

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 підсистеми тестування захищеності доменної
інфраструктури Windows-мережі на базі рішення PingCastle»

Виконав студент 4-го курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»

 Віталій Гусєв

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

 Юрій Россінський

Доцент кафедри КІ та КБ, к.пед.н.

 Олена Головня

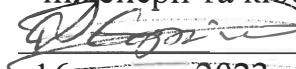
Житомир – 2023

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
16 травня 2023 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу бакалавра

Студент: Гусєв Віталій Сергійович

Тема роботи: «Проект підсистеми тестування захищеності доменної інфраструктури Windows-мережі на базі рішення PingCastle»

затверджена Наказом університету від 16 травня 2023 р. № 99

Термін здачі студентом закінченої роботи 30 червня 2023 р.

Вихідні дані роботи : Мережеві інфраструктури на базі ОС Windows та проблеми їх захищеності.

Обладнання та програмне забезпечення:

1. ОС Windows
2. Active Directory
3. PingCastle

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 16.05.2023	 16.05.2023
2	Єфіменко А.А.	 17.05.2023	 17.05.2023

Студент  Віталій Гусєв

Керівник  Юрій Россінський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	16.05.2023 - 20.05.2023	
2	Аналіз літературних джерел	21.05.2023 - 22.05.2023	
3	Аналіз предметної області для виконання завдань	23.05.2023 - 28.05.2023	
4	Постановка задачі дослідження	29.05.2023 - 04.06.2023	
5	Ознайомлення з принципами роботи інструментів	04.06.2023 - 11.06.2023	
6	Встановлення програмного забезпечення	12.06.2023- 21.06.2023	
7	Налаштування та обробка результатів	22.06.2023- 25.06.2023	
8	Оформлення звіту	25.06.2023- 27.06.2023	

Студент  Віталій Гусев

Керівник  Юрій Россінський

АНОТАЦІЯ

Кваліфікаційна роботи бакалавра викладена на 64 аркушах, складається із вступу, двох розділів, висновків. Містить рисунки та 1 таблицю.

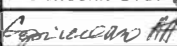
Метою кваліфікаційної роботи є закріплення знань, набутих при вивченні дисципліни «Кібербезпека», а головне, здійснення первинного аналізу джерел в рамках написання бакалаврської кваліфікаційної роботи.

В даній роботі були розглянуті проблеми мережевих інфраструктур Windows мереж, аналіз захищеності мереж інфраструктури. Інструменти такі як: «Active Directory», «PingCastle».

Були описані методи та засоби дослідження захищеності Windows мереж.

Ключові слова: WINDOWS , ACTIVE DIRECTORY, PINGCASTLE, ТЕСТУВАННЯ ЗАХИЩЕНОСТІ.

KKIK<.KP.B – 125 – 6 – ПЗ

					ККІК<.КР.Б – 125 – 6 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми тестування захищеності доменної інфраструктури Windows-мережі на базі рішення PingCastle	Літ.	Арк.	Аркушів
Розроб.		Гусев В.С.		29.06				
Керівник		Росієвський Ю.М.		29.06.23				
Реценз.		Головня О.С.		30.06.23				
Н. контр.				28.06.23				
Затверд.		Єфіменко А.А.		29.06.23				
						ФІКТ, Гр. КБ-19-2		

ANNOTATION

The bachelor's thesis is set out on 64 pages, it consists of an introduction, two chapters, and conclusions. It includes figures and 1 table.

The purpose of preparing this research is to consolidate the knowledge acquired in the course "Cybersecurity" and, most importantly, to conduct preliminary source analysis within the framework of writing a bachelor's qualification work.

This study examines the issues of Windows network domain infrastructure, analyzes the security of network infrastructure, and explores tools such as "Active Directory" and "PingCastle."

Methods and tools for investigating the security of Windows networks were described.

Keywords: WINDOWS, ACTIVE DIRECTORY, PINGCASTLE, SECURITY TESTING.

		Гусев В.С.			ККИКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ІНФОРМАЦІЙНИХ МЕРЕЖ.....	9
1.1. Базові підходи та моделі побудови windows мереж та історія	9
1.2 Проблеми захисту мережевих інфраструктур windows мереж.....	18
1.3. Методи та інструменти дослідження захищеності windows мереж...	20
1.4 Методи та засоби підвищення рівня захищеності windows мереж.....	22
Висновок до першого розділу	24
РОЗДІЛ 2. ПРОЄКТУВАННЯ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ТА АНАЛІЗ ЇЇ ЗАХИЩЕНОСТІ.....	26
2.1. Проєктування мереж інфраструктури.....	26
2.2. Аналіз захищеності мереж інфраструктури.....	29
2.3. Доменна модель	31
РОЗДІЛ 3. ПРОЄКТУВАННЯ ДОМЕННОЇ ІНФРАСТРУКТУРИ	32
3.1.Рогортання доменної структури Active Directory	32
3.2. Налаштування ДНСР	40
3.3. Перенесення облікових записів в домен	51
ВИСНОВКИ	62
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	63

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – Програмне забезпечення

ПК – Персональний комп'ютер

ОС – Операційна система

		Гусєв В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі зростають загрози кібербезпеці, особливо для бізнесів та організацій, що використовують Windows-мережі. Кіберзлочинці постійно шукають нові способи атак та вразливостей, тому необхідно систематично перевіряти захищеність мережевої інфраструктури. Доменні інфраструктури Windows-мереж часто містять важливі корпоративні дані, які потребують надійного захисту.

Метою кваліфікаційної роботи розглянути PingCastle, який є потужним інструментом для аналізу та оцінки захищеності доменних інфраструктур Windows-мереж. Використання цього рішення може допомогти виявити вразливості та недоліки у налаштуваннях, політиках безпеки та інших аспектах мережі, що дозволить підвищити рівень безпеки і запобігти можливим атакам.

Об'єктом дослідження є PingCastle є потужним інструментом для аналізу та оцінки захищеності доменних інфраструктур Windows-мереж. Використання цього рішення може допомогти виявити вразливості та недоліки у налаштуваннях, політиках безпеки та інших аспектах мережі, що дозволить підвищити рівень безпеки і запобігти можливим атакам.

Предметом дослідження Конкретні аспекти, які можуть бути включені до дослідження, включають: аналіз конфігурації та налаштувань доменної інфраструктури Windows-мережі; виявлення потенційних слабкостей та вразливостей у налаштуваннях безпеки; оцінка ефективності політик безпеки, таких як паролі, контроль доступу і шифрування даних; виявлення можливих загроз та ризиків безпеки для мережевої інфраструктури.

Дослідження спрямоване на забезпечення високого рівня безпеки доменної інфраструктури Windows-мережі за допомогою використання рішення PingCastle. Результати дослідження можуть бути використані для виявлення потенційних проблем безпеки, прийняття заходів для підвищення захищеності та забезпечення безпечної експлуатації мережі.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1. Базові підходи та моделі побудови windows мереж та історія

Побудова мереж Windows може бути здійснена за допомогою різних базових підходів та моделей. Ось декілька найпоширеніших з них:

1.1.1. Історія Active Directory та PingCastle

Active Directory є службою директорії, розробленою компанією Microsoft, яка забезпечує централізоване управління об'єктами мережевої інфраструктури. Система Active Directory була вперше представлена в операційній системі Windows 2000 і з того часу стала ключовою складовою багатьох корпоративних мереж.

Створення Active Directory відбулося в результаті необхідності розробки розширеної системи управління обліковими записами, ресурсами та політиками безпеки для комп'ютерів, користувачів та інших об'єктів у мережі. Ідея полягала в тому, щоб замінити розпорошені локальні бази даних облікових записів на централізовану директорію, яка забезпечує односторонній доступ до ресурсів та політик на різних комп'ютерах.

Active Directory стала широко використовуваною технологією в корпоративному середовищі завдяки своїм можливостям з управління доступом, аутентифікації, авторизації, аудиту та ролевого управління. Вона забезпечує досить гнучкі інструменти для створення ієрархічних структур об'єктів, таких як користувачі, групи, об'єкти політик, ресурси тощо, і дозволяє виконувати централізоване управління цими об'єктами.

