякісна інфраструктура.

Метою кваліфікаційної роботи є розробка підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду

Встановлена мета створює наступні завдання:

- вибір та аналіз сучасних приладів;
- вибір засобів для реалізації локальної мережі;
- вибір засобів для створення серверу для мережі;
- розробка системи захисту для мережі.

Об'єктом дослідження є процес захисту мережної інфраструктури.

Предметом дослідження є методи і засоби для розробки захисту в локальній мережі.

В процесі розробки кваліфікаційної роботи був розроблений проект підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду.

Апробація результатів:

1. Савчук А.В., Вакалюк Т.А. Проект підсистеми захищеного багатоточкового підключення до мережі провайдера інтернет // Тези IV Всеукраїнської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих учених «Інформаційно-комп'ютерні технології: стан, досягнення та перспективи розвитку», м. Житомир, 25-26 листопада 2021 року – Житомир: Житомирська політехніка, 2021. С. 60-61.

						4

РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ГЕТЕРОГЕННІЙ МЕРЕЖІ ПІДПРИЄМСТВА. ПРИНЦИП ПОБУДОВИ МЕРЕЖІ ТА СПОСОБИ ЗАХИСТУ

1.1 Особливості побудови мережі підприємства

Комп'ютерна мережа – це комплекс ПК та інших пристроїв (комутаторів, маршрутизаторів, і т.д.), що об'єднанні між собою за допомогою кабелів. Також пристрої локальної мережі мають змогу обмінюватися інформацією між собою.

Переваги використання локальної мережі[1]:

1) Однією із головних переваг є економічна складова. Використання локальної мережі дає можливість спільно використовувати периферійні пристрої. Тобто не потрібно купувати принтер для кожного співробітника – можна підключити його до одного комп'ютера, налаштувати спільний доступ і усі співробітники які мають доступ до мережі зможуть їм користуватися. Вважаючи що такого роду пристрої досить поширені в державних установах - це дасть змогу зекономити досить велику кількість бюджету установи що розробляє свою мережу.

2) Локальна мережа на підприємстві дає можливість економити досить багато робочого часу за допомогою того що дає змогу обмінюватися даними досить швидко, що також вплине і на продуктивність.

3) Дозволяє декільком користувачам використовувати програмне забезпечення, тобто це дозволить одночасно виконувати спільну роботу при необхідності

4) Локальна мережа дозволить всім користувачам отримати вихід до мережі Інтернет. Більш того, контролювати інтернет-серфінг співробітників набагато простіше

5) Надає змогу віддаленого доступу до файлів на робочому комп'ютері з дому. Про те це працює тільки в тому випадку якщо локальна мережа налаштована, і надає доступ до Інтернету робочому комп'ютеру. Це не тільки надає можливість робітникам працювати віддалено, а й дає змогу адміністратору і службі підтримки надавати технічну допомогу віддалено.

Як і будь-яка мережа підприємства, вона повинна відповідати наступним

						4

вимогам:

- 1) Спільний доступ користувачам мережі до файлів та можливість обміну інформацією
- 2) Доступ до Інтернету
- 3) Спільна робота з деяким програмним забезпеченням
- 4) Спільний доступ до периферійних пристроїв
- 5) Велика пропускна здатність, можливість підключення нових співробітників без зниження продуктивності, стабільність роботи та безпека, можливість швидко контролювати роботу та вирішувати будь-які проблеми в її роботі.
- 6) Налаштування резервного копіювання

Перед початком проектування мережі необхідно вибрати мережеву технологію.

Мережеві технології представляються стандартними протоколами і програмно-апаратними засобами які допомагають їх реалізувати, за допомогою яких можна побудувати обчислювальну мережу.

Мережева архітектура визначає декілька параметрів мережі[2]:

- 1) Швидкість передачі даних (Визначає кількість інформації в бітах, яка може передаватися за допомогою мережі)
- 2) Формат мережевих кадрів (Інформація в мережі передається за допомогою пакетів інформації тобто «кадри», а мережеві кадри в різних технологіях мережі мають різні формати)
- 3) Середовище передачі. (Вибір кабелю через який буде проходить вся інформація, тобто «трафік»)
- 4) Топологія мережі. (Схема мережі, від вибору топології залежить, пропускна здатність, доступність, працездатність мережі.

При розробці мережі також необхідно приділити увагу монтажу кабельної системи. Структуру кабельної системи визначається інформаційними технологіями, адже є чіткі зміст конкретного проекту відповідно від вимог.

Прокладка витой пари має ряд особливостей. Кабель вита пара має допустимий радіус вигину. Про те сильний вигин призводить до порушення ізоляції кабелю.

						4

Також необхідно залишати запас кабелю не менше 3-ох метрів. Він може використовуватися при перенесенні монтажних конструктивів або для підтяжки кабелю в разі ремонту, наприклад, при обриві і відновлення оптичної кабельної лінії.

1.2 Локальна мережа підприємства

Локальна мережа – це мережа з обмеженою кількістю користувачів, що об'єднує їх в одну цілу систему. Локальна мережа створюється для того щоб об'єднати всі пристрої між собою.

Зараз тяжко уявити собі підприємство яке б працювало без локальної мережі. Вона дозволяє швидко обмінюватися інформацією, мати спільні паки, та дані а також користуватися периферійними пристроями віддалено.[3]

У будь-якому офісі переважно ставиться один сервер (для зберігання, обробки інформації), робочі станції (ПК) для співробітників, та комутатори для того щоб працівники могли мати доступ до локальної мережі і в випадку якщо мережа підключена до Інтернету мали доступ до Інтернету.

При розробці локальної мережі досить велику увагу приділяють вибору топології мережі. Існують 3 найпоширеніших топології[4]:

1) Шина – це мережа зв'язок в якій відбувається через один загальний шлях. При передаванні будь-якої інформації, вона відразу стає доступна для всіх інших користувачів які підключенні до даної мережі

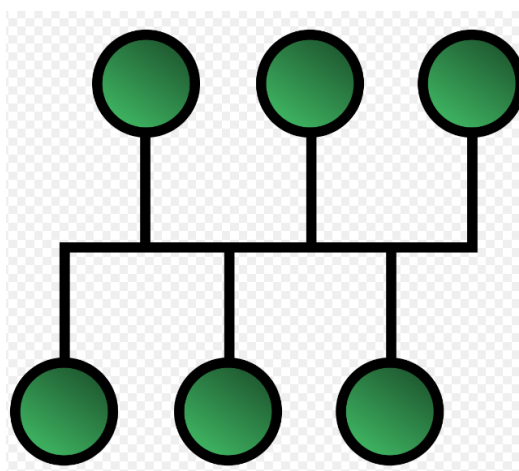


Рисунок 1.1 – Топологія «шина».

Переваги даної топології являється те що вона дуже економна і проста в використанні. Також її дуже легко розширювати і додавати нових користувачів. Про

те вона має один із головних недоліків який дуже сильно впливає на працездатність такої мережі, в випадку коли кабель до якого під'єднано багато користувачів, виходить із ладу то це дуже сильно впливає на працездатність. Також якщо до спільного кабелю під'єднати багато користувачів, то це зменшить пропускну здатність мережі. Ще недоліком мережі являється те що дуже складно вирішувати проблеми не припиняючи роботу користувачів мережі;

2) Кільце – це мережа взули якої пов'язуються між собою в виді кільця (до кожного вузла тільки дві лінії), дані проходять по кільцю, тому доступні тільки по черзі для кожного користувача.

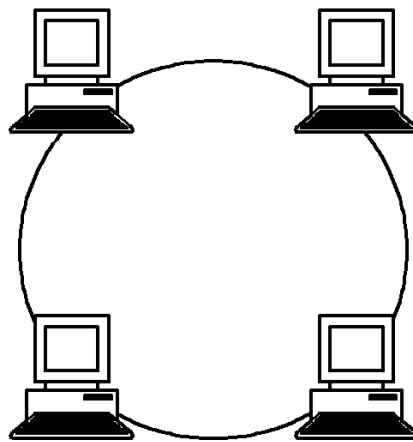


Рисунок 1.2 – Топологія «кільце».

Переваги даної топології що всі комп'ютери мають рівний доступ. Також кількість користувачів не впливає на продуктивність мережі. Недоліками цієї топології є те що вихід з ладу одного вузла може призвести до того що з ладу може вивести всю мережу. Тяжко вирішувати проблеми з мережею, а також зміна налаштувань мережі потребує зупинку всієї мережі ;

3) Зірка – це мережа у якій є головний (центральний) вузол і від нього розходяться всі з'єднання.



Рисунок 1.3 – Топологія «зірка».

Перевагами даної мережі є те що її легко покращувати, легко додавати нові вузли, тобто користувачів. Централізований контроль. Про те є один великий недолік, а саме якщо центральний вузол виходить з ладу то з ладу виходить і вся мережа.

Кожна із них має як і свої переваги так і мінуси, тому виходячи з того яку мережу і для яких цілей потрібно будувати вибирається своя топологія.

Важливим аспектом будь-якої мережі є адресація. Будь-яка мережа адресується за допомогою IP-адрес. Це унікальна адреса вузла в мережі, побудована на основі протоколів TCP/IP.

IP – адреси можуть бути статичними та динамічними. Статична IP-адреса вважається тоді коли користувач чи адміністратор призначає її вручну для кожного пристрою. Така IP-адреса не може бути призначена іншому пристрою. Динамічною IP-адреса вважається тоді коли пристрій отримує її автоматично коли підключається до мережі[5]. Таке адреса використовуються протягом обмеженого проміжку часу. В випадку коли пристрій більше не під'єднаний до мережі його адресу може отримати інший пристрій мережі. Список адрес які можуть отримати користувачі мережі зазначається адміністратором мережі і налаштовується ним.

DHCP – це мережевий протокол за допомогою якого пристрої мережі можуть отримувати IP-адресу та інші необхідні дані автоматично.

Даний протокол працює за принципом «клієнт-сервер»[6]. Для отримання налаштувань

пристрій-клієнт звертається до DHCP серверу та отримує необхідні параметри.

При налаштуванні адміністратор задає діапазон адрес, що розподіляється сервером серед інших користувачів. Це спрощує роботу, дозволяючи уникнути помилок при ручному налаштуванні комп'ютерів. Здебільшу протокол DHCP використовується в мережах TCP/IP.

Для розділення зовнішньої мережі від внутрішньої використовується протокол NAT. Він дасть змогу мати доступ до мережі Інтернет всім користувачам локальної мережі за однією зовнішньою адресою. NAT – це протокол який дозволяє змінювати локальну адресу для того щоб користувачі мережі мали доступ до інтернету[7].

В локальній мережі може бути багато користувачів, тому даний протокол дозволяє виділити невеликий діапазон адрес.

1.3 Захист мережі

Кожна мережа потребує навіть мінімального захисту. Проте в великих компаніях, держ. установах, підприємствах потрібно відповідально віднестися до захисту мережі. Зараз існує багато способів отримати доступ до даних в мережі, перехоплювати трафік а також просто виводу з ладу мережу задля своєї вигоди. Більшість атак не являються успішними із-за кваліфікованого захисту про те необхідно знати які бувають атаки і способи захисту.

Для того щоб дізнатися які атаки бувають на сучасні мережі, необхідно знати їх класифікацію. Це потрібно для того щоб можна було розібратися в тому як вони працюють і на що впливають

Найбільш поширені атаки на мережу є зіставлення атак рівням теоретичної моделі OSI[8].

Тобто розглянемо можливі атаки і на що кожна із них впливає. Більшість атак можна розділити так:

- пошук хостів, які мають доступ до зовнішньої мережі;
- пошук хостів, які не мають доступу до зовнішньої мережі;
- сканування хостів;

						4

- сніффінг (прослуховування трафіку);
- атаки на локальну мережу;
- заміна трафіку частково чи окремих пакетів даних.

Пошук хостів, які мають доступ до зовнішньої мережі. Набір атак які належать до цієї групи можна назвати скануванням мережі. Вони надають змогу ідентифікувати, які саме хости доступні, тобто визначити чи є з ними зв'язок. Переважно ця група реалізується за допомогою спостереження за стандартними протоколами які повинні працювати на доступних хостах. Для пошуку хостів можна скористатися протоколом ICMP. Цей протокол створювався для того, щоб збирати дані про проблеми в мережі. Збір даних можна здійснити опираючись на відповідях хостів. Для збору даних про доступність хоста може бути задіяний echo запит. Будь-які відповіді від цільових хостів будуть важитися як доступність хоста.

Пошук хостів, які не мають доступу до зовнішньої мережі. Це набір атак такий же як і попередній, але крім них, їх можна розширити, залежно від принципів побудови мережі, зважаючи на додаткову інформацію та методи отриманих даних. Можна поділити на 2 частини:

Перша – це пасивний збір даних при можливості прослуховування трафіку: деякі протоколи можуть містити в собі інформацію про те, що передається і ким.

Друга частина включає методи на мережу. Здійснюються вони у вигляді використання протоколів:

Пошук хостів, які не мають доступу до зовнішньої мережі. Почасти цей етап може включати попередній пункт, але, крім нього, цей крок можна поширити, залежно від принципів побудови мережі, на додаткові протоколи та методи отримання даних. Пункт можна поділити на 2 частини. Перша — це пасивний збір даних за можливості прослуховувати трафік: деякі протоколи прикладного рівня можуть розкривати подробиці про те, що передається і ким.

Друга частина включає методи на мережу. Здійснюються вони у вигляді використання протоколів:

- ARP – механізм запиту даних про IP адреси та MAC адреси хостів;
- NetBIOS – механізм, який називається Browser. У ньому передається

						4

інформація про назву операційної системи та її версії;

- IPv6 — надсилання мультикастових запитів для отримання даних про доступні хости.

Сніффінг (прослуховування трафіку). Атака, яка може бути успішна у випадку або якщо неправильно налаштовано мережеве обладнання, або через особливості топології мережі. Застосовується для вивчення даних у трафіку, а також для отримання даних, які можуть бути використані для підвищення рівня доступу до мережі або на окремих системах, що беруть участь у мережевій взаємодії. У більшості випадків збір даних можна проводити з операційних систем хостів, хоча і з мережевих пристроїв ті самі дії так само можливі[9].

Захистом від прослуховування трафіку є правильно налаштована мережа. Та правильний вибір топології під час проектування мережі. Від топології залежить багато чого, тому що якщо зломисник може підключатися до серверу мережі, то це вже не правильно проектування мережі.

Атаки на локальну мережу. Атаки, які в більшості випадків змінюють топологію мережі та заповнюють мережу великою кількістю однотипних пакетів. Робиться це для того, щоб не відбувалося відновлення початкового стану маршрутів мережі.

Для того щоб попередити дану атаку необхідно обмежити кількість прийняття пакетів за певний час.

ARPSpoofing - базовий блок для всіх атак, які мають на увазі зміну трафіку в мережі. Має на увазі відправлення великої кількості пакетів з даними, що дозволяють зломиснику прикидатися будь-яким хостом у мережі. Найбільш вигідні хости в цьому випадку - gateway або хост, де розміщуються цільові для атаки сервіси.

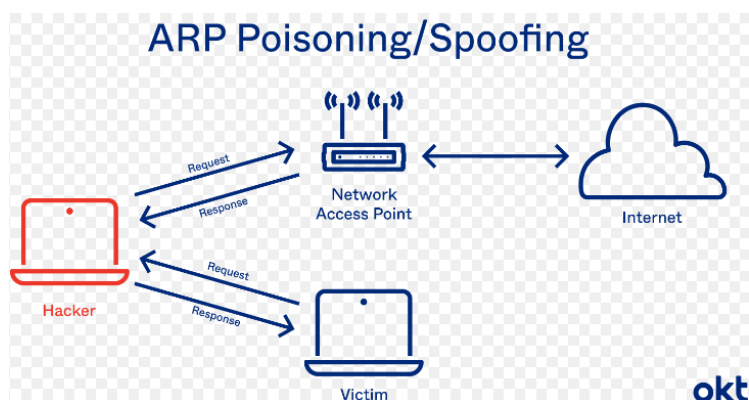


Рисунок 1.4 – Принцип роботи ARPSpoofing

Захистом від даної атаки є використання спеціального програмного забезпечення яке зможе шифрувати пакети, і не дасть зловмиснику відстежувати трафік[10].

Dynamic Trunking. Так як чи не єдиним ефективним засобом для боротьби зі зміною топології мережі може бути використання стандарту 802.1Q VLAN, то, природно, при його виявленні потрібно перевірити можливість атак на його неправильну конфігурацію. Цей вид атаки передбачає, що при доступі хоча б одного VLAN можна перевести з'єднання в стан, при якому будуть видно всі дані з інших VLAN.

Для захисту потрібно правильне налаштування, щоб зловмисник не міг отримати доступ до VLAN.

VLAN Hopper — атака, яка дозволяє шукати хости у сусідніх VLAN та надсилати повідомлення.

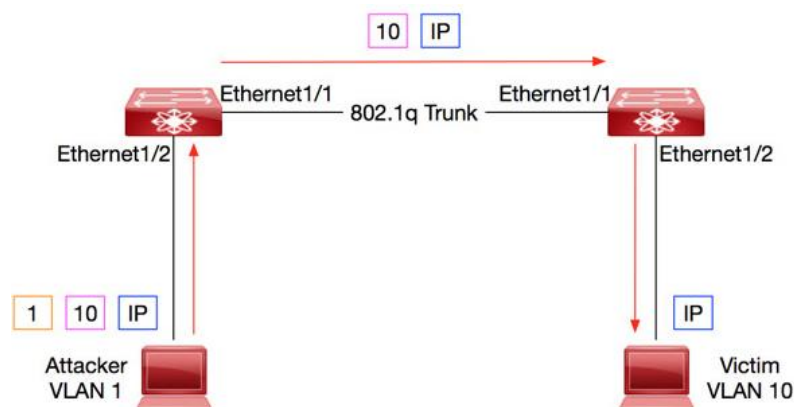


Рисунок 1.5 – Принцип роботи VLAN Hopper

Захист від даної атаки простий, потрібно налаштувати комутатор так щоб від не надавав автоматичної згоди для порта.

Double Tagging – атака, яка можлива, якщо атакуючий знає номер VLAN, ір адресу системи жертви. Атакуючий у цьому випадку може запакувати повідомлення для надсилання цільової системи. Недоліком атаки вважатимуться відсутність зворотний зв'язок, оскільки цільова система зможе відправляти відповіді.