PingCastle:

PingCastle є інструментом безпеки, розробленим французькою компанією PingCastle, який спеціалізується на аналізі та тестуванні захищеності доменних інфраструктур, зокрема Active Directory. Він надає засоби для виявлення

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

потенційних вразливостей, недоліків і слабких місць в налаштуванні та конфігурації Active Directory.

PingCastle дозволяє здійснювати оцінку безпеки та аналіз стану доменної інфраструктури, виявляти ризики та рекомендувати відповідні заходи щодо підвищення рівня захисту. Інструмент надає різноманітні звіти та метрики, що сприяють кращому розумінню стану безпеки домену.

Історія розробки PingCastle не є докладно документованою, але він став популярним інструментом у співтоваристві кібербезпеки, оскільки дозволяє фахівцям проводити оцінку стану безпеки доменних інфраструктур та вживати необхідні заходи для підвищення рівня захисту.

1.1.2. Робоча група (Workgroup).

Робоча група (Workgroup) є однією з моделей організації комп'ютерних мереж. Історія робочої групи починається з появи перших комп'ютерних мереж на початку розвитку комп'ютерної технології. Основна ідея робочої групи полягає в тому, що комп'ютери об'єднуються в мережу без централізованого сервера управління.

У початкових етапах розвитку комп'ютерних мереж, коли мережеві операційні системи були менш розповсюдженими, комп'ютери зазвичай працювали самостійно і не були підключені до централізованого сервера. Кожен комп'ютер у мережі мав свою власну локальну базу даних облікових записів і власні ресурси, до яких можна було мати доступ. Такі мережі були відомі як "робочі групи" (Workgroups).

У робочій групі кожен комп'ютер має свої власні облікові записи користувачів і відповідає за керування доступом до своїх ресурсів. Користувачі повинні бути реєстровані окремо на кожному комп'ютері, і доступ до ресурсів залежить від налаштувань на самому комп'ютері.

Протягом часу робочі групи стали основним способом організації малих мереж, особливо в домашніх та невеликих офісних середовищах. Вони прості у

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштуванні і не вимагають наявності додаткового сервера. Кожен комп'ютер може виконувати роль як клієнта, так і сервера, і керувати своїми власними ресурсами.

Однак, з поширенням більших мереж і зростанням компаній, робочі групи виявилися обмеженими в плані масштабованості та управління. Вони не забезпечують централізованого керування користувачами, політиками безпеки та ресурсами. Тому було розроблено більш потужні моделі, такі як доменні мережі на базі Active Directory, які надають централізоване управління та забезпечують більшу безпеку й ефективність для організацій з великою кількістю комп'ютерів та користувачів.

Незважаючи на те, що робочі групи втратили свою популярність у більших мережах, вони все ще залишаються використовуваними в деяких сценаріях, де не потрібне централізоване управління або коли мережа складається з невеликої кількості комп'ютерів, які працюють незалежно один від одного.

Цей підхід передбачає створення робочої групи, в якій кілька комп'ютерів об'єднуються для спільного використання ресурсів і файлів. У робочій групі немає центрального сервера або домена, кожен комп'ютер виступає незалежним членом мережі. Робочі групи зазвичай використовуються в невеликих мережах з невеликою кількістю комп'ютерів.

1.1.3. Доменна мережа (Domain Network)

Доменна мережа (Domain Network) є однією з моделей організації комп'ютерних мереж, яка забезпечує централізоване управління користувачами, ресурсами та політиками безпеки. Історія доменних мереж починається з розробки і впровадження технології Active Directory компанією Microsoft.

В кінці 1990-х років Microsoft представила поняття Active Directory (AD) як новий спосіб керування об'єктами мережі, такими як користувачі, комп'ютери, групи і ресурси. Active Directory створювався з метою поліпшення

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

управління великими мережами, де робочі групи були недостатніми. Ця нова технологія забезпечувала централізовану базу даних, де зберігалися облікові записи користувачів та інша інформація про мережу.

Запровадження Active Directory дало змогу створювати доменні мережі, де комп'ютери та користувачі об'єднувалися в єдину структуру. В доменній мережі був наявний централізований сервер, відомий як контролер домена (Domain Controller), який зберігав базу даних Active Directory і керував усією інформацією про домен, включаючи аутентифікацію, авторизацію та доступ до ресурсів.

Переваги доменних мереж були великими. Вони дозволяли централізовано керувати користувачами та ресурсами, встановлювати політики безпеки, групи користувачів і права доступу до ресурсів. Крім того, доменні мережі забезпечували одночасний доступ до ресурсів з будь-якого комп'ютера в мережі без необхідності створення окремих облікових записів на кожному комп'ютері. Зараз доменні мережі на базі Active Directory є широко використову

У доменній моделі мережі комп'ютери об'єднуються в домен, керований Windows Server. Домен може бути настроєний для забезпечення централізованого керування користувачами, групами безпеки, політиками безпеки та спільними ресурсами. Цей підхід зазвичай використовується в організаціях з багатьма комп'ютерами, де потрібно централізоване керування та забезпечення безпеки.

1.1.4. Змішана модель (Mixed Mode)

Змішана модель (Mixed Mode) є підходом до управління доменною мережею, який був введений компанією Microsoft в контексті системи Active Directory (AD). Історія змішаної моделі пов'язана з етапами розвитку та розгортання Active Directory.

Після впровадження Active Directory у 2000 році, вона забезпечувала можливість створення та управління доменними мережами. Початково,

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

впровадження Active Directory відбувалося у режимі "чистого режиму" (Native Mode), де було підтримувано тільки нові версії операційних систем Windows, такі як Windows 2000 та пізніше.

Однак, багато організацій на той час вже мали існуючі доменні мережі на основі попередніх версій Windows, таких як Windows NT 4.0. Щоб забезпечити сумісність та можливість поступового оновлення, була введена змішана модель (Mixed Mode).

Змішана модель дозволяла співіснувати доменним контролерам, що працюють на попередніх версіях Windows, і новим доменним контролерам, що працюють на підтримуваних версіях Windows 2000 і вище. Це дало можливість організаціям поступово оновлювати свою існуючу інфраструктуру без необхідності переривати роботу або повністю замінити старі сервери.

Змішана модель забезпечувала зворотню сумісність з попередніми версіями Windows та дозволяла поступово переходити до нової версії Active Directory, зберігаючи наявну функціональність та інтеграцію з існуючими системами.

Проте, згодом змішана модель стала менш поширеною, оскільки більшість організацій оновили свої мережі до підтримуваних версій Windows, а старі системи вийшли з експлуатації. Зараз Active Directory функціонує в режимі "чистого режиму" (Native Mode) за замовчуванням, де забезпечується повна функціональність та безпека для сучасних версій Windows Server.

Цей підхід поєднує елементи робочої групи та доменної мережі. У такій моделі можуть існувати окремі робочі групи, але деякі комп'ютери можуть бути також приєднані до домену. Це дає більшу гнучкість, оскільки різні комп'ютери можуть мати різні рівні доступу і керування.

1.1.5. Клієнт-серверна модель (Client-Server)

Клієнт-серверна модель (Client-Server) є однією з основних архітектурних моделей у сфері комп'ютерних мереж та програмного забезпечення. Її історія

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

пов'язана з розвитком комп'ютерних технологій та появою потреби у взаємодії між комп'ютерами.

Поняття клієнт-серверної моделі з'явилося в 1960-х роках. У той час було встановлено, що одним комп'ютером може керувати кілька інших комп'ютерів, використовуючи мережеві з'єднання. В такій моделі "клієнт" є пристроєм або програмою, що використовує ресурси або послуги "сервера", який забезпечує ці ресурси або послуги. Клієнт і сервер взаємодіють за допомогою мережевого протоколу, такого як TCP/IP.

У 1970-х роках з появою мереж комп'ютерів з'явилися більш розширені та складні додатки, що вимагали централізованого управління та обробки даних. Це призвело до подальшого розвитку клієнт-серверної моделі, де сервери надавали потужні ресурси обробки даних, а клієнти взаємодіяли з ними для отримання необхідних послуг або обробки інформації.

З появою Інтернету та розширення мережевих технологій в 1990-х роках клієнт-серверна модель отримала ще більший розповсюдження. Веб-додатки та послуги стали основою багатьох комп'ютерних систем, де веб-браузери діяли як клієнти, що отримували інформацію з веб-серверів. Клієнт-серверні мережі стали невід'ємною частиною багатьох бізнес-та побутових сфер.

Сучасна клієнт-серверна модель продовжує розвиватися і використовується в різних галузях, включаючи хмарні обчислення, мобільні додатки, бази даних, веб-сервіси та інші сфери комп'ютерних технологій. Вона надає ефективну та гнучку архітектуру для розподіленої обробки даних та взаємодії між різними пристроями та програмами.

Ця модель передбачає наявність центрального сервера, який надає ресурси та послуги для клієнтських комп'ютерів. Клієнти звертаються до сервера для отримання доступу до файлів, друку, баз даних та інших ресурсів. Цей підхід використовується в більших мережах, де потрібна централізована обробка та керування ресурсами.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Ці підходи та моделі можуть варіюватися залежно від розміру мережі, потреб безпеки та вимог до централізованого керування. Вибір підходу залежить від конкретних вимог та умов використання мережі Windows.

Залежно від обраного підходу до побудови мережі Windows, ви можете використовувати різні моделі та компоненти. Ось деякі з них:

1.1.5.1.Windows Server

Windows Server є операційною системою, спеціально розробленою для використання на серверах і в мережевих середовищах. Історія Windows Server пов'язана з розвитком операційних систем Windows та зростанням потреб у розширених функціях, надійності та управлінні для серверних застосунків.

Ось деякі важливі етапи у розвитку Windows Server:

Windows NT Server: У 1993 році Microsoft представила Windows NT Server, яка була основана на архітектурі Windows NT. Це була перша версія операційної системи Windows, спеціально призначена для серверних задач.

Windows Server 2000: У 2000 році була випущена Windows 2000 Server. Ця версія включала покращені можливості доменних контролерів, активного каталогу, підтримку IPv6 та інші функції для підвищення ефективності та надійності серверних середовищ.

Windows Server 2003: У 2003 році вийшла Windows Server 2003. Ця версія принесла значні покращення у продуктивності, безпеці та управлінні серверами. Вона також включала підтримку нових технологій, таких як ASP.NET та Internet Information Services (IIS) 6.0.

Windows Server 2008: У 2008 році була випущена Windows Server 2008. Ця версія включала значні покращення в галузі віртуалізації, безпеки, управління та продуктивності. Вона також представила новий інтерфейс управління під назвою Server Manager.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Windows Server 2012: У 2012 році була випущена Windows Server 2012. Ця версія включала нові функції, спрямовані на підтримку хмарних обчислень, віртуалізації та масштабованості. Вона також впроваджувала інтерфейс командного рядка PowerShell для управління серверами.

Windows Server 2016 і 2019: У 2016 році була випущена Windows Server 2016, а в 2019 році - Windows Server 2019. Ці версії принесли подальші покращення в галузі хмарних обчислень, безпеки, контейнерів та інших технологій.

Крім основних версій Windows Server, Microsoft також пропонує різні редакції, такі як Standard, Datacenter, Essentials та інші, які відрізняються функціональністю та ліцензуванням.

Розвиток Windows Server продовжується, і Microsoft регулярно випускає оновлення та нові версії, щоб задовольнити зростаючі потреби серверних середовищ і забезпечити продуктивну та безпечну роботу в мережесхематичних інфраструктурах.

Windows Server є операційною системою, спеціально розробленою для роботи в мережесхематичних середовищах. Вона надає широкий спектр функцій і можливостей для керування доменами, політиками безпеки, файловими та друкованими ресурсами, базами даних та іншими сервісами. Windows Server може використовуватись як центральний сервер у доменній моделі або в клієнт-серверній архітектурі.

1.1.5.2. Active Directory

Active Directory (AD) є службою каталогу та керування ідентифікацією в середовищі Windows. Він використовується в доменних мережах для керування користувачами, групами, політиками безпеки та доступу до ресурсів. Active Directory дозволяє централізовано керувати користувачами та ресурсами і забезпечує зручний доступ до них.

1.1.5.3. Group Policy

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Group Policy (Групові політики) є функціональністю в операційних системах Windows, яка дозволяє централізовано управляти параметрами та поведінкою комп'ютерів і користувачів в мережевому середовищі. Історія Group Policy пов'язана з розвитком операційних систем Windows та з необхідністю забезпечити ефективне управління інфраструктурою комп'ютерів у корпоративних мережах.

Ось деякі ключові етапи у розвитку Group Policy:

Windows NT 4.0: У 1996 році була випущена Windows NT 4.0, перша версія операційної системи Windows, яка включала можливості Group Policy. У цій версії було представлено поняття групових політик, які дозволяли адміністраторам налаштовувати параметри комп'ютерів і користувачів у доменній мережі.

Windows 2000: З випуском Windows 2000 у 2000 році функціонал Group Policy був значно покращений. Було впроваджено поняття Group Policy Objects (GPO) та Active Directory, що дозволило адміністраторам створювати більш складні та гнучкі політики для управління користувачами та комп'ютерами у доменній мережі.

Windows XP та Windows Server 2003: З випуском Windows XP та Windows Server 2003 в 2001 та 2003 роках відбувся подальший розвиток Group Policy. Були додані нові можливості, такі як програмне встановлення, налаштування безпеки, обмеження доступу до ресурсів та інші. Це робило Group Policy ще потужнішим і ефективнішим інструментом управління мережевою інфраструктурою.

Подальший розвиток: Згодом Group Policy продовжила розвиватися відповідно до нових версій операційних систем Windows, таких як Windows Vista, Windows 7, Windows 8, Windows 10 та відповідні серверні версії. Кожна нова версія вносила покращення в області управління політиками, забезпечуючи більшу гнучкість, безпеку та функціональність.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Сьогодні Group Policy залишається ключовим інструментом управління корпоративними мережами на основі Windows. Вона надає можливості централізованого керування параметрами, безпекою, програмами та іншими аспектами комп'ютерів та користувачів в мережесередовищах.

Group Policy (групова політика) дозволяє вам визначати і накладати політики безпеки та конфігурації на комп'ютери та користувачів в мережі Windows. Ви можете використовувати Group Policy для управління різними параметрами, такими як права доступу, настройки робочого столу, обмеження програм та багато іншого. Це дозволяє вам забезпечити єдність у конфігурації та безпеці в мережі.

1.1.5.4. File Sharing

В Windows ви можете встановлювати спільний доступ до файлів та папок між комп'ютерами в мережі. Це дозволяє користувачам обмінюватись файлами і спільно працювати над ними. Ви можете настроїти рівні доступу до файлів та папок, контролювати права користувачів та забезпечувати безпеку

1.2 Проблеми захисту мережесередовищ windows мереж

Захист мережесередовищ Windows мереж важливий для забезпечення конфіденційності, цілісності та доступності даних, а також запобігання несанкціонованому доступу та інших загроз. Ось деякі проблеми, з якими можуть стикатися мережесередовища Windows:

1.2.1. Програмне забезпечення та віруси.

Шкідливе програмне забезпечення, таке як віруси, черв'яки та троянські коні, може скеровуватися на мережесередовища Windows з метою викрадення даних, розповсюдження шкідливого коду або завдання інших збитків. Важливо мати актуальні антивірусні програми та регулярно оновлювати їх бази даних, щоб виявляти та усувати такі загрози.

1.2.2. Несанкціонований доступ

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Несанкціонований доступ до мережевих ресурсів може стати наслідком слабких паролів, неякісної аутентифікації, недостатніх прав доступу або вразливостей в мережевому програмному забезпеченні. Важливо використовувати надійні паролі, встановлювати адекватні політики безпеки та застосовувати механізми контролю доступу, такі як ролі та групові політики.

1.2.3. Нестача оновлень

Недостатня установка патчів і оновлень для операційної системи Windows та інших компонентів може залишити мережеву інфраструктуру вразливою перед відомими загрозами. Важливо регулярно оновлювати операційну систему та програмне забезпечення до останніх версій і встановлювати критичні патчі якомога швидше.