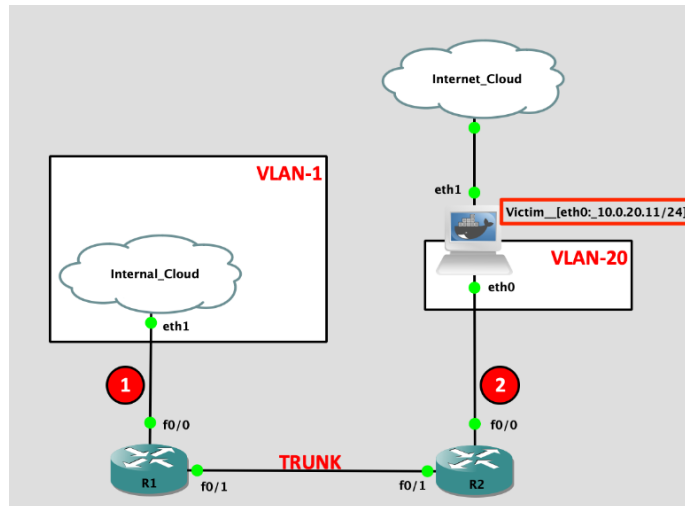


Рисунок 1.6 – Принцип роботи Double Tagging

Атаки з Double Tagging можна запобігти, якщо власну VLAN магістральних портів відрізнити від VLAN користувача.

DHCP Starvation — використовується для контролю надавання адреси для учасників у мережі. Може бути використане для крадіжки даних із додатків.[11]

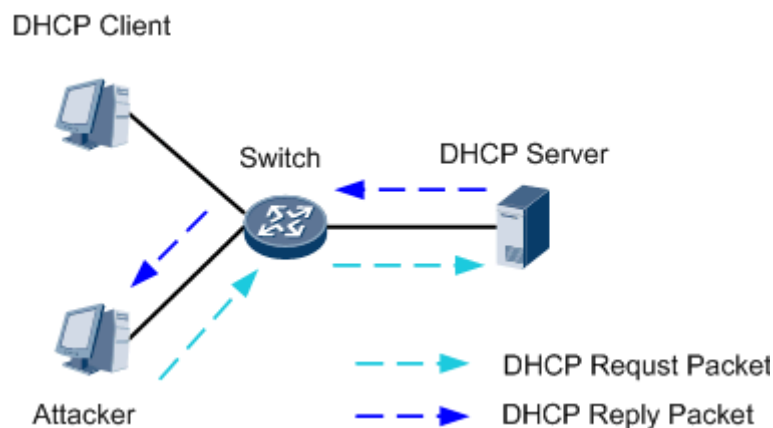


Рисунок 1.7 – Принцип роботи DHCP Starvation

Для того щоб захистити мережу від даної атаки необхідно обмежити число MAC-адреса на порту комутатора. Таким чином атака не зможе вичерпати весь ліміт IP – адрес.

Підміна сервера DNS. Багато програм, які працюють з мережею без належних перевірок, можуть зайво довіряти серверу, який використовується для реалізації роботи програми. Може бути використано для компрометації даних, що відправляються на сервер, при проведенні одночасної атаки на зміну стандартного маршруту всередині мережі[12].

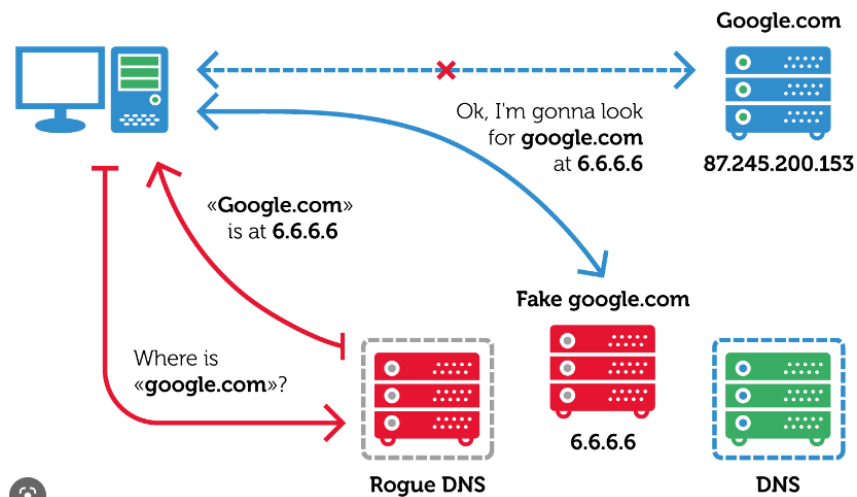


Рисунок 1.8 – Принцип роботи підміни DNS сервера

Для захисту від цієї атаки необхідно мати якісне обладнання а також постійно його оновлювати. Також в налаштуваннях необхідно в налаштуванні відключати доступ обладнання поза межами локальної мережі

Підміна gateway – за рахунок механізмів динамічного налаштування маршрутів мережі можна прослуховувати всю інформацію, яка пролітає через мережу.

Підміна сервісів ОС – використання недосконалості протоколів операційних систем та мережевих пристроїв. Найбільш популярна при дії на мережу, учасниками якої є машини під керуванням Windows.

Захистом від двох атак вище, це є постійний контроль трафіку в мережі, щоб запобігти його прослуховуванню, також постійне оновлення програмного забезпечення, адже часто в оновленнях виходять виправлення помилок и багів минулої версії.

1.4 Загальні технічні відомості та вимоги до програмного та апаратного забезпечення мережі.

Мережа буде розроблятися і складатися з однієї локальної мережі, та декількох підмереж щоб в подальшому її легко можна було розширювати, також в мережі буде Windows Server в якому будуть зберігатися всі дані і за допомогою якого буде працювати мережа.

В мережі буде створено:

						4

- одна велика локальна мережа з декількома підмережами для масштабованості
- різні операційні системи
- налаштування DHCP серверів
- налаштування захисту мережі
- налаштування серверу за допомогою якого мережа буде працювати

Підсумовуючи це, до програмно-апаратного забезпечення будуть такі вимоги:

- використання Windows Server для роботи мережі
- використання різних операційних систем
- наявність DHCP серверів
- налаштування захисту мережі

Роблячи висновки з цього, для локальної мережі буде налаштовано сервер, він призначений для управління апаратним забезпеченням серверів, що володіють необхідними для цього функціональними особливостями. Також ці серверні ОС містять спеціалізовані служби (програмні компоненти), призначені для організації, моніторингу та управління IT-інфраструктурою підприємства, починаючи від управління адресним простором протоколу IP та обліковими записами користувачів та закінчуючи організацією стійких до відмови мережевих сервісів.

В мережі будуть налаштовані декілька DHCP серверів. Вони будуть налаштовані на комутаторах. Це потрібно для того щоб в подальшому мати змогу розширювати мережу за необхідності. Простота налаштування DHCP дозволяє легко реалізовувати його в мережі, і надає багато переваг. Одна з головніших переваг це те що користувачі мережі отримають IP-адресу автоматично, що дозволить легко налаштувати мережу без ручного налаштування.

Висновок до розділу 1

Роблячи висновок з цього для побудови працездатної мережі, необхідно відповідально віднестись до побудови мережі. Спочатку потрібно розробити план приміщення де буде побудована мережа. Далі необхідно обрати топологію мережі, в залежності від того яка мережа нам потрібна.

Було розглянуто різні додаткові технології які покращать працездатність

						4

мережі. А саме DHCP протокол які допоможе в налаштуванні мережі, а в подальшому і дозволить більш легше її розширювати при необхідності. Також протокол NAT який дозволить мережі мати вихід до глобальної мережі Інтернет.

В мережі також потрібно розробити сервер на основі Windows Server, який буде відповідати за працездатність мережі. Для створення цієї мережі буде використано таку програму як GNS, він підтримує майже всі функції які можна реалізувати в реальному житті.

РОЗДІ 2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ІНФРАСТРУКТУРИ КОРОСЕТНСЬКОГО МІСЬРАЙОННОГО СУДУ

2.1 Проектування локальної мережі

Проектуючи мережу потрібно не забувати, що це мережа підприємства. Тобто мережа буде складатися з багатьох підмереж. В мережі буде використовуватися сервер, який і буде відповідати за її працездатність. Для кращої масштабованості мережі, доцільно буде використати DHCP протокол для кращого розподілу IP адреса. Це дасть змогу в подальшому додавати нових користувачів чи видаляти старих при цьому не налаштовуючи вручну IP-адресацію. Було розроблено чотири підмережі, з DHCP серверами.

Топологію з'єднань буде наведено в таблиці 2.1

Таблиця 2.1

Параметри з'єднань мережі

Пристрої	Інтерфейси	Підключення	Підключення до інтерфейсів
R_SERVER	E0/1	SW_SERVER	E0/0
SW_SERVER	E0/0	R_SERVER	E0/1
	E0/1	SW_1	E0
	E0/2	SW_2	E0
	E0/3	SW_3	E0
	E1/0	SW_ADMIN	E0
	E1/1	Windows Server	E0

можливість швидко вирішувати несправності в цьому рівні для безперервної парцездатності мережі. Основні характеристики рівня:

- високотехнічне обладнання та його надійність
- масштабованість

2) Розподільчий рівень – відповідає за зв'язок між рівнем доступом та рівнем ядра. Основна функція рівня це забезпечення маршрутизації, фільтрація та доступ до глобальної мережі, а також визначення того, хто має доступ до рівня ядра. Цей рівень визначає найшвидший спосіб доступу до запитів мережевих послуг, наприклад як запит файлу пересилається на сервер і якщо потрібно, пересилається на рівень ядра. Цей рівень зазвичай складається з маршрутизаторів і багаторівневих комутаторів. За допомогою даного рівня розподіляється все навантаження на мережу. Основні характеристики рівня:

- зв'язок між підмережами
- фільтрація трафіку
- розподіл навантаження.

3) Рівень доступу – контролює доступ користувачів до ресурсів мережі. Цей рівень зазвичай містить комутатори і точки доступу, які забезпечують зв'язок між робочими станціями та серверами. Можна керувати контролем доступу та політикою, створювати окремі домени колізій і впроваджувати захист портів. Зазвичай цей рівень потребує більш пильного налаштування захисту адже в цьому рівні підключаються робочі станції. Основні характеристики рівня:

- масштабованість
- безпека
- контроль доступу та політика.

Так як будь яка локальна мережа складається з багатьох пристроїв, для того щоб полегшити налаштування IP-адресації доцільно використовувати DHCP сервера. Це дасть змогу робочим станціям які підключенні до мережі автоматично отримувати адресу, що значно заощадить час в налаштуванні мережі. Також в випадку якоїсь несправності швидко її знайти і виправити.

Будь яка мережа повинна містити сервер в якому будуть зберігатися дані,

						4

налаштовуватися користувачі мережі а також налаштовуватися програмне забезпечення яке дозволить користувачам мережі в ньому працювати. Для цієї ролі ідеально підходить Windows Server 2019. В ньому є всі функції які дозволяють зручно налаштовувати мережу та користувачів в ній.

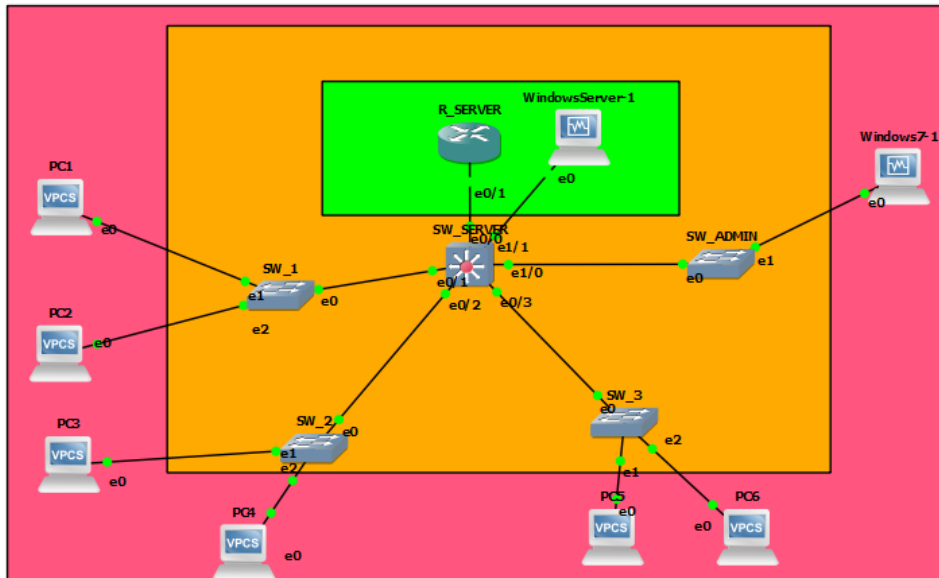


Рисунок 2.1 – Трирівнева модель мережі.

На рисунку 2.1 можна спостерігати розроблену трирівневу ієрархічну структуру мережі. Розберемо кожний рівень окремо.

Рівень ядра складається з одного маршрутизатора R_SERVER та серверу WindowsServer-1, які відповідають за працездатність мережі.

Розподільчий рівень складається з 5 комутаторів. Виділимо комутатор SW_SERVER на якому було налаштовано DHCP сервер. За допомогою даного налаштування в мережу легко додавати нових користувачів.

Рівень доступу складається з 7 віртуальних машин, які і виступають у ролі користувачів даної мережі.

2.3 Вибір обладнання та програмного забезпечення.

При проектуванні і розробці мережі, потрібно вибрати надійне обладнання та програмне забезпечення, тому що кожен пристрій в мережі виконує свою і роботу і від того як він працює буде залежити працездатність мережі, працездатність

користувача мережі. Роблячи висновок до з цього, можна обрати саме таке програмне забезпечення, що включає в себе:

1. Використання надійного і вкошвидкісного маршрутизатора.
2. Використання потужного комутатора який включає в себе велику кількість портів для об'єднання мережі і який зможе виступати у ролі DHCP сервера.
3. Використання Windows Server, який буде виступати у ролі сервера та забезпечувати роботу користувачів в мережі.
4. Налаштування захисту для надійної роботи мережі.
5. Використання ОС Windows 7 та Windows 10 для роботи користувачами мережі.
6. Налаштування віддаленого доступу до пристроїв мережі.

Для побудови будь якої мережі необхідно обрати якісне обладнання яке буде відповідати вимогам мережі. Було обрано обладнання від фірми Cisco. Воно має ряд переваг які виділяють його, а саме[14]:

- Перша і незаперечна перевага це надійність обладнання, яка вже перевірена роками. Компанія використовує високоякісні компоненти у всіх своїх пристроях від матеріалу корпусу до мікропроцесорів чипів на платах. Все це відіграє ключову роль на кінцевому результаті.

- Друге, це ширина модельного ряду. Не один із конкурентів не може надати таку різноманітність рішень для малого бізнесу і для великих компаній. Особлива увага також заслуговує політика компанії Cisco Systems, щодо пошуку та придбання початківців і перспективних компаній, чиї ідеї можуть бути інтегровані в обладнання Cisco.

- Третя дуже важлива відмінність це гнучкість та потужність програмного забезпечення. Це дозволяє за допомогою одного пристрою реалізовувати різні задачі, будь то маршрутизація, комутація, захист і т.д. Тобто достатньо ввести лише декілька команд або налаштувати на графічному інтерфейсі, щоб підняти на пристрої нові сервіси. Що дасть змогу з економити бюджет компанії.

- Четверте – рівень підтримки. Для того щоб знайти будь-яку інформацію що до налаштування чи іншу специфічну інформацію, достатньо пошукати рішення в дуже

						4

докладній і різноманітній документації на сайті cisco. В компанії уже траплялися випадки коли користувачі знаходили не зовсім коректну роботу програмного забезпечення і cisco випускала оновлення саме під цю проблему конкретного клієнта.

- Ну і останній не менш важливий фактор – рівень надаваної гарантії. Гарантійна підтримка в компанії надається на будь-яке обладнання, навіть старе та практично на будь-який термін. Така гарантія дозволяє отримати повну заміну пристрою або будь-якої несправної частини. Такий вид підтримки надають лише деякі компанії-виробники, що свідчить про те що компанія цінить клієнтів та серйозного підходу.

Тобто на базі обладнання Cisco можна знайти рішення для будь-якого завдання як і для невеликих компаній так і для великих корпорацій.

Підсумовуючи із вище сказаного, мережеве обладнання Cisco, як найкраще підходить для розробки мереже, тому і буде використано в даній мережі, зокрема комутатор Cisco Catalyst 2960 (Рисунок2.2) а також маршрутизатор Cisco 2900 (Рисунок2.3).



Рисунок 2.2 – Комутатор Cisco Catalyst 2960

Чому саме Cisco Catalyst 2960, тому що він має ряд таких переваг як[15]:

1. Мають достатню кількість портів для того щоб об'єднати всю мережу, існують з 24 портами чи 48, в залежності від мережі (для побудови мережі було вибрано з 24 портами)
2. Комутатори цієї моделі підтримують USB-прилади, що в подальшому

						4

допоможе в резервному копіюванні и дозволить зберігати інформацію в зручних місцях.

3. Дуже легкий в налаштуванні.

4. Надійний пристрій що дозволить мережі працювати безперебійно а також підтримує налаштування захисту що являє собою одну із найважливіших функцій будь-якої мережі.



Рисунок 2.3 – Маршрутизатор Cisco 2900

Перевагами даного пристрою є те що його також легко налаштовувати, високий рівень безпечного підключення, а також сумісність з новими технологіями[16].

Також в мережі було використано Windows Server, який виконує функцію файлового сервера, сервера служби веб-застосунків, сервера терміналів, поштового сервера, сервера віддаленого доступу, служби DNS (доменних імен), служби каталогів, сервера потоків мультимедіа та інші.

Дуже багато особливостей Windows Server дають можливість співробітникам організації працювати продуктивніше. Файлові служби та служби друку дозволяють керувати файловими ресурсами. У той же час зберігається безпека та доступ для користувачів. Служба каталогів у Windows Server називається Active Directory. Завдяки цій службі зберігаються відомості про мережеві об'єкти. Крім того, Active Directory дозволяє адміністратору швидко знайти цю інформацію. Ця служба також спрощує роботу з проектування, розгортання та управління каталогами мережі. В оптимальній роботі Active Directory допоможе консоль керування груповими політиками[17].

Така модель має деякі недоліки. По-перше, якщо є досить багато загальних ресурсів, то доведеться створити багато груп. По-друге, не можна проконтролювати

						4

доступ з урахуванням будь-яких атрибутів користувача або параметрів пристрою, з якого здійснюється підключення. Достатньо членства користувача у певній групі. По-третє, досить проблематично здійснити складні сценарії доступу. Користувач може випадково викласти закриту інформацію у спільну папку, де кожен із членів групи може її прочитати.[18]

Для розробки самої мережі буде використано GNS3. GNS3 (Graphical Network Simulator) – це безкоштовне програмне забезпечення, яке дає можливість створювати топологію від маленької, яка складається з декількох пристроїв, так і до великих, які складаються з багатьох пристроїв, віртуальних машин і тому подібне. Для цього не потрібне реальне обладнання, адже GNS використовує емулятори того самого обладнання, що дає змогу максимально наблизитися до реального. Основна перевага GNS заключається в тому, що він дозволяє використовувати віртуальні машини операційних систем. Тобто це дозволяє нам створювати майже реальну мережу якогось підприємства чи компанії. Все ж таки будь-яке програмне забезпечення має свої недоліки, і GNS не виключення. Для того, щоб зручно і безперешкодно працювати в GNS, потрібно мати достатньо потужний ПК, адже розробка мереж це ресурсозатратний процес. Тому не на всіх ПК є можливість працювати в даному симуляторі[19].