1.2.4. Фішинг та соціальний інжиніринг

Атаки, що використовують фішингові листи та соціальний інжиніринг, можуть спрямовуватися на користувачів мережі з метою отримання конфіденційної інформації, такої як паролі або дані доступу. Важливо навчати користувачів розпізнавати підозрілі повідомлення та приймати обережність при роботі з електронною поштою та веб-сайтами.

1.2.5. Недостатня моніторинг та журналювання

Відсутність системи моніторингу та журналювання може ускладнити виявлення і реагування на потенційні загрози. Важливо мати в силу механізми моніторингу мережі та журналювання подій, щоб виявляти підозрілу активність, аналізувати події та вживати заходів для врегулювання інцидентів безпеки.

1.2.6. Втрати даних та резервне копіювання

Випадкове видалення даних, технічні проблеми або зловмисна діяльність можуть призвести до втрати важливої інформації. Важливо регулярно

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

резервувати дані та мати механізми відновлення, щоб уникнути серйозних наслідків в разі виникнення проблем.

Ці проблеми вимагають систематичного підходу до захисту мережевих інфраструктур Windows. Важливо постійно оновлювати свої знання про нові загрози та використовувати надійні методи та інструменти для захисту мережі.

1.3. Методи та інструменти дослідження захищеності windows мереж

Дослідження захищеності Windows мереж включає в себе використання різноманітних методів та інструментів для виявлення потенційних вразливостей та оцінки рівня безпеки системи. Ось деякі методи та інструменти, які можна використовувати для дослідження захищеності Windows мереж:

1.3.1. Вразливість сканування

Використання інструментів, таких як Nessus, OpenVAS або Qualys, PingCastle дозволяє сканувати мережеві пристрої та операційні системи на наявність вразливостей. Ці інструменти виявляють потенційні слабкі місця та рекомендують заходи для їх виправлення.

PingCastle - це інструмент для сканування та аналізу захищеності доменної інфраструктури Windows-мереж. Він призначений для виявлення потенційних уразливостей, конфігураційних проблем та ризиків безпеки, пов'язаних з розгортанням та управлінням доменами в середовищі Active Directory.

Основні функції та можливості PingCastle:

Сканування доменних контролерів: PingCastle дозволяє проводити сканування доменних контролерів для виявлення потенційних проблем безпеки. Він аналізує різні аспекти доменної інфраструктури, включаючи права доступу, налаштування групових політик, служби, безпеку паролів тощо.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Аналіз ризиків безпеки: Інструмент проводить оцінку ризиків безпеки на основі зібраних даних. Він надає детальну інформацію про виявлені проблеми та рекомендації щодо їх вирішення.

Звіти та аналітика: PingCastle генерує звіти, які містять інформацію про виявлені проблеми, їх серйозність та пропозиції щодо вдосконалення безпеки. Звіти можуть бути використані для аудиту безпеки, підготовки рекомендацій та моніторингу стану захищеності доменної інфраструктури.

Порівняння доменів: Інструмент дозволяє порівнювати рівень захищеності різних доменів в мережі. Це дозволяє ідентифікувати слабкі місця та просунуті налаштування безпеки, які можуть бути використані для усунення проблем та покращення безпеки доменних контролерів.

Планування вдосконалень: PingCastle допомагає розробити план вдосконалень для підвищення рівня безпеки доменної інфраструктури. Він надає рекомендації та пріоритети для вирішення виявлених проблем та запровадження рекомендованих заходів забезпечення безпеки.

Застосування PingCastle у дипломній роботі може включати використання інструмента для сканування та аналізу безпеки доменної інфраструктури Windows-мереж, оцінку ризиків безпеки, генерацію звітів та розробку плану вдосконалень. При цьому можна провести порівняння декількох доменів та проаналізувати їх рівень захищеності.

1.3.2. Аудит безпеки

Виконання аудиту безпеки дозволяє перевірити відповідність системи встановленим стандартам безпеки, таким як CIS Benchmarks або STIGs. Інструменти, такі як Microsoft Baseline Security Analyzer (MBSA) або Security Compliance Toolkit, надають можливість перевірити конфігурацію системи та ідентифікувати можливі проблеми безпеки.

1.3.3. Тестування проникнення

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Цей метод включає в себе спроби зламати або проникнути в мережу, щоб виявити слабкі місця та потенційні вразливості. Інструменти, такі як Metasploit Framework, Burp Suite або Kali Linux, дозволяють виконувати тестування проникнення шляхом емуляції атак та перевірки реакції системи на них.

1.3.4. Моніторинг мережі

Використання систем моніторингу мережі, таких як Wireshark, SolarWinds, PRTG Network Monitor або Nagios, дозволяє виявляти незвичайну або підозрілу активність в мережі. Це може допомогти виявити потенційні атаки або аномалії, які можуть вказувати на проблеми з безпекою.

1.3.5. Інцидентний реагування

Мати налагоджену систему інцидентного реагування дозволяє швидко виявляти, аналізувати та врегулювати безпекові інциденти. Інструменти, такі як Security Information and Event Management (SIEM) системи, допомагають збирати, аналізувати та реагувати на події безпеки в реальному часі.

Це лише кілька методів та інструментів, які можна використовувати для дослідження захищеності Windows мереж. Важливо мати на увазі, що безпека є постійним процесом, і регулярне оновлення та вдосконалення заходів безпеки є необхідними для ефективного захисту мережі.

1.4 Методи та засоби підвищення рівня захищеності windows мереж

Для підвищення рівня захищеності Windows мереж можна використовувати різноманітні методи та засоби. Ось деякі з них:

1.4.1. Оновлення систем

Регулярне оновлення операційних систем Windows і встановлення оновлень безпеки є критичним. Це дозволяє закрити відомі вразливості і виправити помилки, які можуть бути використані для атак.

1.4.2. Встановлення брандмауера

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

Брандмауер (firewall) допомагає контролювати трафік, що входить і виходить з мережі. Це дозволяє блокувати небажаний або підозрілий трафік і зменшує ризик вторгнень.

1.4.3. Використання антивірусного програмного забезпечення

Встановлення і оновлення надійного антивірусного програмного забезпечення допомагає виявляти і блокувати шкідливі програми, віруси та інші загрози безпеці.

1.4.4. Застосування політик безпеки

Встановлення і виконання строгих політик безпеки допомагає забезпечити належну конфігурацію системи, обмежити доступ користувачів і зменшити ризик витоку інформації.

1.4.5. Використання сильних паролів

Встановлення складних і унікальних паролів для облікових записів користувачів допомагає ускладнити процес несанкціонованого доступу до системи.

1.4.6. Шифрування даних

Використання шифрування файлів та дисків допомагає захистити конфіденційну інформацію в разі втрати або крадіжки пристроїв.

1.4.7. Мультифакторна аутентифікація

Використання мультифакторної аутентифікації (МФА) додає додатковий шар захисту, вимагаючи введення додаткових підтверджень, таких як одноразові паролі або відбитки пальців, для доступу до системи.

1.4.8. Моніторинг подій безпеки

Використання систем моніторингу подій дозволяє виявляти підозрілі активності, несподівані зміни в системі та інші ознаки порушення безпеки.

1.4.9. Сегментування мережі

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Розділення мережі на сегменти та використання мережевих сегментаторів допомагає обмежити розповсюдження атак і зменшити вплив інцидентів на всю мережу.

1.4.10. Навчання та свідомість користувачів

Проведення навчання з питань безпеки та підвищення свідомості серед користувачів допомагає зменшити ризик соціально інженерних атак і небезпечних дій.

Ці методи та засоби можуть використовуватися окремо або в поєднанні для підвищення рівня захищеності Windows мереж. Важливо регулярно оновлювати та адаптувати заходи безпеки відповідно до змінюються загроз та вимог безпеки.