Для того, щоб додавати та використовувати різні операційні системи, буде використано Virtual Box. Virtual Box – це програмне забезпечення, яке дозволяє додавати, використовувати, видаляти та працювати в різних операційних системах, при цьому не змінюючи свої. До основних переваг програми можна віднести:

- зручний та простий інтерфейс;
- тестування різних ОП не змінюючи свої основної;
- налаштування ресурсо-затратності різних ОП[20].

Висновок до розділу 2

В даному розділі було розроблено схему з'єднання пристроїв між собою, розроблено схему IP-адресації мережі. Було описано доцільність використання в мережі DHCP сервері.

						4

Було розглянуто трирівневу ієрархічну модель мережу, і прийняте рішення в її використанні в подальшому побудові мережі.

Також було вибрано обладнання яке підходить для використання в мережі. Розглянуто його переваги для даної мережі. Було вибрано підходяще програмне забезпечення, за допомогою якого можна побудувати мережу і реалізувати всі задумки. А також було вибрано операційну систему сервера, який ідеально підходить для розробки такої мережі.

						4

РОЗДІЛ 3 НАЛАШТУВАННЯ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ КОРОСТЕНСЬКОГО МІСЬКРАЙОНОГО СУДУ

3.1 Базове налаштування мережі

В цьому підрозділі буде розроблено схему мережі та проведено базове налаштування пристроїв мережі. Загальна схема мережі, що розробляється, зображена на рисунку 3.1.

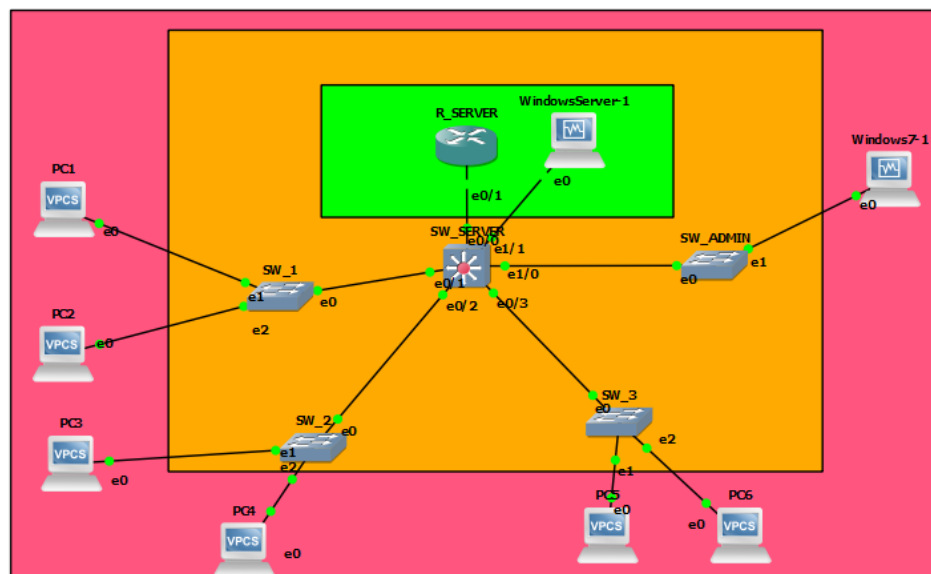


Рисунок 3.1 – Схема мережі

Далі необхідно налаштувати маршрутизацію мережі. На рисунку 3.2 можна побачити налаштування адресації.

На комутаторі необхідно об'єднати всі інтерфейси для локальної мережі. На рисунку 3.3 будуть налаштування.

Також за DHCP сервер буде відповідати маршрутизатор, тому потрібно його налаштувати.

На рисунку 3.4 було налаштовано DHCP адресацію на маршрутизаторі.

```
R_SERVER(config)#int e0/1.1
R_SERVER(config-subif)#enca
R_SERVER(config-subif)#encapsulation dot1Q 1
R_SERVER(config-subif)#ip add 192.168.0.1 255.255.255.0
R_SERVER(config-subif)#exit
R_SERVER(config)#int e0/1
R_SERVER(config-if)#no sh
R_SERVER(config-if)#exit
R_SERVER(config)#
```

Рисунок 3.2 – Налаштування адресації мережі.

```
SW_SERVER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_SERVER(config)#int range e0/1-3,e1/0
SW_SERVER(config-if-range)#swit
SW_SERVER(config-if-range)#switchport access vlan 1
SW_SERVER(config-if-range)#exit
SW_SERVER(config)#
```

Рисунок 3.3 – Налаштування комутатора SW_SERVER

```
R_SERVER(config)#ip dhcp pool vlan 1
R_SERVER(dhcp-config)#network 192.168.0.0 255.255.255.0
R_SERVER(dhcp-config)#exit
R_SERVER(config)#ip dhcp ex
R_SERVER(config)#ip dhcp excluded-address 192.168.0.1
R_SERVER(config)#
```

Рисунок 3.4 – Налаштування DHCP сервера.

Далі необхідно провести базове налаштування Windows Server. На рисунку 3.5 проводимо налаштування IP-адресації.

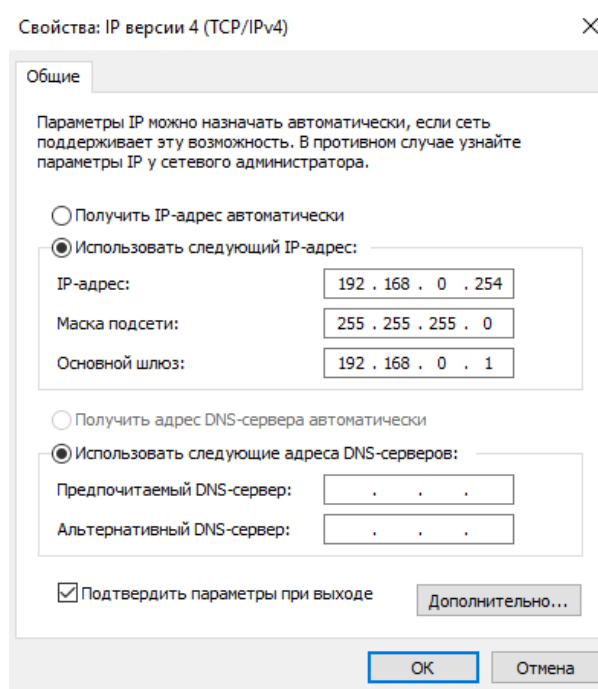


Рисунок 3.5 – Налаштування IP-адресації на Windows Server

Проведення базових налаштувань на Windows Server та установка потрібних служб. На рисунках буде показано 3.6 -

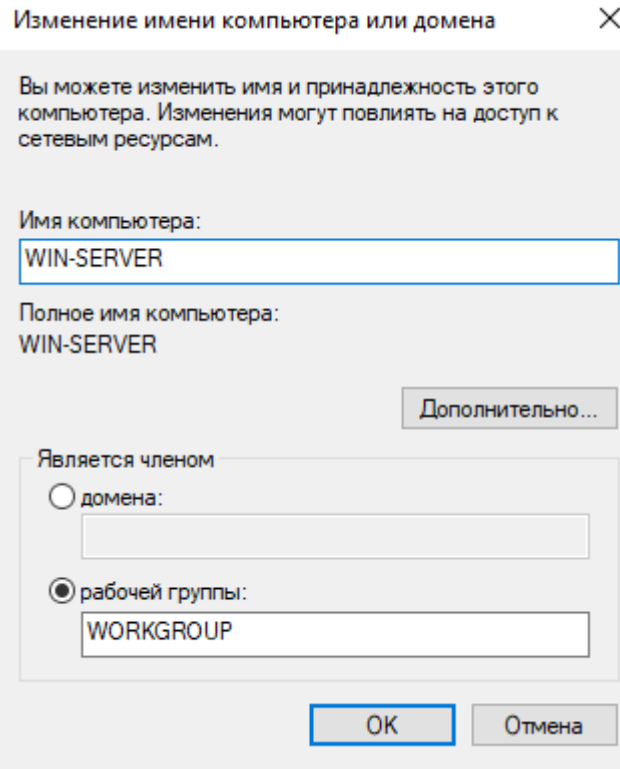


Рисунок 3.6 – Настройка Windows Server

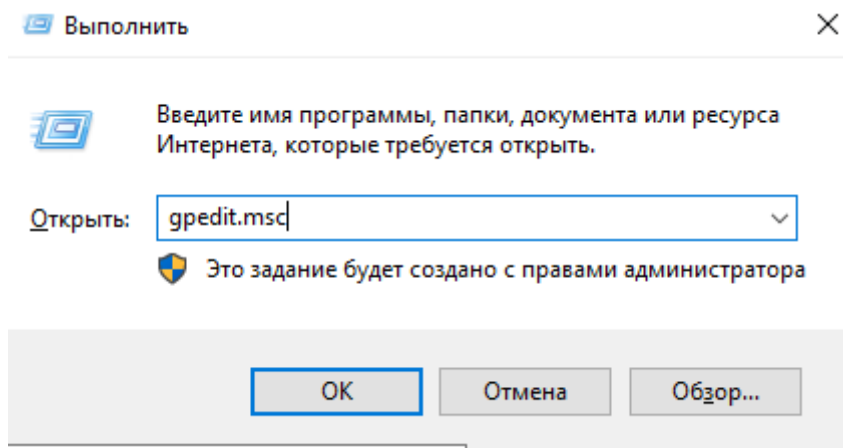


Рисунок 3.7 – Настройка NTP

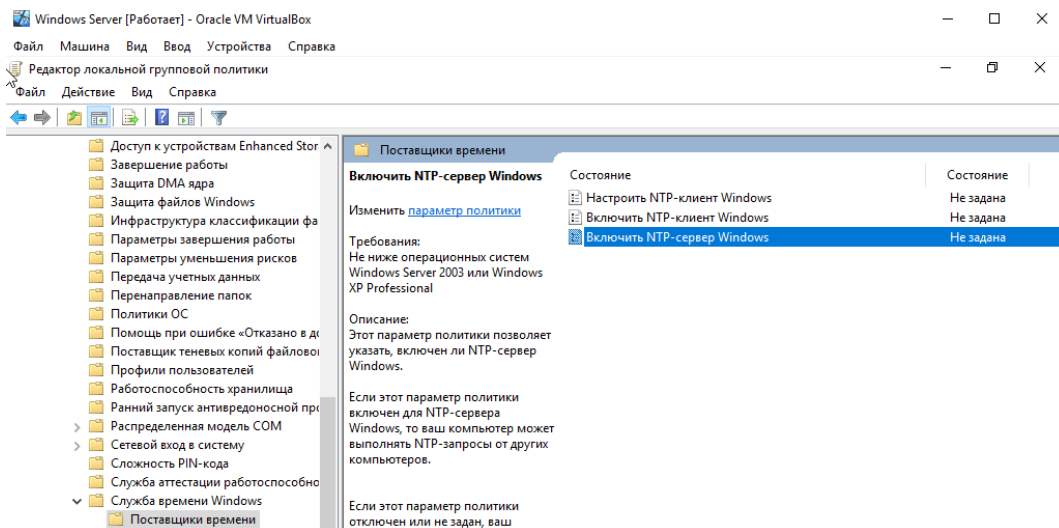


Рисунок 3.8 – Налаштування NTP

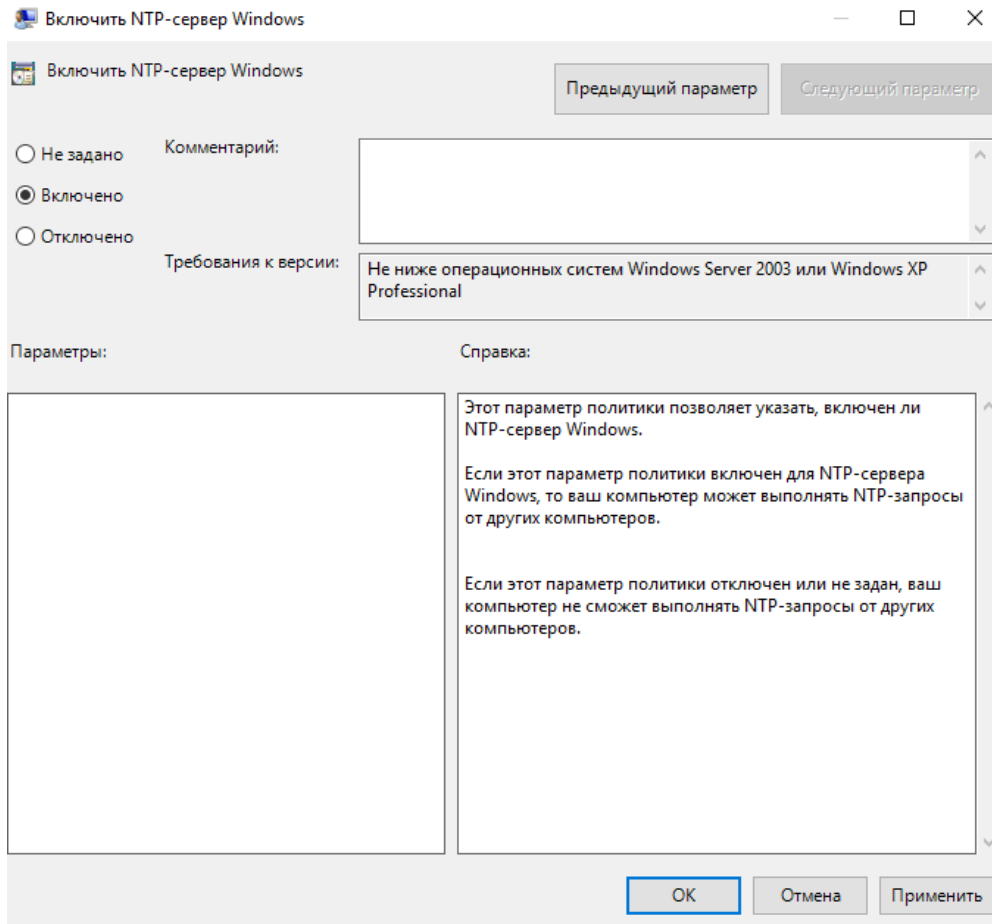


Рисунок 3.9 – Налаштування NTP

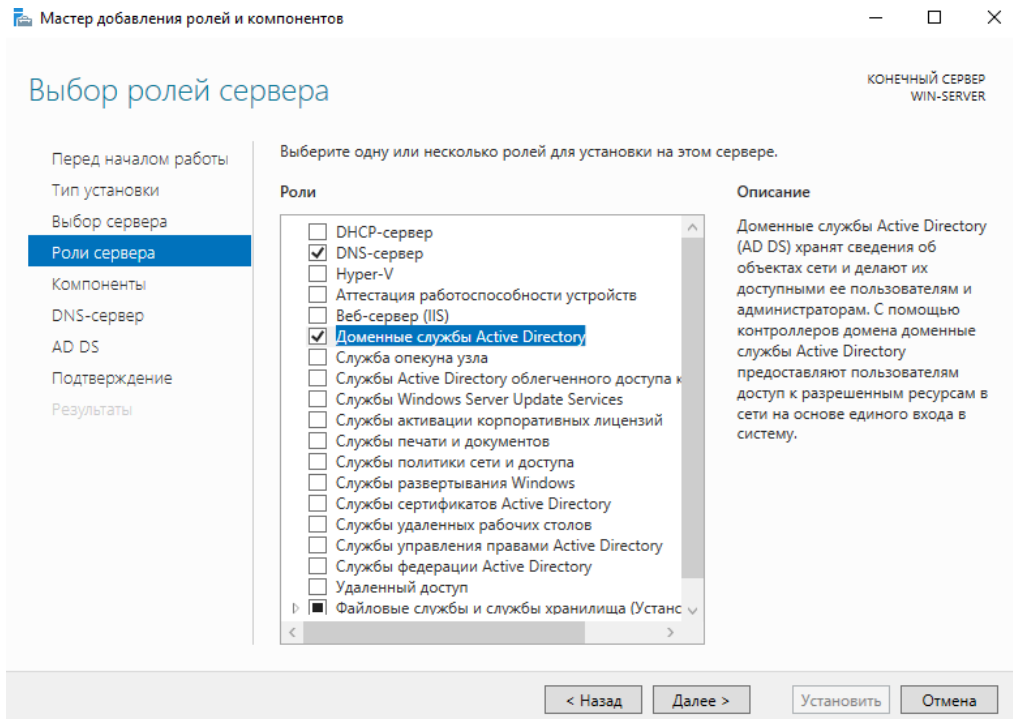


Рисунок 3.10 – Встановлення служб DNS-сервера, та Active Directory

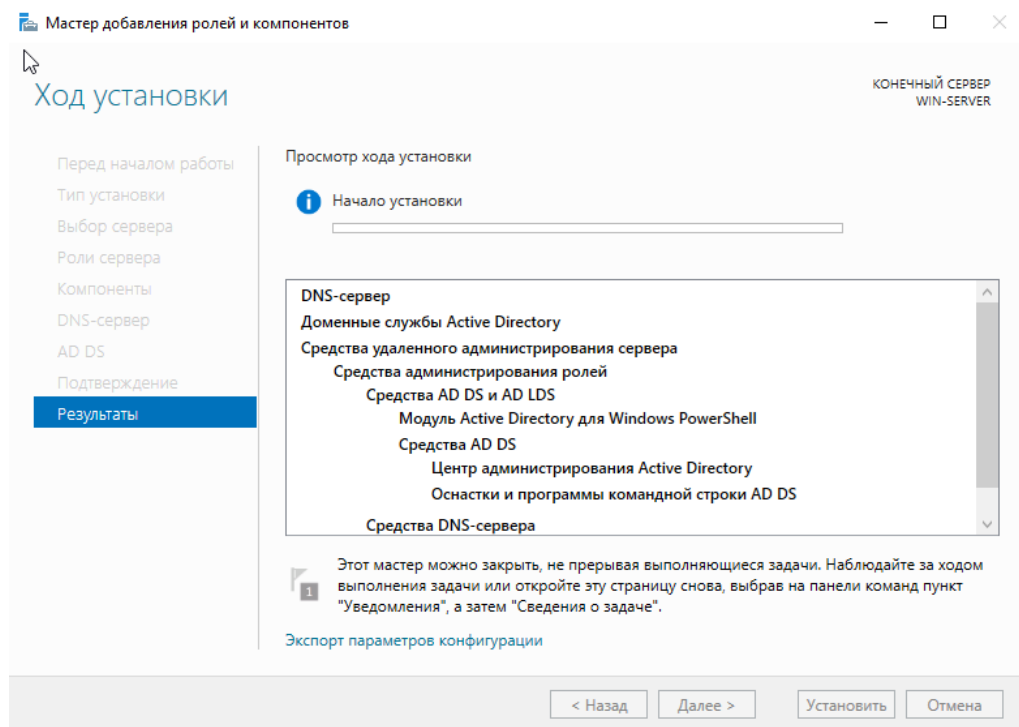


Рисунок 3.11 – Встановлення служб DNS-сервера, та Active Directory

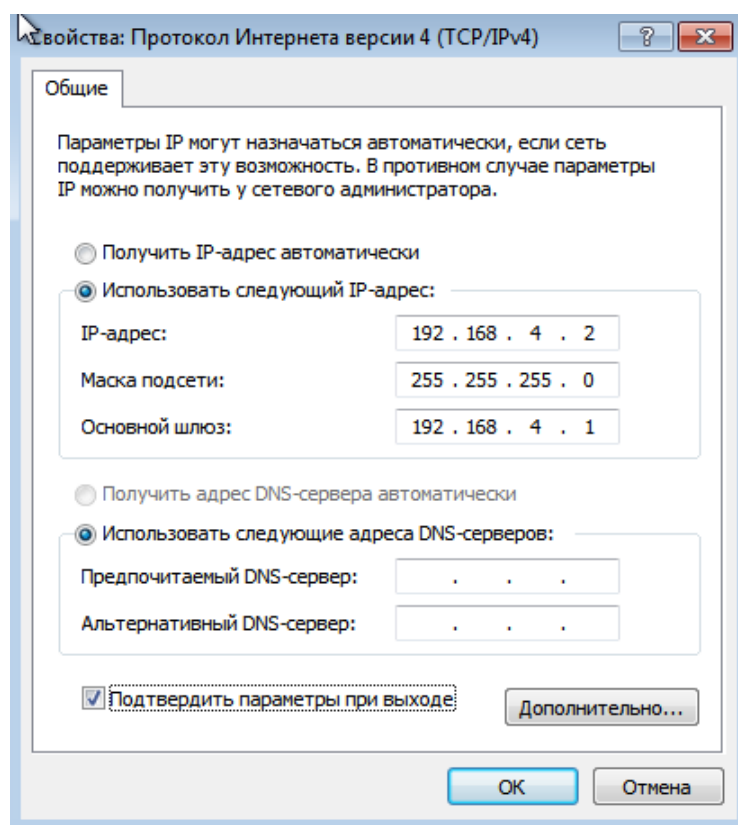


Рисунок 3.12 – Налаштування Windows 7

На рисунку 3.12 було проведено базові налаштування адресації на робочій станції Windows 7 яка буде виступати в ролі користувача мережі.

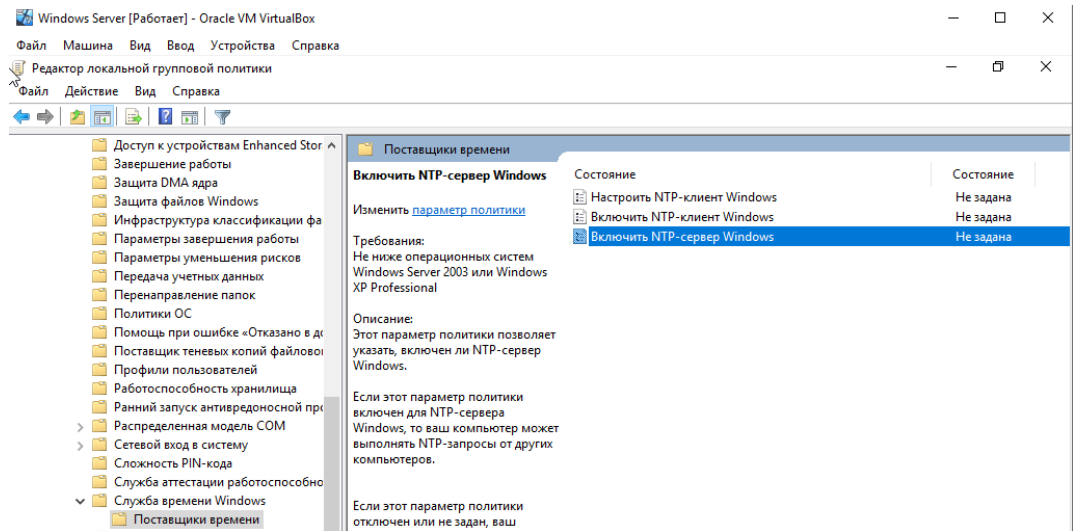


Рисунок 3.16 – Налаштування NTP

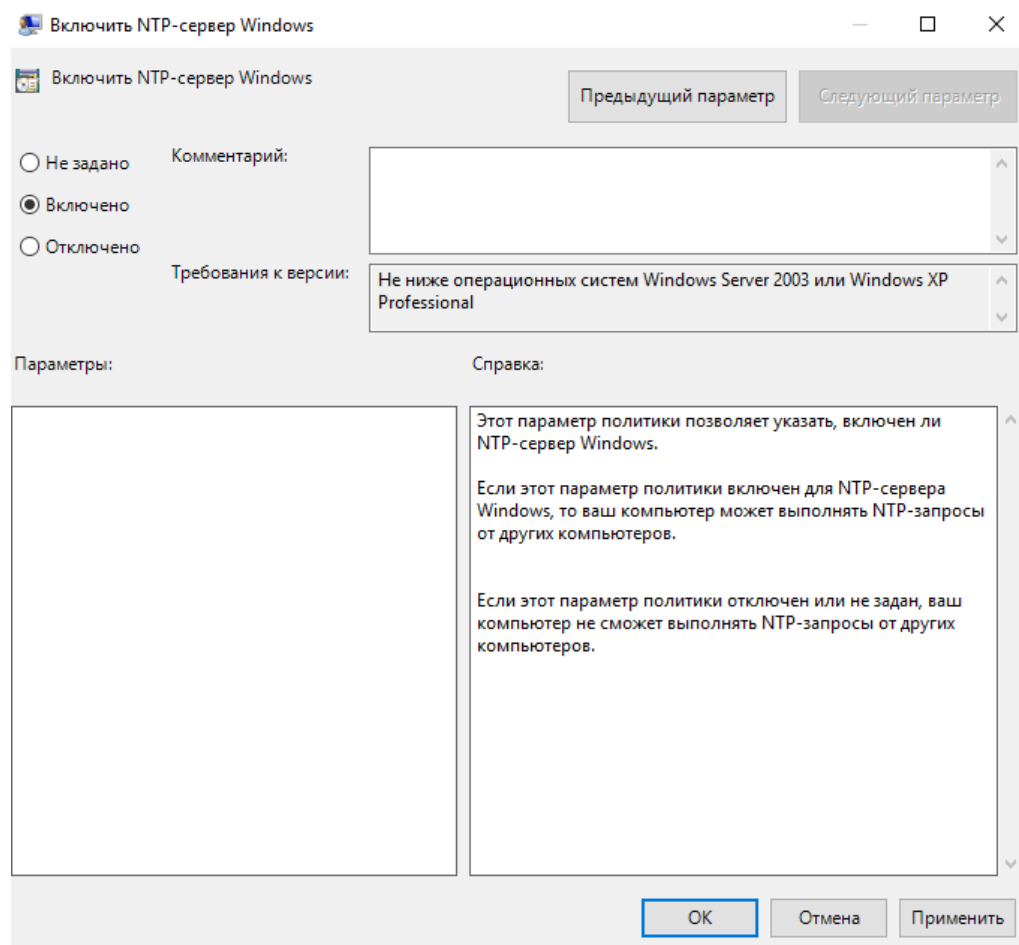


Рисунок 3.17 – Налаштування NTP

Після цього потрібно включити і налаштувати глобальні параметри конфігурації. (Рисунок 3.18)

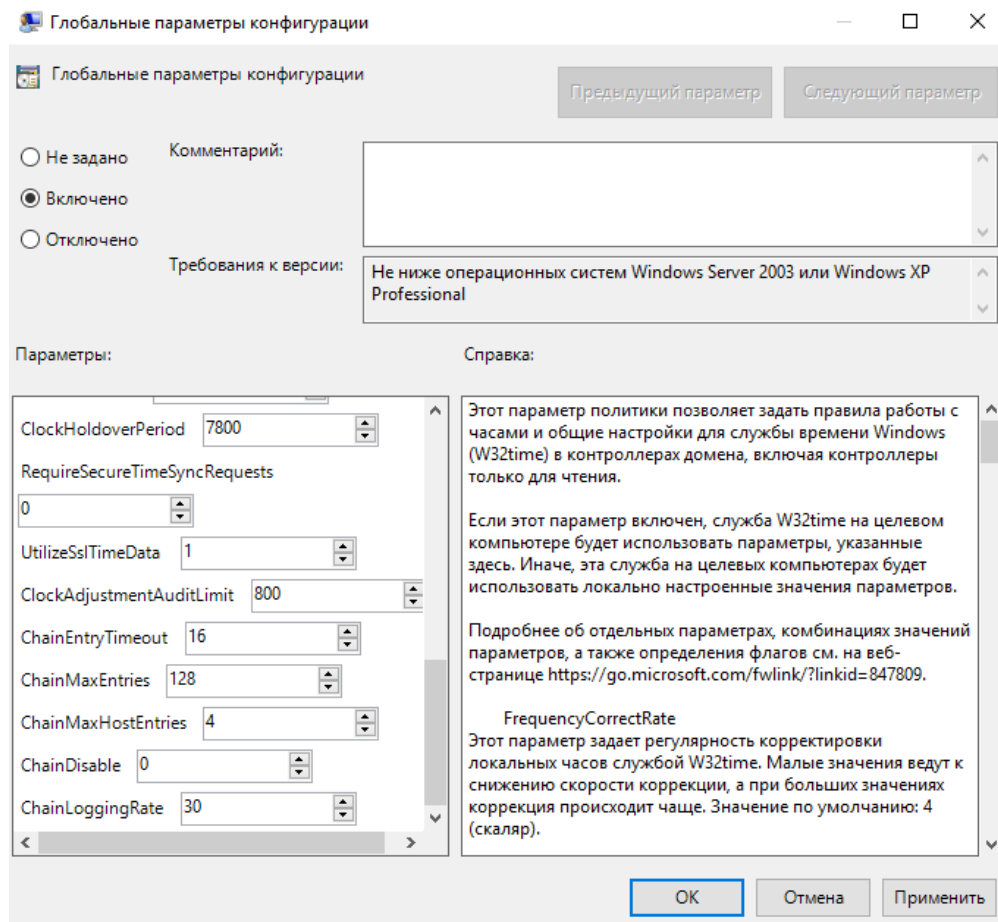


Рисунок 3.18 – Налаштування NTP

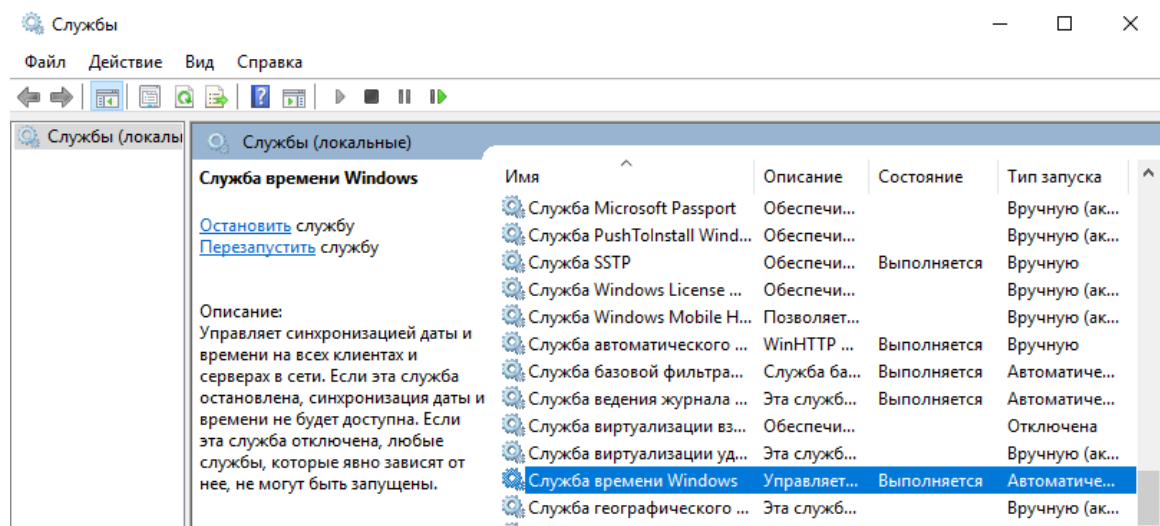


Рисунок 3.19 – Перевірка служби часу

Далі необхідно створити правило для користувачів мережі. (Рисунок 3.20 – 3.24)

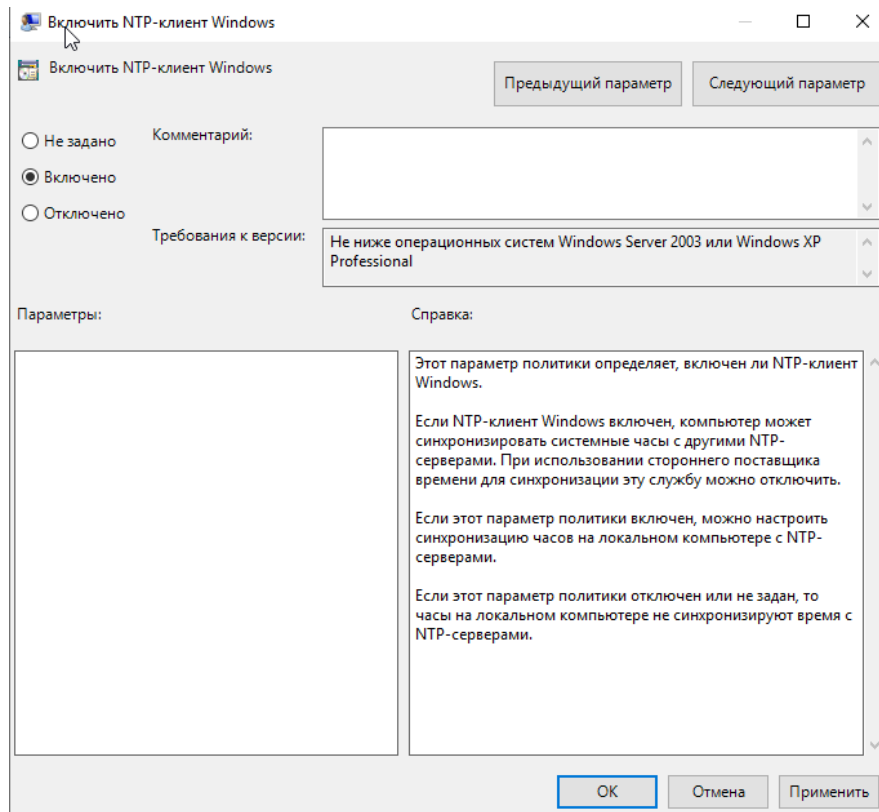


Рисунок 3.24 – Включения NTP клієнта

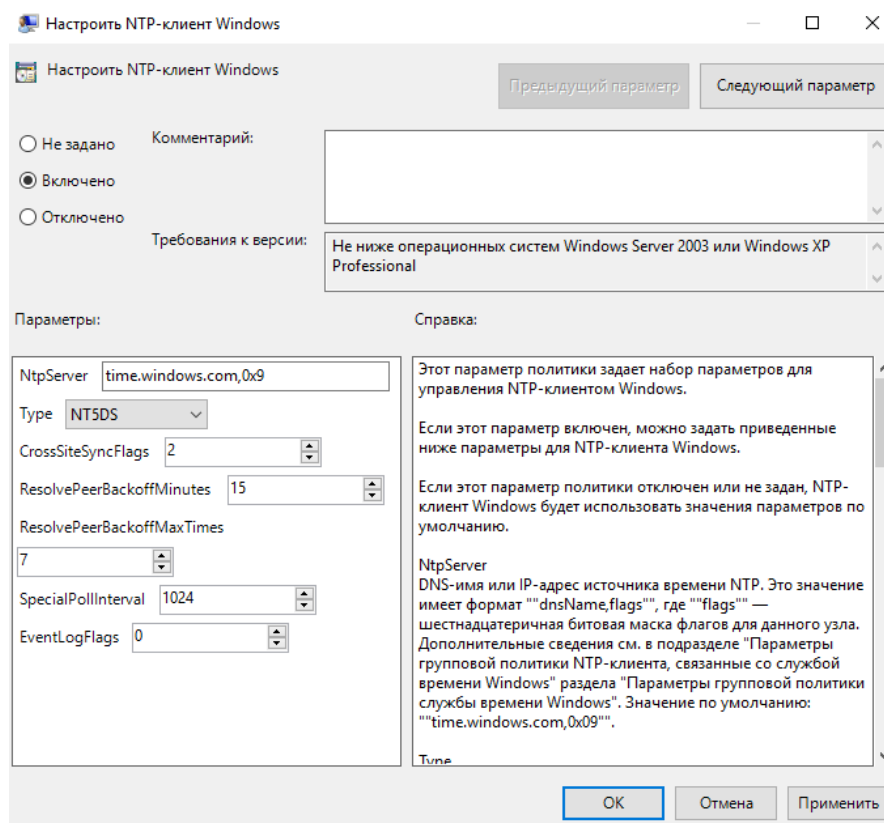


Рисунок 3.25 – Налаштування NTP клієнта

Тепер необхідно налаштувати RDP – це протокол за допомогою якого можна підключитися до іншого комп'ютера через мережеве з'єднання. Це необхідно для

						4

покращення адміністрування серверу, щоб адміністратор мережі міг підключатися до серверу віддалено і працювати в ньому. Спочатку необхідно створити користувача, якому буде надана так можливість. (Рисунок3.26)

Новый пользователь ? X

Пользователь: Admin

Полное имя:

Описание:

Пароль:

Подтверждение:

☒ Требовать смены пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

Справка Создать Закрыть

Рисунок 3.26 – Створення користувача

Тепер необхідно надати користувачу відповідні ролі. (Рисунок 3.27-3.39)

Свойства admin

Удаленное управление

Профиль служб удаленных рабочих столов Входящие звонки

Общие Членство в группах Профиль Среда Сеансы

Член групп:

Пользователи

Добавить... Удалить

Изменения членства в группах вступят в силу после следующего входа пользователя в систему.