Висновок до першого розділу

Побудова інформаційних мереж є складним процесом, який вимагає уваги до деталей і розуміння теоретичних аспектів. Основні теоретичні аспекти побудови інформаційних мереж включають такі елементи:

Топологія мережі: Вибір правильної топології мережі визначає, як вузли та пристрої підключаються і взаємодіють один з одним. Популярні типи топологій включають зірку, дерево, кільце, мешок та лінійку. Кожна топологія має свої переваги і недоліки, і вибір залежить від вимог та потреб конкретної мережі.

Протоколи мережі: Протоколи мережі визначають правила та стандарти для обміну даними між вузлами мережі. Вони включають такі аспекти, як адресація, маршрутизація, передача даних та керування помилками. При виборі протоколів важливо враховувати їх сумісність, ефективність та безпеку.

Апаратне забезпечення: Вибір правильного апаратного забезпечення, такого як маршрутизатори, комутатори, сервери та кабельна інфраструктура, є

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

важливим аспектом побудови інформаційних мереж. Вони повинні бути сумісними з обраною топологією та протоколами мережі, а також забезпечувати потрібну швидкість, пропускну здатність та надійність.

Безпека мережі: Забезпечення безпеки в інформаційних мережах має велике значення. Це включає захист від несанкціонованого доступу, вірусів, вторгнень та витоку конфіденційної інформації. Застосування шифрування, брандмауерів, систем ідентифікації та аутентифікації, а також моніторингу подій безпеки є важливими аспектами захисту мережі.

Тому побудова інформаційних мереж вимагає уважного планування, врахування теоретичних аспектів та вибір оптимальних рішень. Топологія мережі, протоколи мережі, апаратне забезпечення та безпека є основними елементами побудови мережі. Правильний вибір цих елементів допоможе забезпечити ефективну та безпечну роботу інформаційної мережі.

		Гусєв В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЄКТУВАННЯ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ТА АНАЛІЗ ЇЇ ЗАХИЩЕНОСТІ

2.1. Проєктування мереж інфраструктури

Перед розгортанням доменної структури в мережі важливо спланувати її та мати чітке уявлення про призначення окремих серверів та процесів взаємодії між ними.

Перед створенням першого контролера домену необхідно визначитися з режимом його роботи, який залежить від версії операційної системи. Розглянемо популярні режими: Windows Server 2003, 2008 і 2008 R2.

Режим Windows Server 2003 слід вибрати тільки в тому випадку, якщо в інфраструктурі вже є сервери на цій ОС і планується використовувати один або кілька таких серверів як контролери домену. У інших випадках потрібно вибрати режим Windows Server 2008 або 2008 R2 в залежності від придбаних ліцензій. Слід пам'ятати, що режим роботи домену можна завжди підвищити, але знизити вже не вдасться (крім випадку відновлення з резервної копії). Тому до цього питання потрібно підходити обережно, з урахуванням можливих розширень, ліцензій у філіях тощо.

Важливо звернути увагу, що в повноцінній структурі Active Directory має бути принаймні два контролери домену. У противному разі це призведе до непотрібного ризику, оскільки в разі відмови єдиного контролера домену структура AD буде повністю зруйнована. Найкраще мати актуальну резервну копію, з якої можна буде відновитися. В будь-якому випадку мережа буде повністю паралізована.

Тому після створення першого контролера домену необхідно негайно розгорнути другий, незалежно від розмірів мережі та бюджету. Другий контролер має бути запланований ще на етапі планування, і без нього розгортання AD не рекомендується. Також не рекомендується поєднувати роль контролера домену з будь-якими іншими серверними ролями. З метою

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечення надійності операцій з базою AD на диску відключається кешування записів, що може призвести до різкого падіння продуктивності дискової підсистеми (це пояснює довге завантаження контролерів домену).

Всі контролери домену в AD є рівнозначними та містять повну інформацію про об'єкти домену. Однак, розподіл ролей FSMO (Flexible Single Master Operations) між контролерами може впливати на функціональні можливості та надійність мережі.

FSMO відповідає за спеціалізовані операції у системі AD. Якщо сервер, що містить ролі FSMO, вийде з ладу або буде вимкнений на тривалий термін, то деякі операції, пов'язані з цими ролями, можуть бути обмеженими або недоступними. Наприклад, якщо контролер домену, який має роль господаря інфраструктури, стане недоступним, то не буде можливості вносити зміни в схему AD. Або якщо контролер, який має роль емулятора PDC (Primary Domain Controller), стане недоступним, то можуть виникнути проблеми з аутентифікацією користувачів.

Тому рекомендується мати не менше двох глобальних каталогів (DC), особливо якщо в мережі використовуються додатки, які вимагають наявності глобального каталогу. Це забезпечує надійність та доступність AD навіть при відмові одного контролера. Також розглядається можливість використання контролерів домену доступних тільки на читання (RODC) для розширення мережі та забезпечення безпеки від несанкціонованого доступу.

Адміністратор домену повинен чітко розуміти, як розподілені ролі FSMO між серверами та в разі вимкнення або відмови сервера передавати ці ролі іншим контролерам. В разі втрати сервера з ролями FSMO можна виконати процес захоплення цих ролей на іншому контролері для відновлення повноцінної роботи служби каталогів.

Однак, важливо зауважити, що сама відмова одного контролера домену не призведе до відмови всієї AD. Залишаючись принаймні з одним працюючим

		Гусєв В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

контролером, мережа зможе продовжувати працювати, і користувачі зможуть авторизуватись та отримувати доступ до ресурсів.

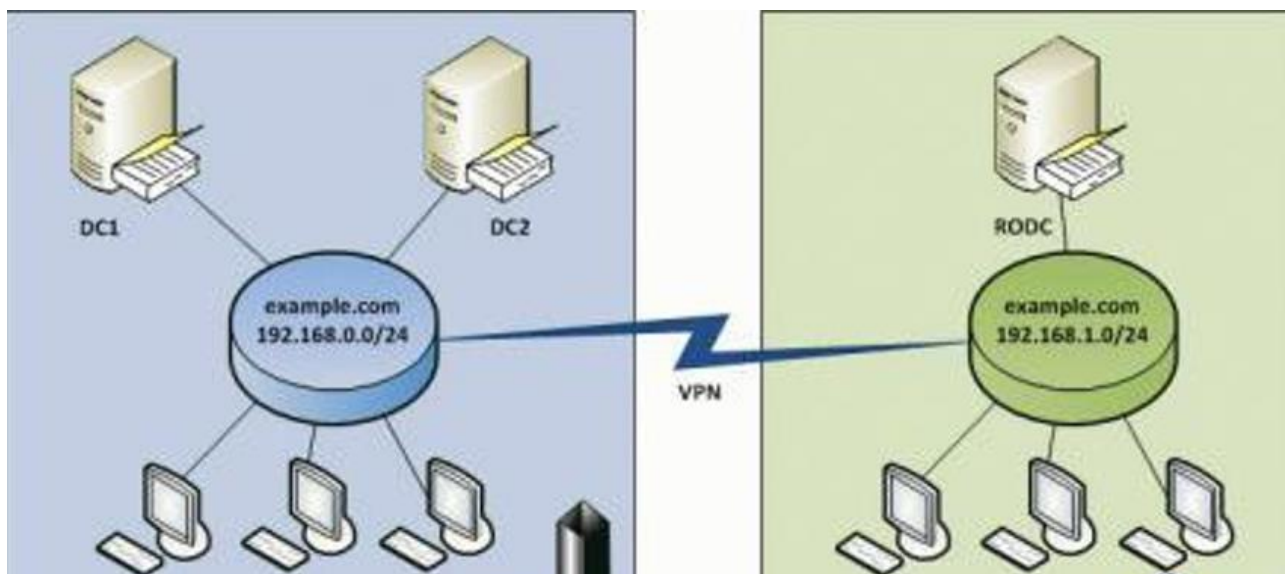


Рисунок 1 – Схема підключення філіалу організації

При налаштуванні RODC у філії можуть виникати проблеми з довгим часом входу в систему та великим обсягом інтернет-трафіку через повільний канал зв'язку. Однією з основних причин цього є процес реплікації, який автоматично поширює зміни, зроблені на одному контролері домену, на інші контролери. Цей процес реплікації працює незалежно від швидкості каналу, тому всі зміни, внесені в офісі, негайно реплікуються до філії, що може завантажувати канал зв'язку та спричиняти велику витрату трафіку.