OK Отмена Применить Справка

Рисунок 3.27 – Надання ролей

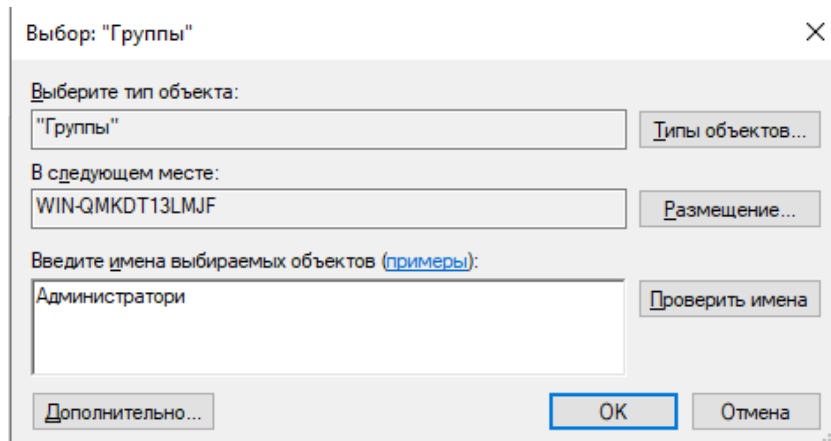


Рисунок 3.28 – Надання ролей

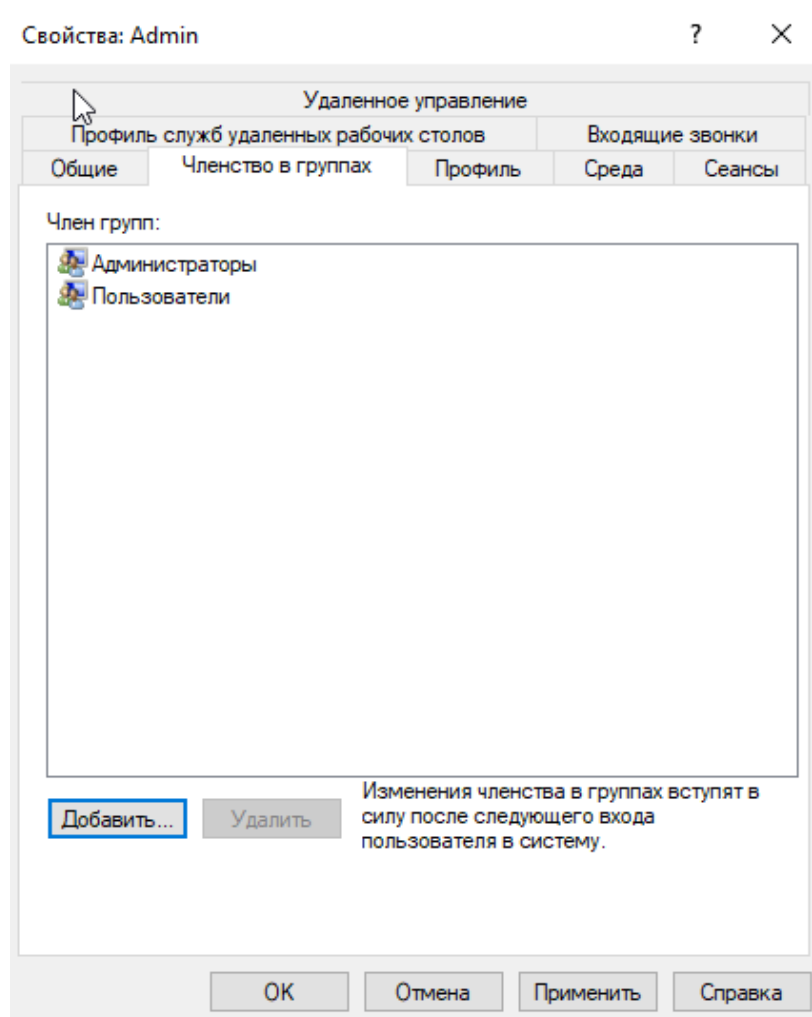


Рисунок 3.29 – Надання ролей

Далі необхідно запустити саму службу віддаленого робочого стола і надати доступ до неї користувачу якого було створено.(Рисунок3.30-3.32)

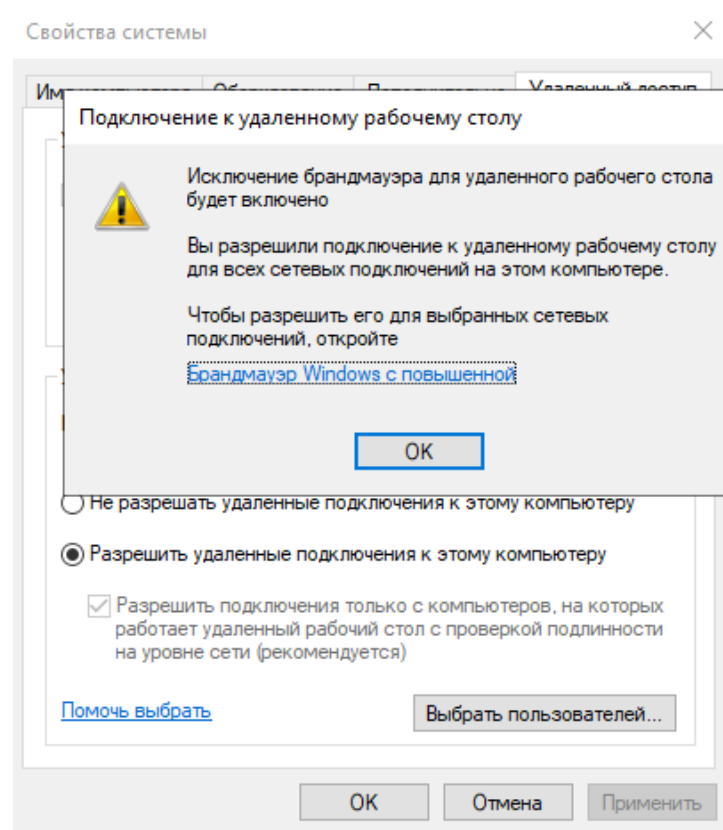


Рисунок 3.30 – Налаштування віддаленого робочого стола

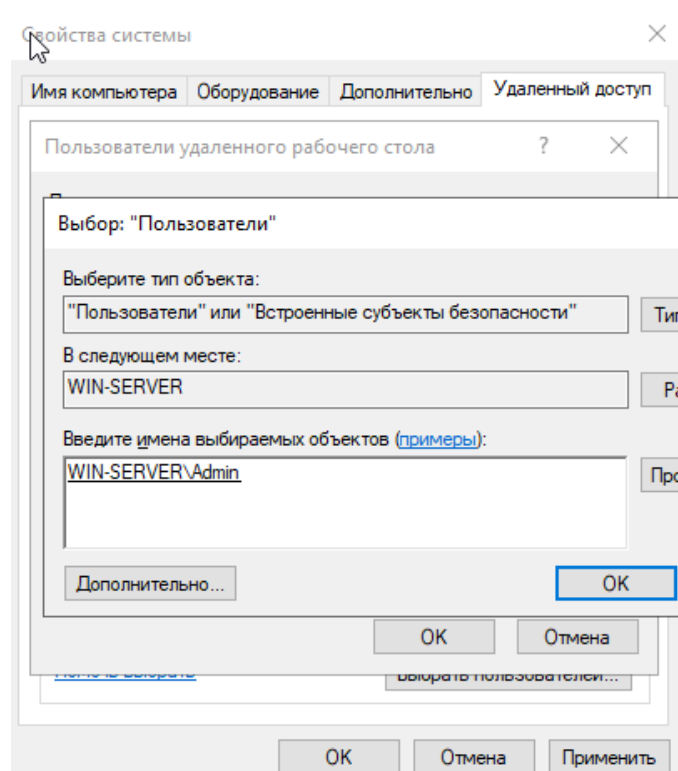


Рисунок 3.31 – Налаштування віддаленого робочого стола

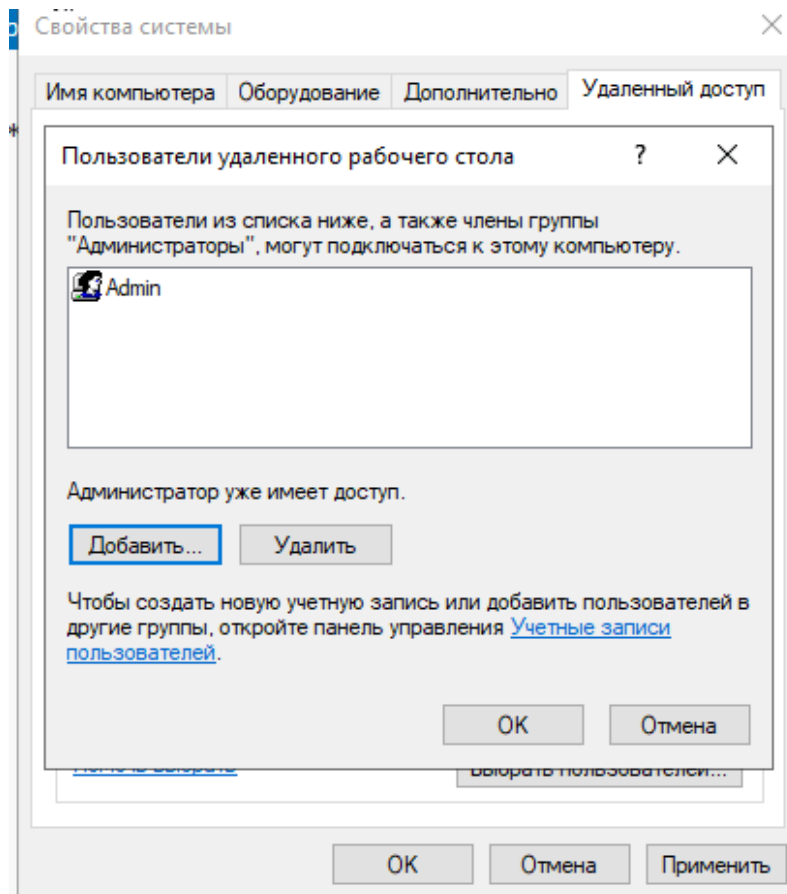


Рисунок 3.32 – Налаштування віддаленого робочого стола

Тепер користувач Admin може підключатися до сервера зі своєї робочої станції.

Перейдемо до налаштування служби Active Directory – це служба яка існує для спрощення адміністрування мережі. Вона дозволяє управляти робочими станціями які підключенні до мережі, дозволяє об'єднати всі ці станції і проводити роботи з ними об'єднано а не з кожною окремо.

Спочатку налаштуємо DNS сервер. (Рисунок3.33)

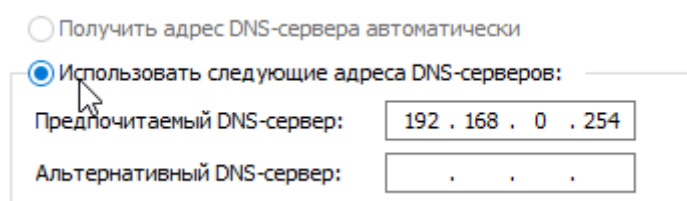


Рисунок3.33 – Налаштування DNS сервера

Далі необхідно налаштувати рівень контролю домену. (Рисунок 3.34-3.37)

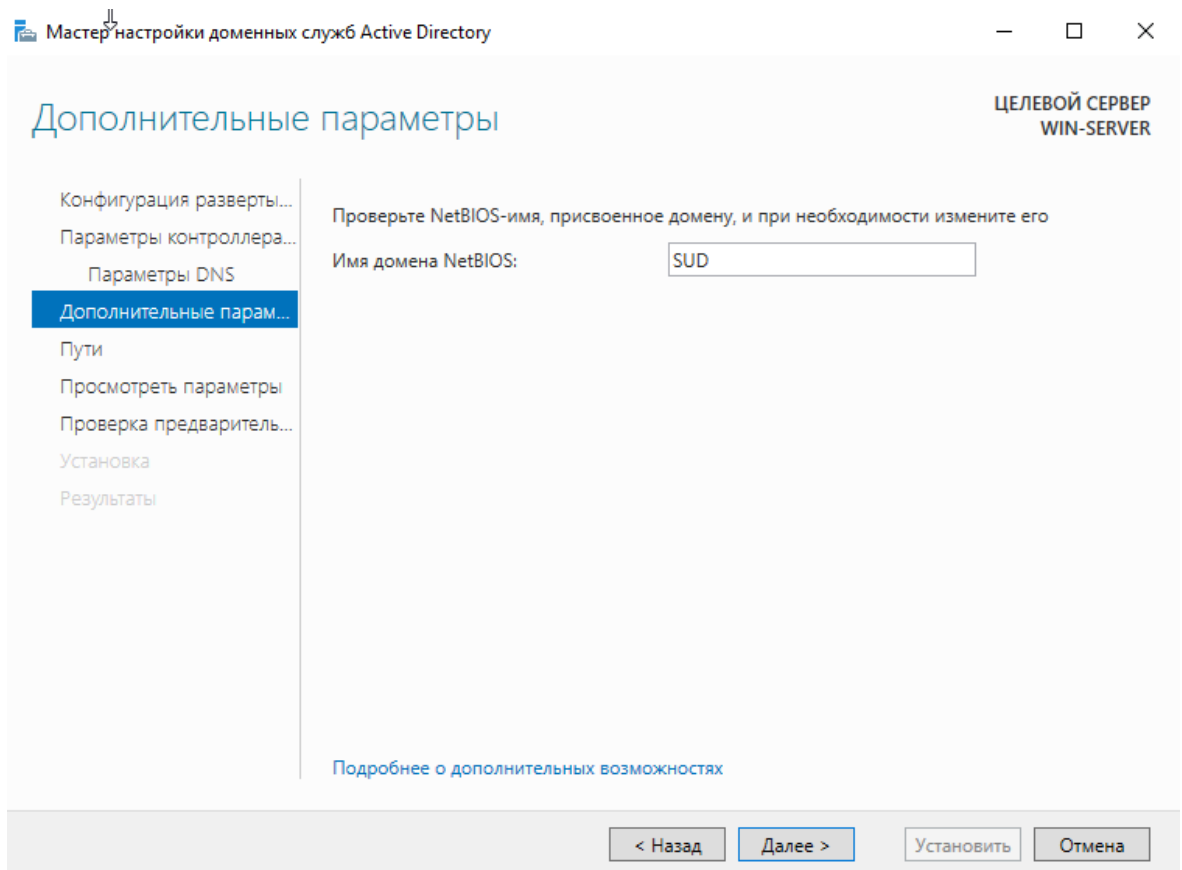


Рисунок 3.36 – Налаштування рівень контролю домену.

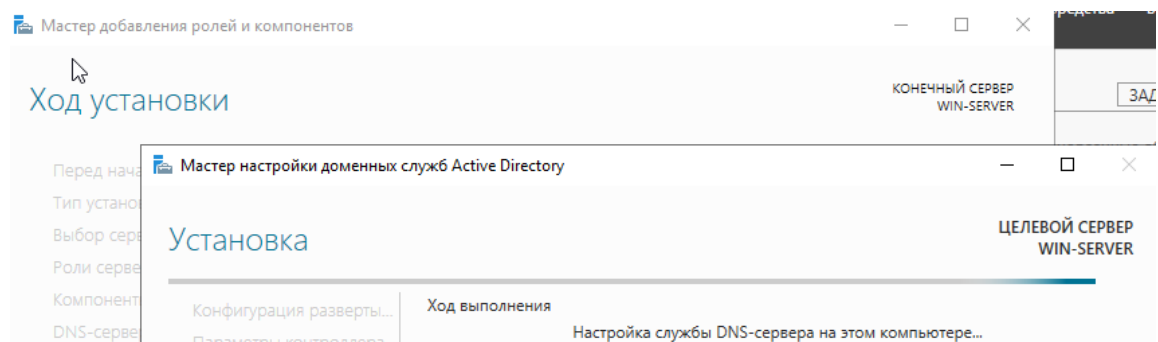


Рисунок 3.37 – Налаштування рівень контролю домену.

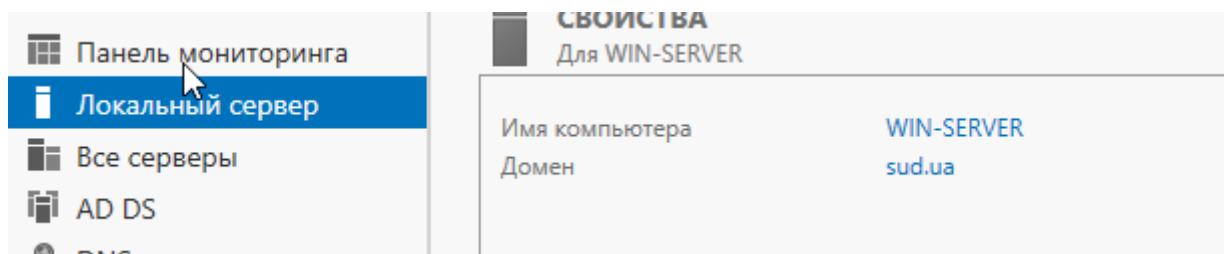


Рисунок 3.38 – Виконання налаштувань

Як можна побачити на рисунку 3.38 налаштування пройшли успішно.

Після цього необхідно створити користувачів які в подальшому будуть

працювати в цій мережі. Спочатку в DNS потрібно створити зону зворотного перегляду, для того щоб створити користувачів, а також бачити саме які робочі станції підключені до мережі. (Рисунок 3.39-

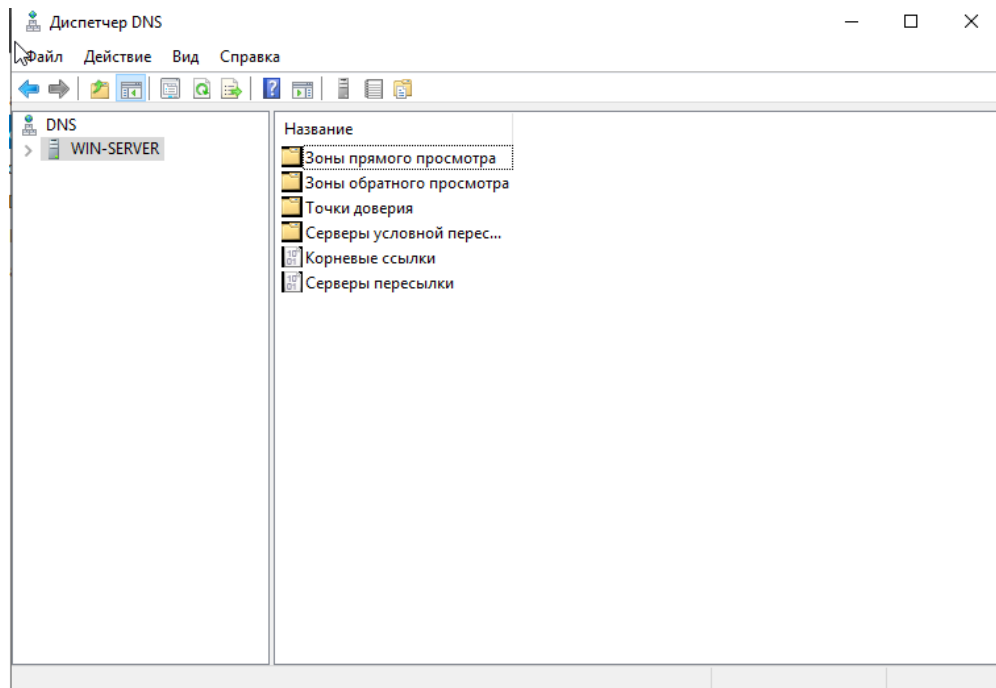


Рисунок 3.39 – Створення зони зворотного перегляду

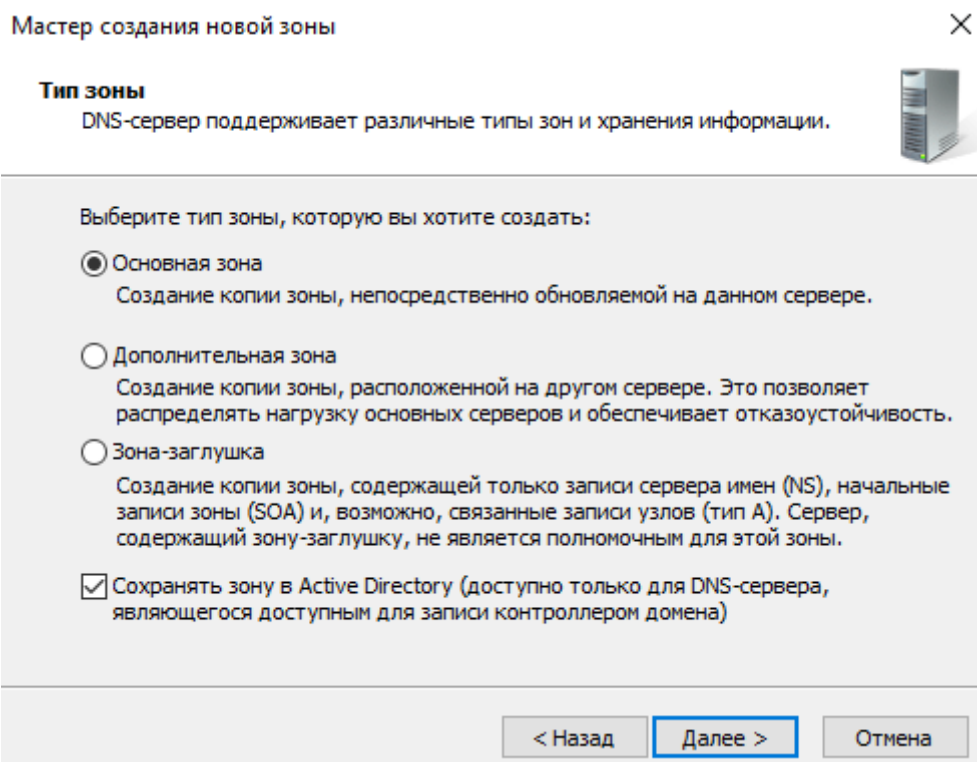


Рисунок 3.40 – Створення зони зворотного перегляду

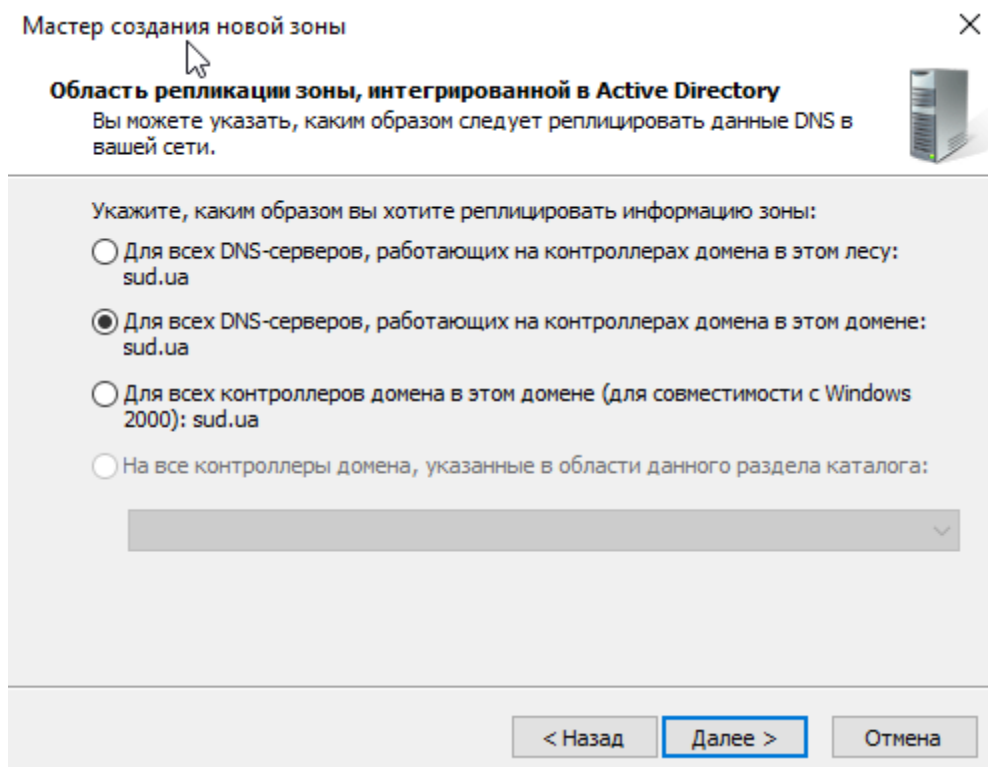


Рисунок 3.41 – Створення зони зворотного перегляду

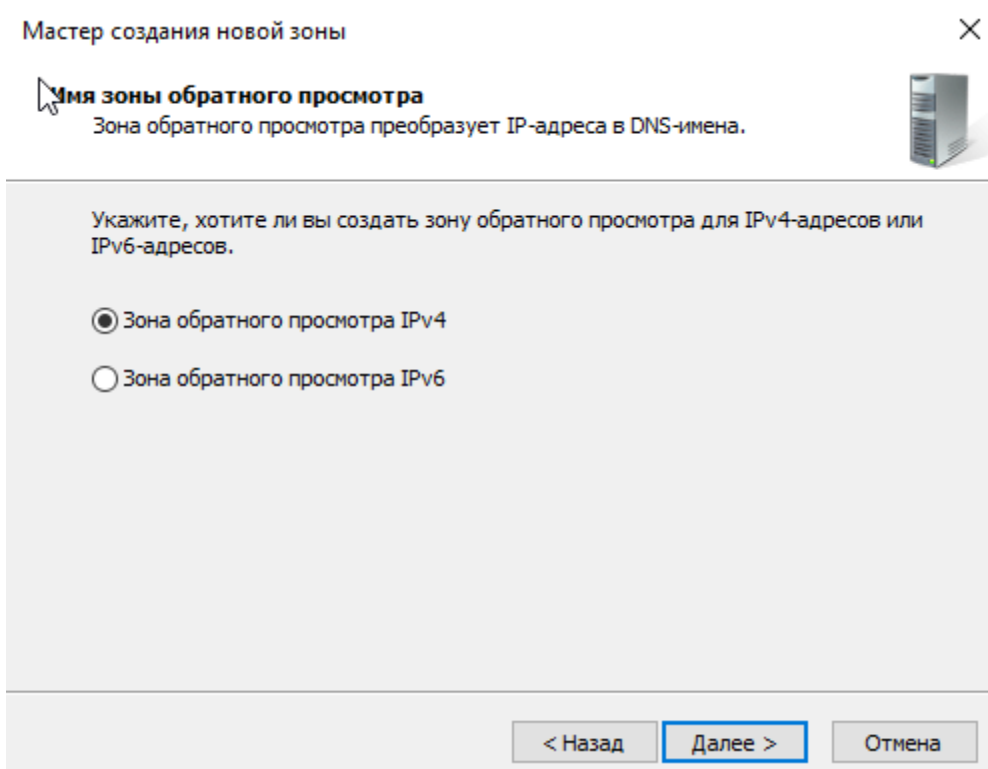


Рисунок 3.42 – Створення зони зворотного перегляду

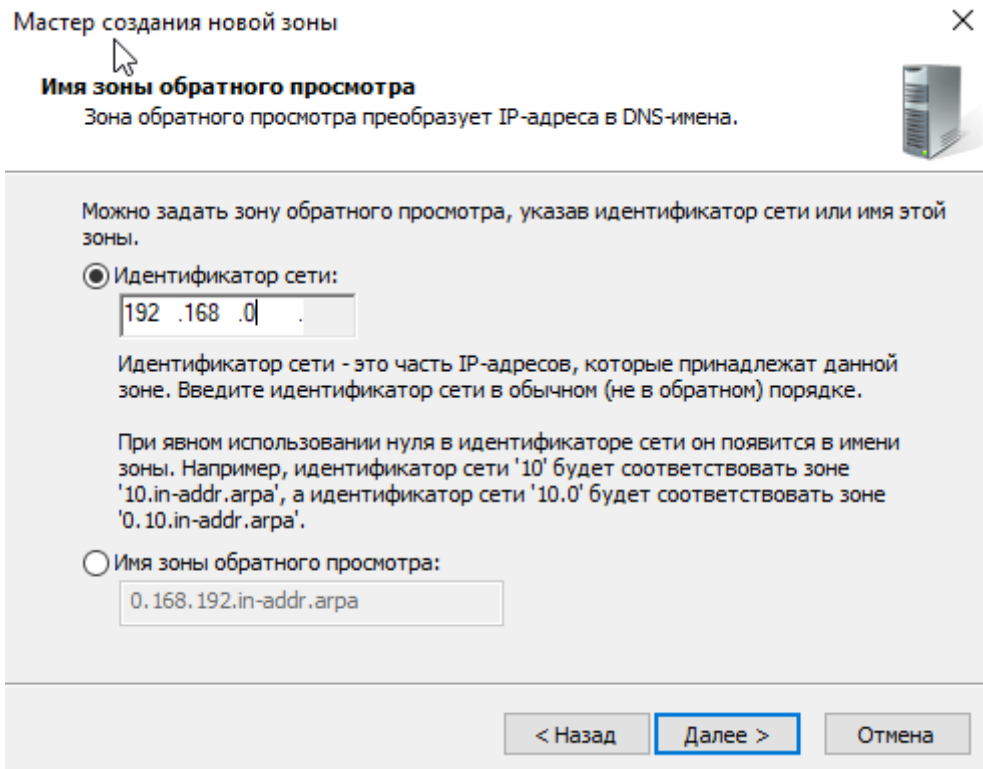


Рисунок 3.43 – Створення зони зворотного перегляду

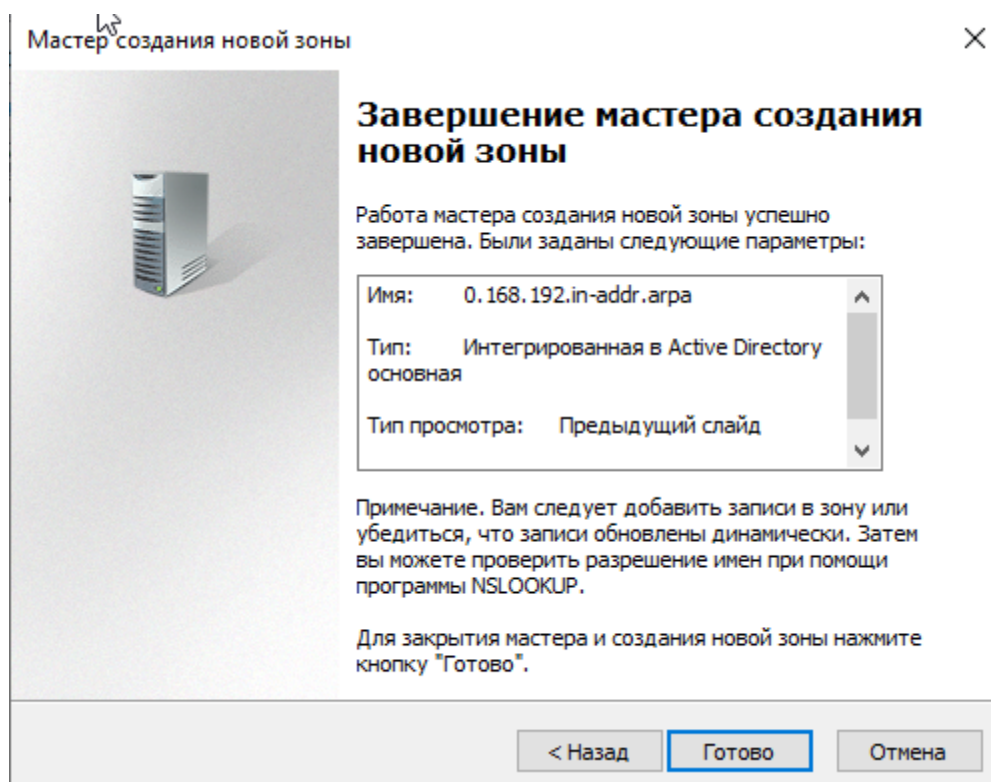


Рисунок 3.44 – Створення зони зворотного перегляду

Саме після цього вже можна створювати користувачів, за допомогою яких користувачі мережі можуть працювати за робочими станціями. З початку і для подальшого необхідно створити підгрупи. Вони потрібні для того щоб знати ким

працює користувач, налаштовувати спільні налаштування для групи користувачів і т.д.(Рисунок3.44-3.45)

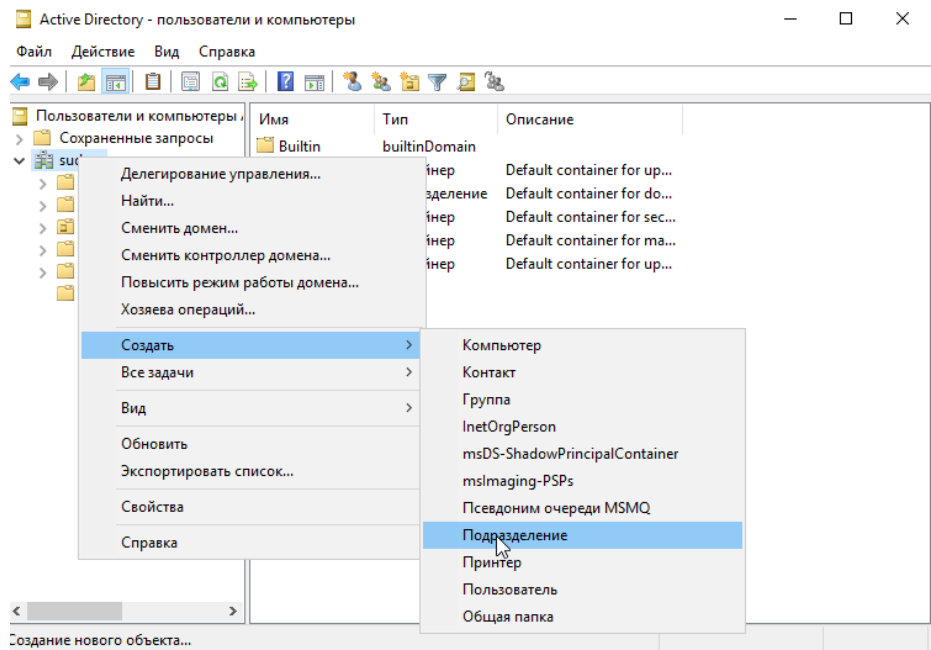


Рисунок 3.44 – Створення підгрупи

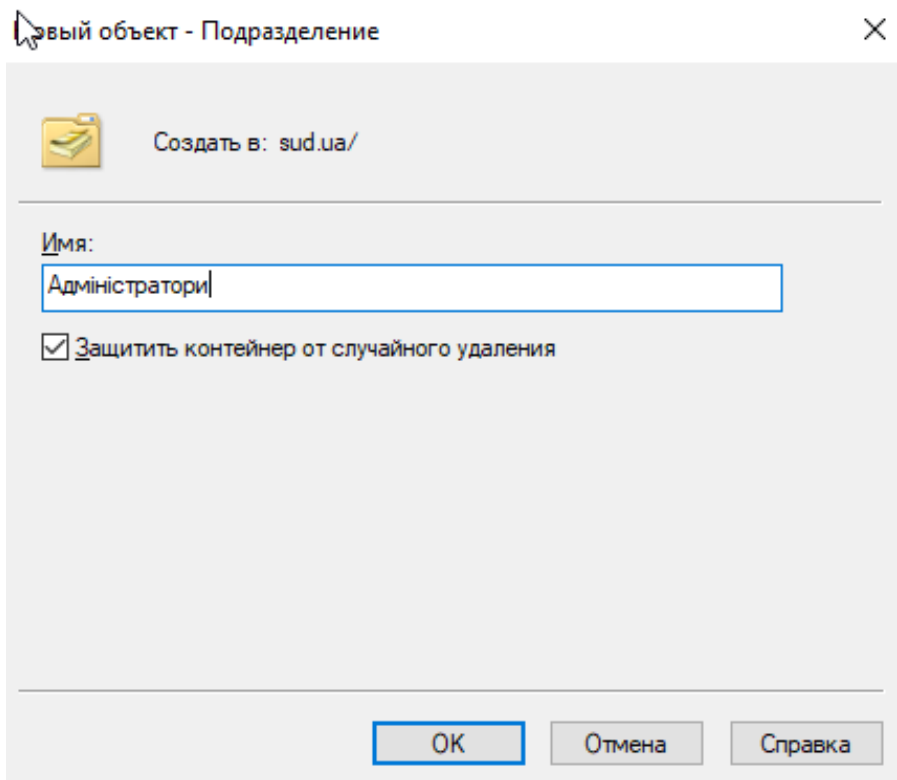


Рисунок 3.45 – Створення підгрупи

Далі вже можемо створювати користувача. (Рисунок3.46 – 3.47)

Новый объект - Пользователь

Создать в: sud.ua/Адміністратори/Users

Имя: Andriy Инициалы:

Фамилия: Savchuk

Полное имя: Andriy Savchuk

Имя входа пользователя: andriy @sud.ua

Имя входа пользователя (пред-Windows 2000): SUD\ andriy

< Назад Далее > Отмена

Рисунок 3.46 – Створювання користувача

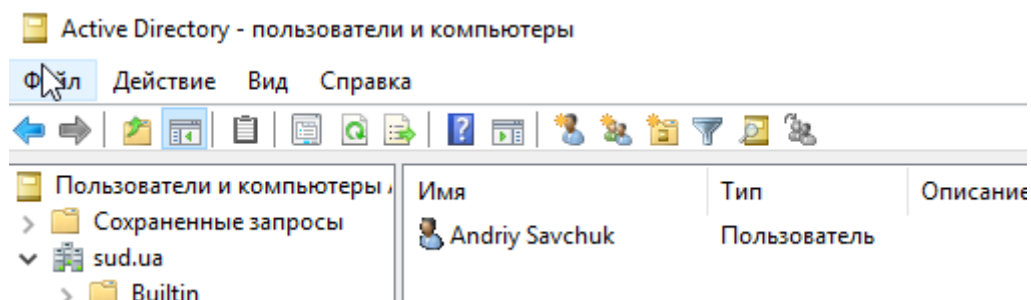


Рисунок 3.47 – Створений користувач

Для того щоб даний користувач міг працювати в мережі і підпорядковувася їй робочі станції які будуть підключені до мережі необхідно також підключити до домену.