Для вирішення цієї проблеми рекомендується налаштувати сайти Active Directory. Сайти Active Directory дозволяють фізично розділити структуру служби каталогів на області, які мають повільні та нестабільні канали зв'язку. Сайти створюються на основі підмереж, і всі клієнтські запити спочатку направляються до контролерів свого сайту. Крім того, бажано мати в кожному сайті свій глобальний каталог.

У вашій мережі рекомендується створити два сайти: "AD Site 1" для центрального офісу і "AD Site 2" для філії (або додати філію до вже існуючого сайту). Це дозволить керувати трафіком і зменшити завантаження

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

каналу зв'язку. Тепер розглянемо як відбувається реплікація в мережі з декількома сайтами на рисунку 2 .

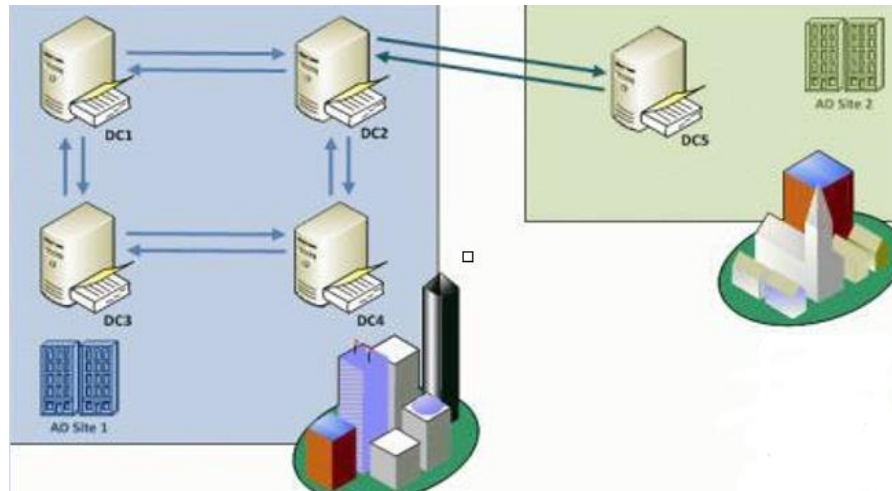


Рисунок 2 - Реплікація з налаштованими сайтами Active Directory

Організація розвилася і головний офіс містить цілих чотири контролери домену, реплікація між контролерами одного сайту називається внутрішньосайтовою і відбувається миттєво. Топологія реплікації будується за схемою кільця з умовою, щоб між будь-якими контролерами домену було не більше трьох кроків реплікації. Схема кільця зберігається до 7 контролерів включно, кожен контролер встановлює зв'язок з двома найближчими сусідами, при більшій кількості контролерів з'являються додаткові зв'язки і загальне кільце як би перетворюється в групу накладених один на одного кілець.

Міжсайтова реплікація відбувається інакше, в кожному домені автоматично вибирається один з серверів (сервер-плацдарм) який встановлює зв'язок з аналогічним сервером іншого сайту. Реплікація за замовчуванням відбувається раз в 3 години (180 хвилин), проте можна встановити будь-який розклад реплікації і для економії трафіку всі дані передаються в стислому вигляді. При наявності в сайті тільки RODC реплікація відбувається однонаправлено.

2.2. Аналіз захищеності мереж інфраструктури

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Модель "Робоча група" є простою і примітивною моделлю управління безпекою корпоративної мережі, призначеною для невеликих однорангових мереж з обмеженим числом комп'ютерів (зазвичай від 3 до 10). У цій моделі кожен комп'ютер в мережі має свою власну локальну базу даних облікових записів, яка знаходиться в реєстрі операційної системи і називається базою даних SAM (Security Account Manager).

Приклад управління доступом при використанні такої моделі наступний:

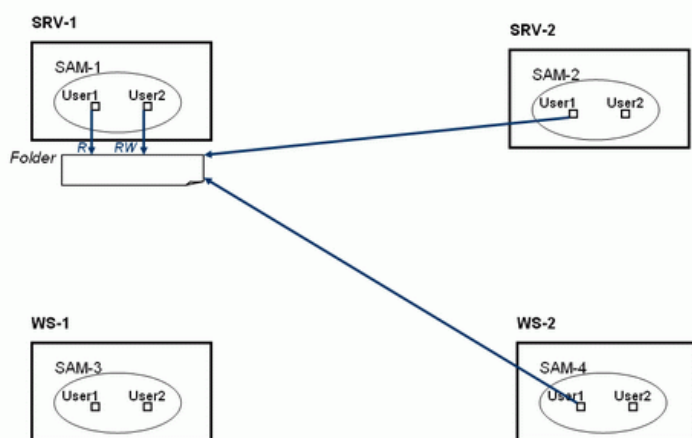


Рисунок 3 - Приклад управління доступом.

Управління доступом до ресурсів здійснюється на рівні кожного окремого комп'ютера за допомогою локальної бази даних. Це означає, що кожен комп'ютер самостійно контролює доступ користувачів до своїх ресурсів і встановлює права доступу на основі облікових записів, зареєстрованих у його локальній базі даних SAM.

Важливо зауважити, що бази даних окремих комп'ютерів у моделі "Робоча група" повністю ізольовані одна від одної і не мають взаємного зв'язку. Це означає, що кожен комп'ютер вирішує питання доступу до своїх ресурсів незалежно від інших комп'ютерів у мережі.

Управління доступом в моделі "Робоча група" здійснюється на рівні окремих комп'ютерів і може бути обмежене. Наприклад, адміністратор кожного

комп'ютера повинен вручну керувати обліковими записами та правами доступу до ресурсів на своєму комп'ютері.

Ця модель може бути використана в невеликих офісах або домашніх мережах, де немає потреби в централізованому управлінні доступом і великій кількості комп'ютерів. Однак, вона не підходить для великих корпоративних мереж, де вимагається більш централізоване управління безпекою та забезпечення єдиної бази даних облікових записів і політик доступу.

2.3. Доменна модель

У доменній моделі управління безпекою, користувачі реєструються на комп'ютері шляхом входу в систему зі своїм доменним обліковим записом. Незалежно від конкретного комп'ютера, на якому відбувається реєстрація, користувач отримує доступ до необхідних мережевих ресурсів. У цій моделі немає необхідності створювати багато локальних облікових записів на кожному комп'ютері, оскільки всі записи створюються одноразово в доменній базі даних.

Централізоване управління доступом до мережевих ресурсів здійснюється за допомогою доменної бази даних, яка доступна всім комп'ютерам у мережі. Для цього встановлюються спеціалізовані сервери, відомі як контролери домена, які зберігають цю базу даних на своїх жорстких дисках.

В доменній моделі існує єдина база даних служб каталогів, яка містить інформацію про користувачів, групи, політики безпеки та інші відомості, необхідні для управління доступом. Ця база даних забезпечує централізоване та однорідне управління безпекою в мережі незалежно від кількості комп'ютерів.

Доменна модель надає більш гнучкий та масштабований підхід до управління безпекою у великих корпоративних мережах. Вона спрощує процес створення, керування та відстеження облікових записів користувачів, а також надає можливість встановлення централізованих політик безпеки для всієї мережі.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

У підсумку, доменна модель управління безпекою дозволяє ефективно керувати доступом до ресурсів в мережі, спрощує адміністрування та забезпечує високий рівень безпеки у великих мережових інфраструктурах.