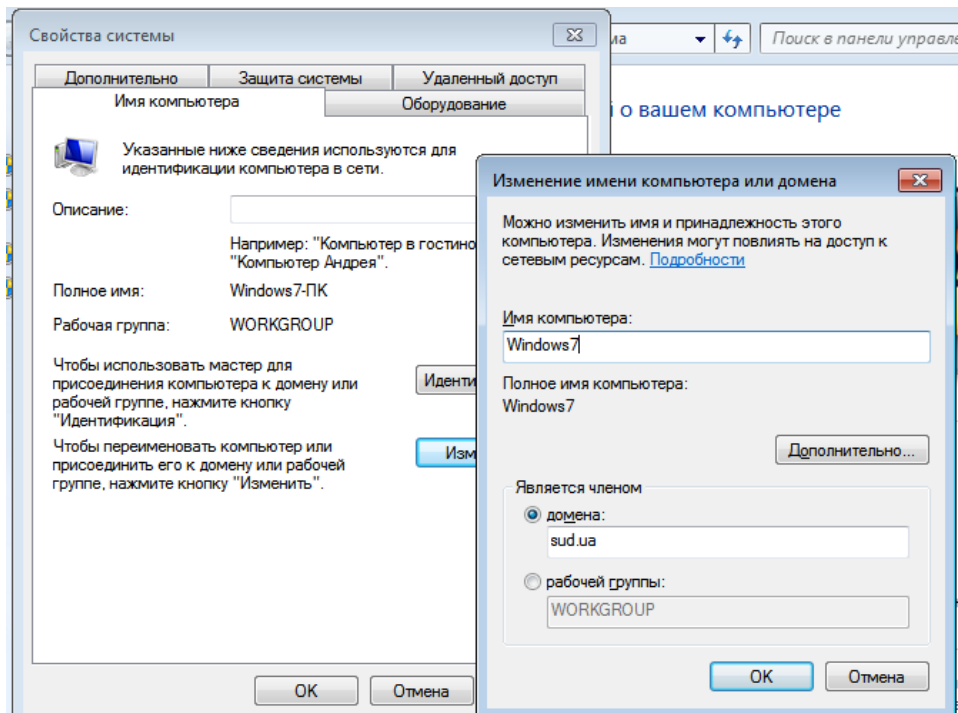


Рисунок 3.48 – Підключення робочої станції до домену

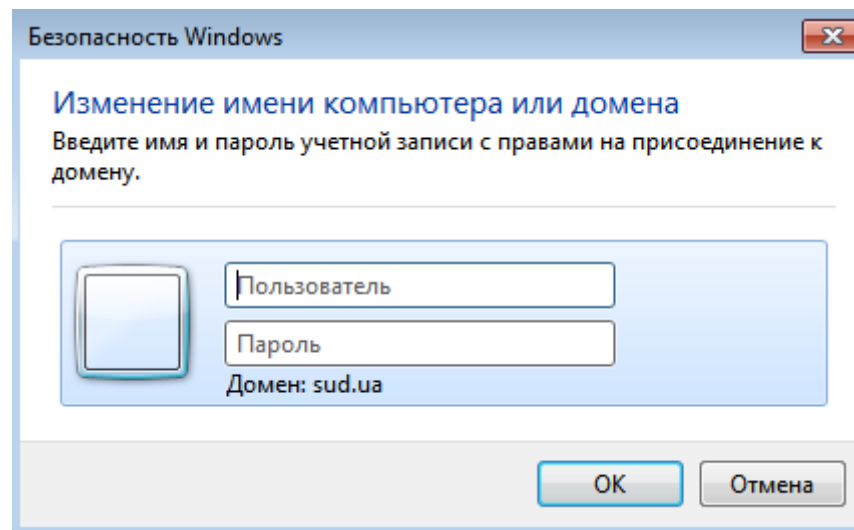


Рисунок 3.49 – Підключення робочої станції до домену

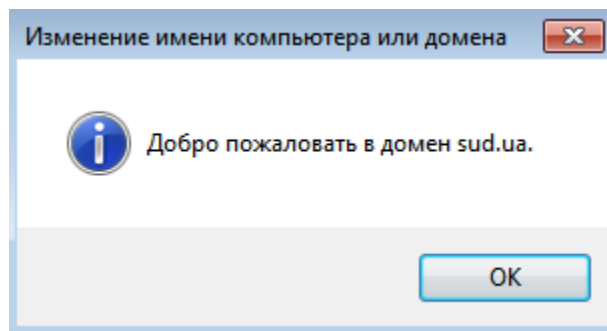


Рисунок 3.50 – Підключення робочої станції до домену

На рисунках 3.48 – 3.50 можна побачити як підключається робоча станція до домену.

Для того щоб мати змогу адмініструвати всі робочі станції мережі разом, необхідно налаштувати групову політику

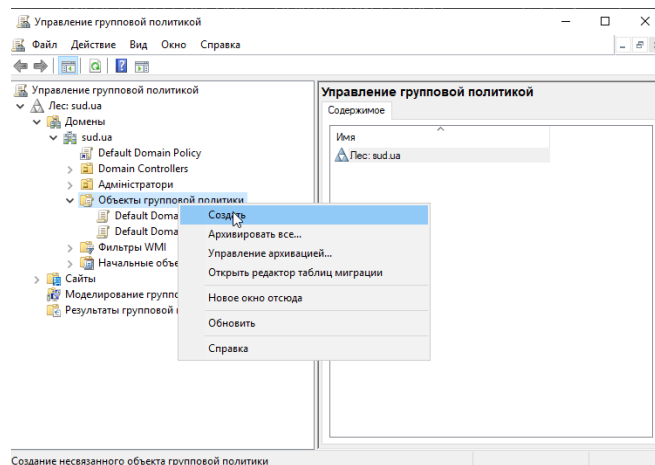


Рисунок3.51 – Налаштування групової політики для домену

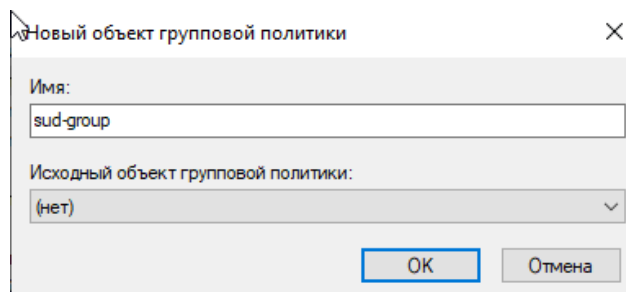


Рисунок3.52 – Налаштування групової політики для домену

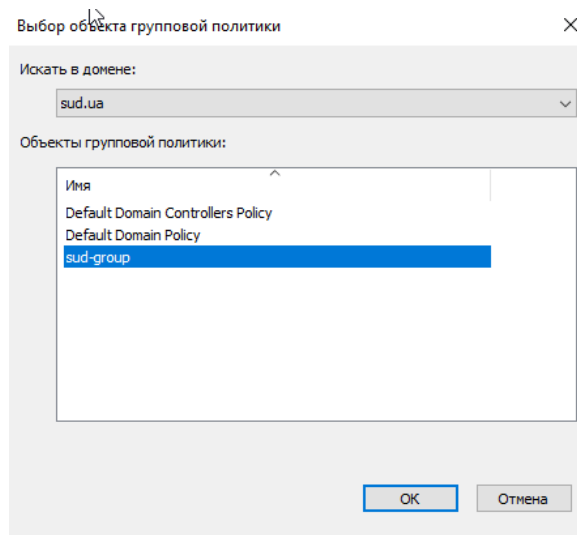


Рисунок3.53 – Налаштування групової політики для домену

Потрібно також налаштувати файловий сервер, для того щоб користувачі зберігали там всю інформацію. Це також дозволити надавати доступ до даних деяким користувачам або закривати доступ до них. (Рисунок3.54-3.58)

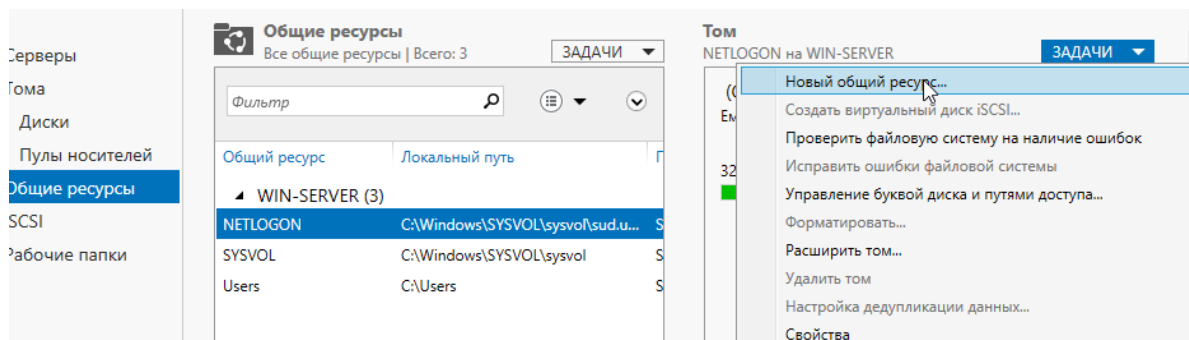


Рисунок 3.54 – Створення файлового серверу

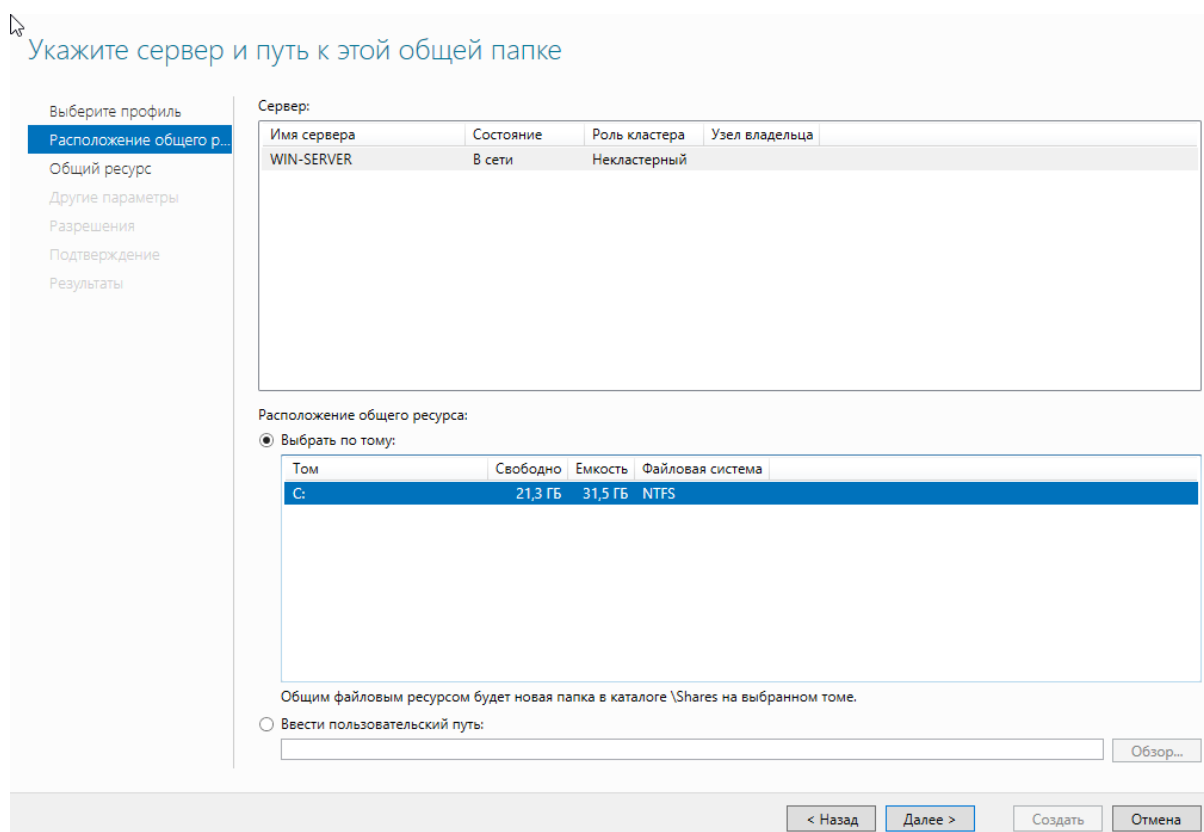


Рисунок 3.55 – Створення файлового серверу

3.3 Налаштування додаткового захисту та перевірка роботи мережі

Для будь-якої мережі необхідно налаштувати захист, щоб порушникам було тяжче або взагалі не малу змогу якось нашкодити мережі. Налаштування захисту проти DHCP starvation(Рисунок3.59)

```
SW_SERVER(config)#int range e0/1-3,e1/1
SW_SERVER(config-if-range)#switchport port-security maximum 10
SW_SERVER(config-if-range)#ip dhcp snooping limit rate 50
SW_SERVER(config-if-range)#exit
SW_SERVER(config)#
```

Рисунок 3.59 – Налаштування захисту

Так як адміністратор мережі повинен знати кількість комп'ютерів підключених до комутатора, то він може зазначити максимальну кількість MAC-адрес на порту а саме 10. Тепер комутатор буде видавати IP-адресу для кожного MAC-адреса який записаний. Також максимальна кількість DHCP-пакетів не перевищує 50.

```
SW_SERVER(config)#ip dhcp snooping vlan 1
SW_SERVER(config)#ip dhcp snooping dat
SW_SERVER(config)#ip dhcp snooping database disk0
SW_SERVER(config)#
*Dec 25 21:35:28.918: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping
database Write succeeded.
SW_SERVER(config)#ip dhcp snooping
SW_SERVER(config)#int range e0/1-3,e1/1
SW_SERVER(config-if-range)#ip dhcp snooping trust
SW_SERVER(config-if-range)#exit
SW_SERVER(config)#
```

Рисунок3.60 – Налаштування захисту

На рисунку 3.60 було налаштовано захист проти DHCP snooping. Дані команди дозволять захистити користувачів мережі від отримання адрес від неавторизованих DHCP серверів.

Перевіримо налаштування NTP. (Рисунок3.61)

Правила для входящих подключений				
Имя	Группа	Профиль	Включено	Действие
NTP		Все	Да	Разрешено

Рисунок 3.61 – Перевірка налаштувань NTP

Тобто тепер при підключення робочої станції до серверу, синхронізація часу буде відбуватися між ними. Що в подальшому дасть змогу виконувати будь-які задачі які прив'язані по часу.

Перевіримо налаштування віддаленого робочого стола.(Рисунок3.62)

						4

Рисунок 3.62 – Перевірка налаштувань RDP

Як можна побачити, протокол RDP працює. Далі спробуємо підключитися віддалено з робочої станції яка підключена до мережі.

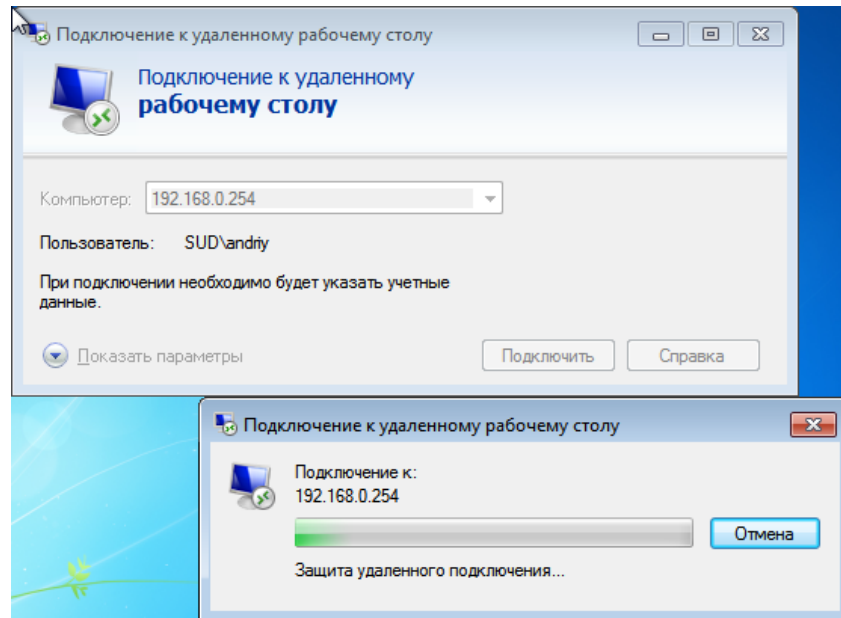


Рисунок 3.63 – Перевірка налаштувань RDP

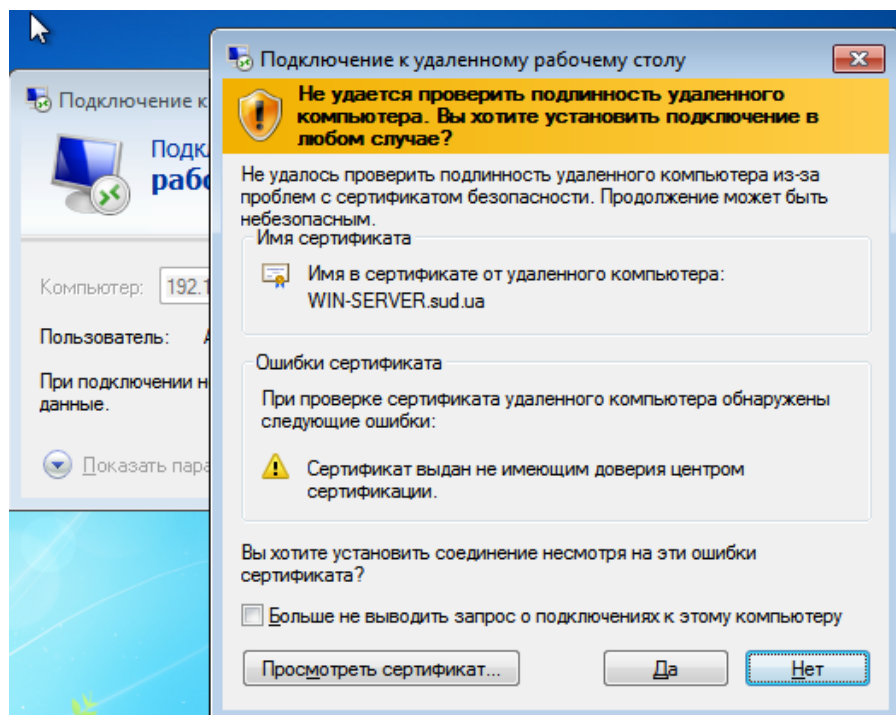


Рисунок 3.63 – Перевірка налаштувань RDP

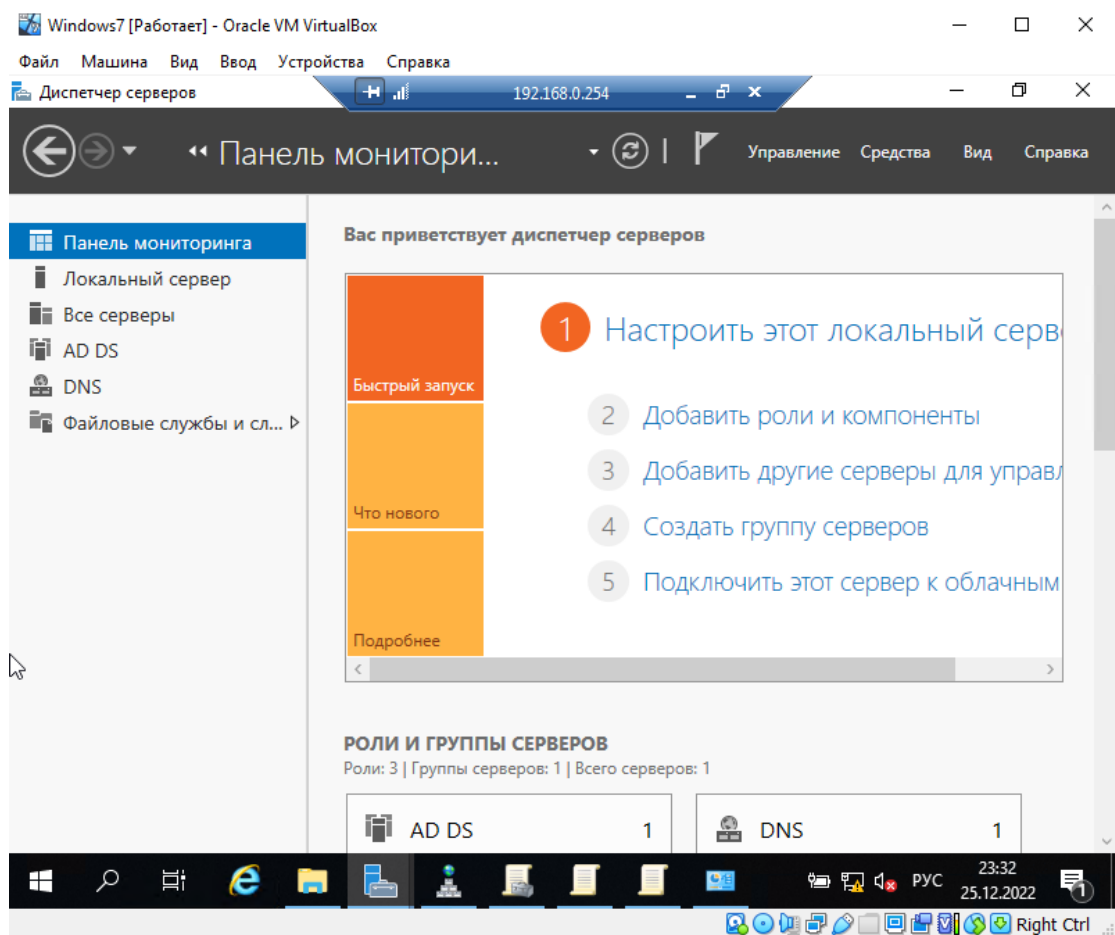


Рисунок 3.63 – Перевірка налаштувань RDP

Як можна побачити, все працює. Ця функція дозволить займатися адмініструванням серверу віддалено. Тобто дозволить в подальшому економити час та ресурси.