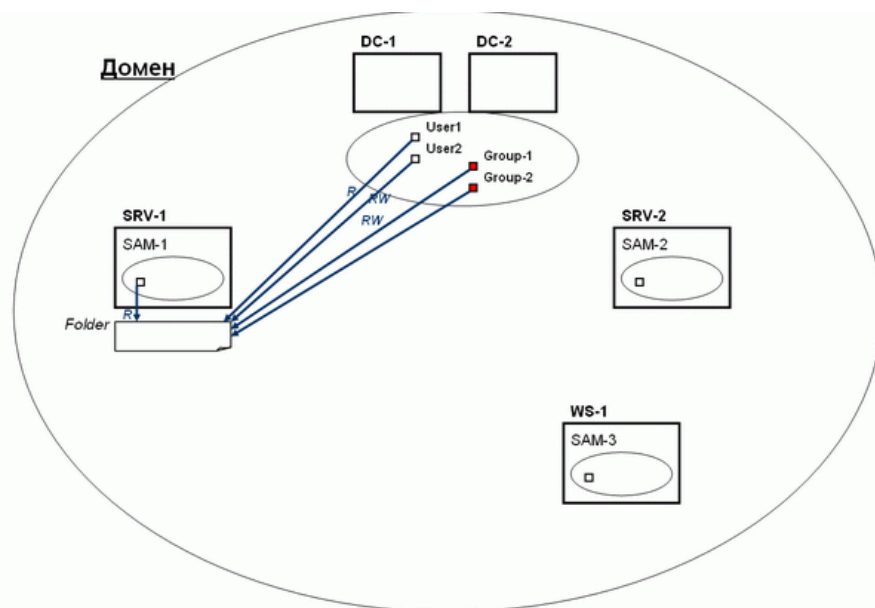


Рисунок 4- Контролери домена

Із рисунка сервери DC-1 і DC-2 — контроллери домена, вони зберігають доменну базу даних облікових записів (кожен контроллер зберігає у себе свою власну копію БД, але всі зміни, вироблювані в БД на одному з серверів, репліцируються на решту контроллерів).

РОЗДІЛ 3. ПРОЄКТУВАННЯ ДОМЕННОЇ ІНФРАСТРУКТУРИ

3.1.Розгортання доменної структури Active Directory

Перед тим як приступити до практичного втілення планів розгортання, необхідно виконати деякі кроки, а саме:

- Назначити майбутньому доменному контролеру зручне для читання ім'я.
- Встановити для мережевого адаптера статичну IP адресу.
- Перейменувати вбудований обліковий запис адміністратора, використовуючи тільки латинські букви і символи.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Після того, як всі вищевикладені рекомендації виконані, було проведено установку ролі «Доменні служби Active Directory», це було виконано через оснащення Ролі в диспетчері сервера (рисунок 5).

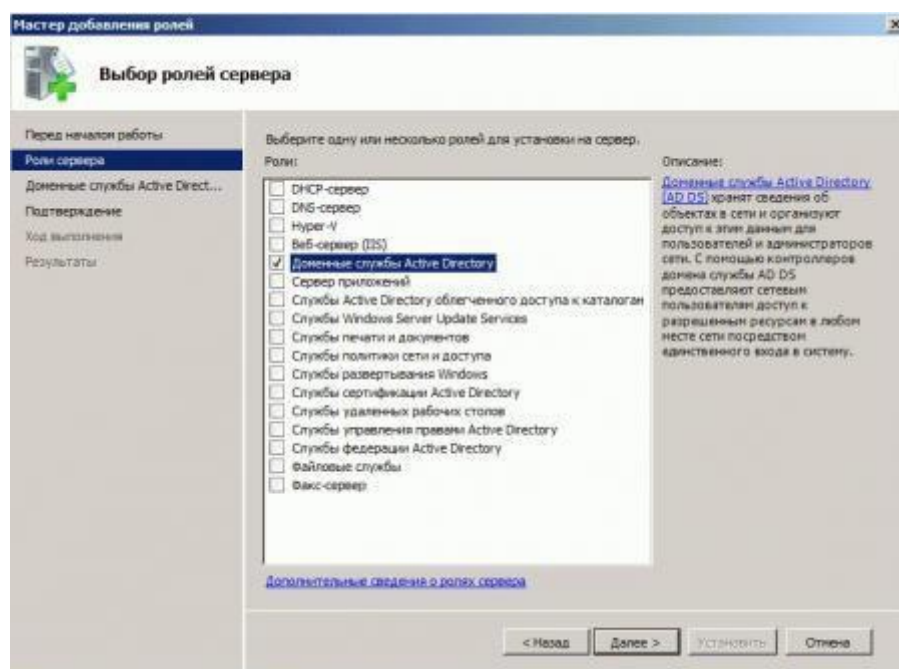


Рисунок 5 – Вибір ролі серверу

Установка даної ролі не робить даний сервер контролером домену, для цього необхідно запустити «Мастер установки доменных служб», що і було запропоновано зробити після закінчення установки (рисунок 6).

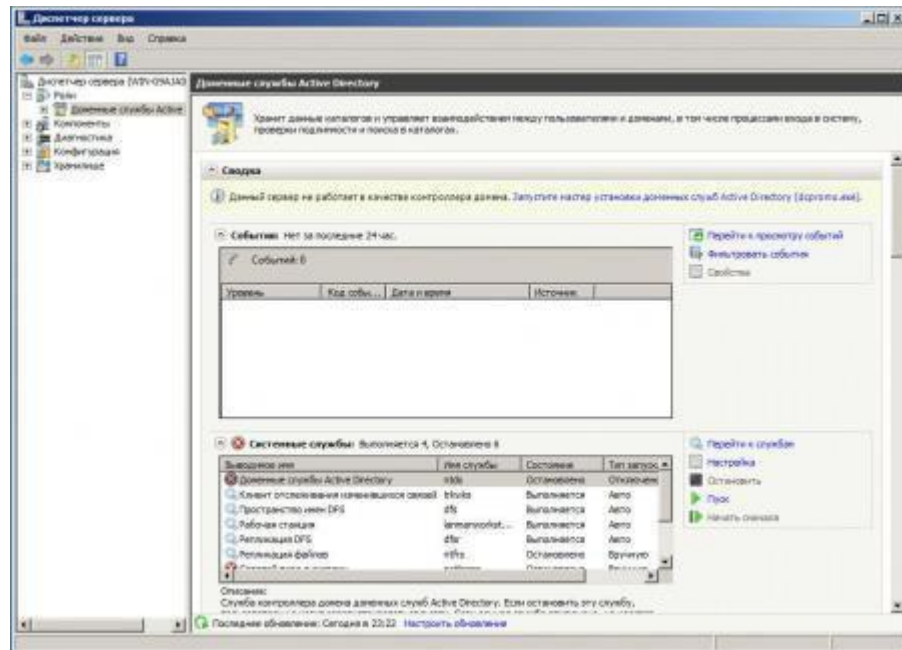


Рисунок 6 – Майстер завантаження доменних служб

Так як це наш перший контролер домену, то вибираємо Створити новий домен в новому лісі (рисунок 7).

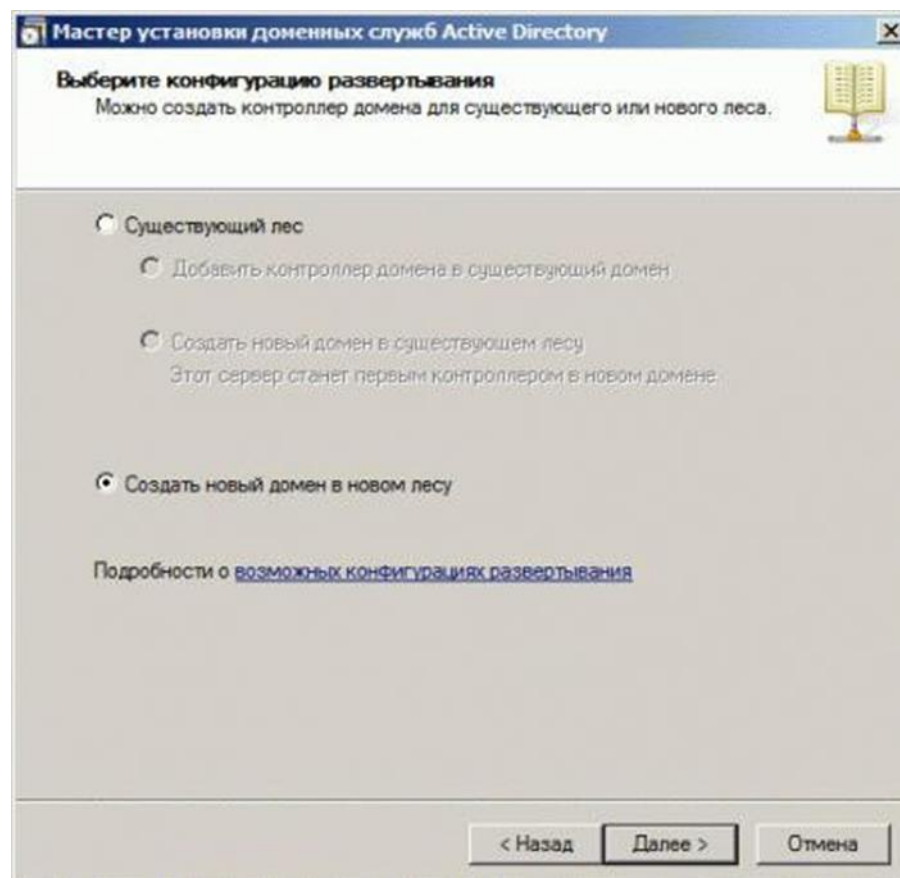


Рисунок 7 – Створення нового домену в новому лісі Наступним кроком вказано ім'я домену.