Перевіримо підключення робочих станцій до серверу.

Имя компьютера, имя домена и параметры рабочей группы —

Компьютер:	Windows7
Полное имя:	Windows7.sud.ua
Описание:	
Домен:	sud.ua

Активация Windows —

Рисунок 3.64 – Перевірка підключення робочої станції

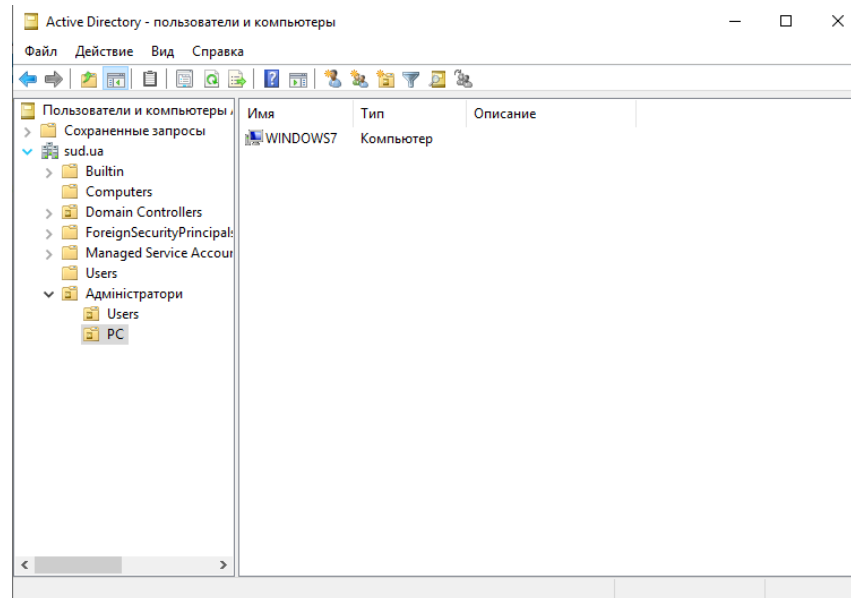


Рисунок 3.65 – Перевірка підключення робочої станції

На рисунках 3.64 – 3.65 можна побачити підключену робочу станцію до серверу. Що в подальшому дасть змогу створювати групу користувачів, слідкувати за нами та робити налаштування як для групи так і для окремого.

Також перевіримо налаштування групової політики. Наприклад виключим диспетчер завдань на робочих станціях. (Рисунок 3.66)

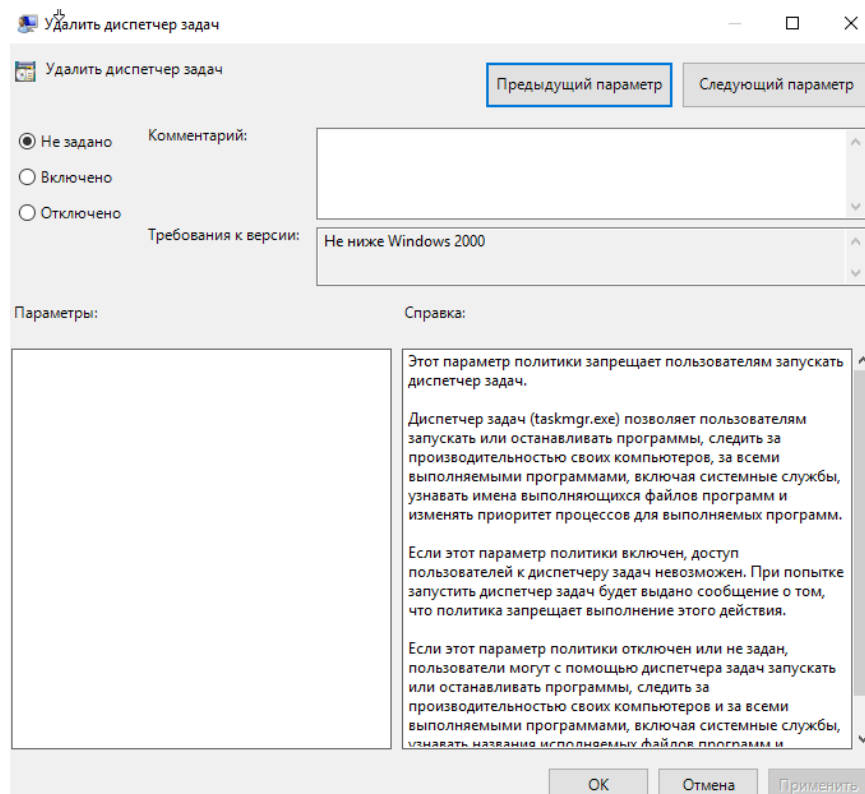


Рисунок 3.66 – Виконання групових політик.

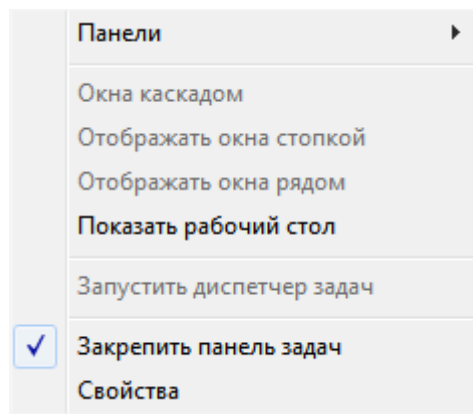


Рисунок 3.67 – Виконання групових політик

Як можна побачити на рисунку 3.67 на робочій станції яка підключена до мережі був вимкнений диспетчер завдань. Це був приклад того що можна виконувати в групових політиках. В подальшому ця функція спростить адміністрування мережі адже дозволить виконувати різноманітні завдання.

3.4 Аналіз результатів тестування

Роблячи висновок з виконаної роботи, всі завдання були виконанні. В подальшому можна розширювати мережу. Для зручності було налаштовано DHCP-сервер, що дозволить додавати нові робочі станції при цьому не налаштовуючи адресацію так як вона отримає IP-адресу автоматично. В рівні ядра та розподільчому рівні, були використанні продукти піл компанії Cisco, що ідеально підходять для побудови таких мереж.

В мережі було налаштовано Windows Server що відповідає за роботу мережі. Саме в ньому було налаштовано протокол NTP. Що дасть змогу синхронізувати час всіх робочих станцій які підключені до мережі. Це в свою чергу дозволить адміністратору виконувати завдання які пов'язані з часом, таких як оновлення програмного забезпечення, оновлення програм на робочих станціях мережі. Також було протокол RDP що дасть змогу адміністраторам мережі які мають доступ до серверу, віддалено в мережі з ним працювати, що в подальшому дозволить зекономити час і швидко вирішувати будь-які проблеми на сервері. Було налаштовано Active Directory та DNS-сервер, що дозволить підключати робочі станції до домену серверу а це в свою чергу дасть змогу керувати робочими станціями, встановлення

програмного забезпечення яке потрібно тому чи іншому підприємству. Було також розглянуте керування груповими політиками і створення користувачів в домені мережі.

Щодо недоліків даної мережі, то можна виділити те що якщо з ладу виходить комутатор чи сервер, то мережа вже не зможе повноцінно функціонувати. Тобто в подальшому мережу можна покращити використовуючи декілька комутаторів та маршрутизаторів які будуть мати зв'язок між собою і випадку коли один прилад виходить з ладу то інший буде його замінити.

Висновок до розділу 3

В даному розділі було розроблено локальну мережу, проведені базові налаштування мережі. Був налаштований DHCP-сервер, який спрощує роботу і подальшому допомагає в розширенні мережі.

Було додано Windows Server, який виступає як сервер мережі. За допомогою його інструментів було налаштовано ряд таких технологій як, NTP протокол за допомогою якого можна синхронізувати час між всіма робочими станціями, RDP – протокол за допомогою якого можна віддалено підключатися до серверу в локальній мережі, були налаштовані Active Directory та DNS-сервер, який допоможе користувачів додавати до домену і керувати ними об'єднано. Також був файловий сервер, за допомогою якого можна зберігати дані на сервері та надавати доступ певній групі користувачів.

Додатково було налаштовано захист від DHCP starvation та rogue DHCP Server, що дасть змогу мати захист від таких атак.

						4

ВИСНОВКИ

Метою магістерської наукової дипломної роботи була розробка проекту підсистеми захисту мережної інфраструктури Коростенського міськрайонного суду.

Було розглянуто основні положення що до побудови локальної мережі в приміщенні. Виділено основні принципи побудови мережі та переваги впровадження мережі для будь-якого підприємства. Розглянуто основні типи топології мережі, дослідження всіх переваг та недоліків кожної топології та обрану найкращої для побудови мережі.

Було обґрунтовано впровадження DHCP-серверу для мережі, який допоможе спростити розширення мережі в подальшому.

Було розглянуто типи атак на локальну мережу, які хакери можуть застосовувати для того щоб порушити роботу мережі, призвести до втрати даних. Також було розглянуто захист від цих типів атак для того щоб забезпечити стабільне функціонування мережі, та безпечне підключення для кожного користувача мережі.

Для побудови самої мережі, був проведений аналіз пристроїв, які краще всього застосовувати в мережі та вибрано список пристроїв які будуть застосовуватися в розробці мережі. Було розроблено таблицю з'єднань пристроїв між собою для найкращого зв'язку в мережі а також для подальшого розширення мережі в випадку коли це буде необхідно. Розроблено IP-адресацію мережі, з використанням динамічної маршрутизації.

Було вибрано оптимально програмне забезпечення мережі, яке слугує для стабільної та безперебійного працездатності мережі. Мережу було розроблено в трирівневій ієрархічній структурі, що на дасть змогу в подальшому без проблем розширювати мережу, дає змогу вже швидко виправляти якісь неполадки. Мережа складається з трьох рівнів: рівня ядра, рівня розподілу, рівень доступу. Кожен із них має важливе значення для мережі, що в цілому позначається на мережі і дає комплекс переваг при побудові такої мережі.

Мережеве обладнання для мережі було обрано від компанії Cisco, тому що саме ця компанія має комплекс незаперечних переваг над іншими компаніями, і ідеально підходить для побудови будь-якої мережі для будь-яких цілей.

						4

Було обрано віртуальне програмне забезпечення яке дозволило побудувати дану мережу віртуально, а саме GNS3. Саме ця програма надає такі можливості для побудови мережі які співпадають з реальним програмним забезпеченням яке використовується в мережі. Для додавання віртуальних машин було використано Virtual Box, що дасть змогу максимально приблизитися до реальної локальної мережі. Також було додана сервер Windows Server 2019, який відповідав за працездатність мережі.

В результаті було створено локальну мережу підприємства, яка складається з:

- комутатора Cisco Catalyst 2960
- маршрутизатора Cisco 2900
- Windows Server 2019, який відповідає за працездатність мережі
- Робочі станції Windows 7, одна з яких відповідає за адміністратора мережі.

Було проведено базові налаштування мережі, налаштування IP-адресація, налаштування DHCP-серверу. Також було налаштовано функції на Windows Server які в подальшому допомагають керувати мережею та налаштовувати її.

Було налаштовано додатковий захист для мережі.

						4

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices | Spiceworks [Електронний ресурс] - [What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices | Spiceworks](#)
2. Що ж таке мережева архітектура? (nettech.ua) [Електронний ресурс] - [Що ж таке мережева архітектура? \(nettech.ua\)](#)
3. What is a LAN? Local Area Network - Cisco [Електронний ресурс] - [What is a LAN? Local Area Network - Cisco](#)
4. Топологія мережі: 6 пояснених та порівняних мережевих топологій (instagalleryapp.com)) [Електронний ресурс] - [Топологія мережі: 6 пояснених та порівняних мережевих топологій \(instagalleryapp.com\)](#))
5. IP АДРЕСА - це що таке, поняття, значення, види, як змінити IP адресу (termin.in.ua) [Електронний ресурс] - [IP АДРЕСА - це що таке, поняття, значення, види, як змінити IP адресу \(termin.in.ua\)](#)
6. What is a DHCP Server? | Learn What They Are & How They Work | Infoblox [Електронний ресурс] - [What is a DHCP Server? | Learn What They Are & How They Work | Infoblox](#)
7. Network Address Translation (NAT) - GeeksforGeeks [Електронний ресурс] - [Network Address Translation \(NAT\) - GeeksforGeeks](#)
8. What are network attacks and how can you prevent them... | AUSY [Електронний ресурс] - [What are network attacks and how can you prevent them... | AUSY](#)
9. What Are Sniffing Attacks, and How Can You Protect Yourself? (eccouncil.org) [Електронний ресурс] - [What Are Sniffing Attacks, and How Can You Protect Yourself? \(eccouncil.org\)](#)
10. Атака канального рівня ARP-spoofing и как защитить коммутатор Cisco [Електронний ресурс] - [Атака канального рівня ARP-spoofing и как защитить коммутатор Cisco / Хабр \(habr.com\)](#)
11. What is a DHCP Starvation Attack? | CBT Nuggets [Електронний ресурс] - [What is a DHCP Starvation Attack? | CBT Nuggets](#)
12. Что такое DNS-спуфинг? | Бесплатное руководство по атакам на DNS-спуфинг

						4

(powerdmars.com) [Электронный ресурс] - [Что такое DNS-спуфинг? | Бесплатное руководство по атакам на DNS-спуфинг \(powerdmars.com\)](#)

13. Campus LAN Basics – The Hierarchical Design Model (howtonetwork.org) [Электронный ресурс] - [Campus LAN Basics – The Hierarchical Design Model \(howtonetwork.org\)](#)

14. 10 Reasons to Choose Cisco Switching [Электронный ресурс] - [Singapore AAG flyer \(cisco.com\)](#)

15. Cisco Catalyst 2960-X Comparison & Features – Router Switch Blog (router-switch.com) [Электронный ресурс] - [Cisco Catalyst 2960-X Comparison & Features – Router Switch Blog \(router-switch.com\)](#)

16. Cisco 2900 Series Integrated Services Routers Data Sheet - Cisco [Электронный ресурс] - [Cisco 2900 Series Integrated Services Routers Data Sheet - Cisco](#)

17. What Is Windows Server and How Is It Different From Windows? [Электронный ресурс] - [What Is Windows Server and How Is It Different From Windows?](#)

18. Преимущества и недостатки OS Windows Server для выделенного сервера • Дата-центр UNIT-IS [Электронный ресурс] - [Преимущества и недостатки OS Windows Server для выделенного сервера • Дата-центр UNIT-IS](#)

19. GNS3 – Графический Сетевой Симулятор [Электронный ресурс] - [GNS3 - Графический Сетевой Симулятор » CiscoLab - Лаборатория Сетей](#)

20. Oracle VM VirtualBox что это за программа и нужна ли она? [Электронный ресурс] - [Oracle VM VirtualBox что это за программа и нужна ли она? \(virtmachine.ru\)](#)

						4

ДОДАТКИ

						4

SW_SERVER#sh run

Building configuration...

Current configuration : 1979 bytes

!

! Last configuration change at 14:28:47 UTC Tue Dec 27 2022

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname SW_SERVER

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

!

						4

```

!
!
!
!
ip arp inspection vlan 1
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
ip dhcp snooping database disk0_00006_00001
ip dhcp snooping
no ip domain-lookup
ip cef
no ipv6 cef
!
!
errdisable recovery cause arp-inspection
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!

```

						4

!

!

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

!

interface Ethernet0/1

switchport port-security maximum 10

ip arp inspection trust

ip dhcp snooping limit rate 50

ip dhcp snooping trust

!

interface Ethernet0/2

switchport port-security maximum 10

ip arp inspection trust

ip dhcp snooping limit rate 50

ip dhcp snooping trust

!

interface Ethernet0/3

						4

switchport port-security maximum 10

ip arp inspection trust

ip dhcp snooping limit rate 50

ip dhcp snooping trust

!

interface Ethernet1/0

!

interface Ethernet1/1

switchport port-security maximum 10

ip arp inspection trust

ip dhcp snooping limit rate 50

ip dhcp snooping trust

!

interface Ethernet1/2

!

interface Ethernet1/3

!

interface Ethernet2/0

!

interface Ethernet2/1

!

interface Ethernet2/2

!

interface Ethernet2/3

!

interface Ethernet3/0

						4

```

!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
  no ip address
  shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0

```

						4

```
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

SW_SERVER#

						4

[illegible]