Не рекомендується давати домену інтернет ім'я зовнішнього домену, також не рекомендується давати ім'я в неіснуючих зонах першого рівня, типу .local або .test і т.д. Оптимальним варіантом для домену AD буде піддомен в просторі імен зовнішнього інтернет домену, наприклад corp.example.com. Якзначається ім'я показано на рисунок 8.

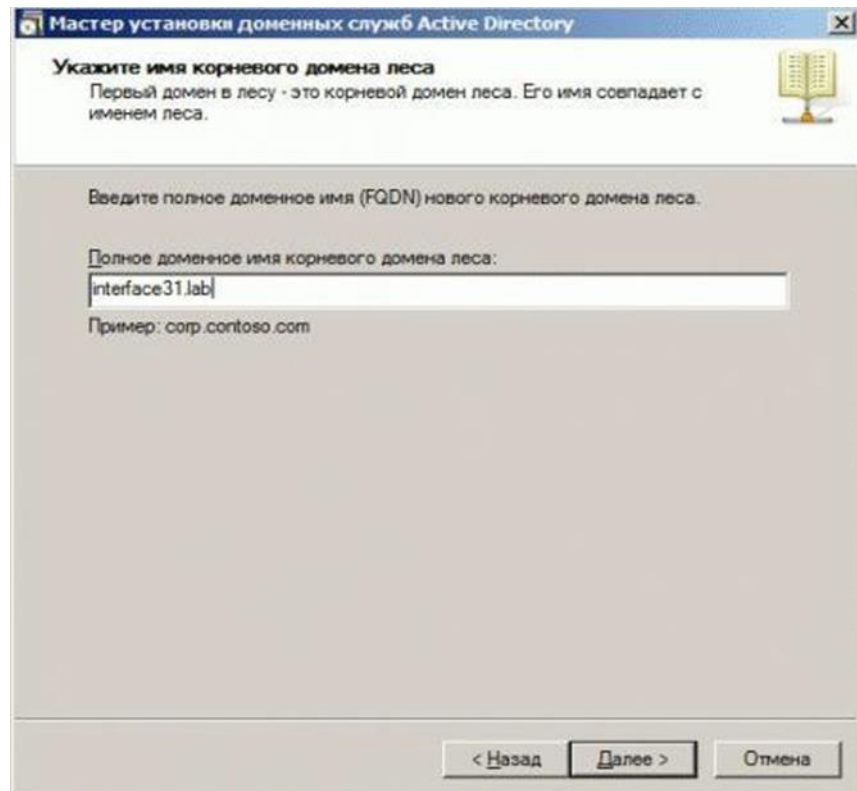


Рисунок 8 – Призначення імені кореневого домену ліса

Необхідно обрати режим роботи лісу (рисунок 9).

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М				35
Змн.	Арк.	№ докум.	Підпис	Дата		

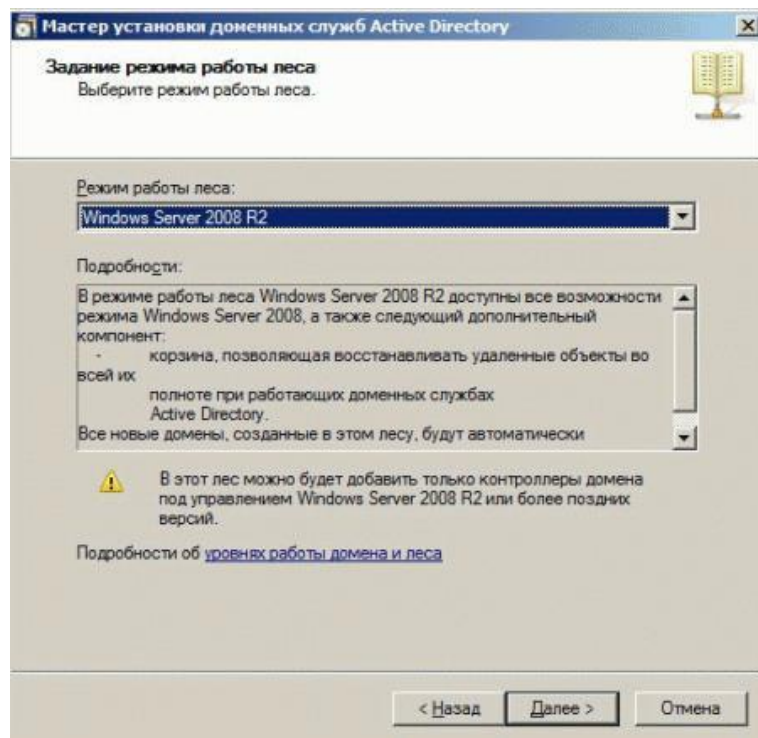
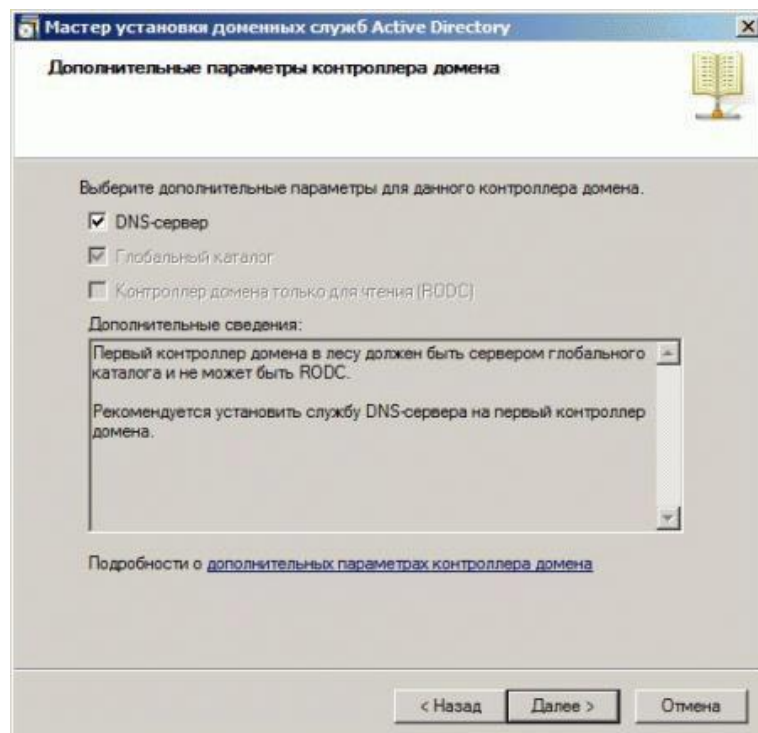


Рисунок 9 – Вибір режиму роботи лісу

У додаткових параметрах необхідно вказати опцію DNS-сервер. Так як Active Directory і служби DNS тісно пов'язані між собою, то необхідно робити кожен контролер домену DNS сервером(Рисунок 10).



		Гусев В.С.		
		Росінський Ю.М		
Змн.	Арк.	№ докум.	Підпис	Дата

Рисунок 10 – Вікно додаткових параметрів контролерів домену

Необхідно вказати пароль адміністратора режиму відновлення служб каталогів (рис унок 11).

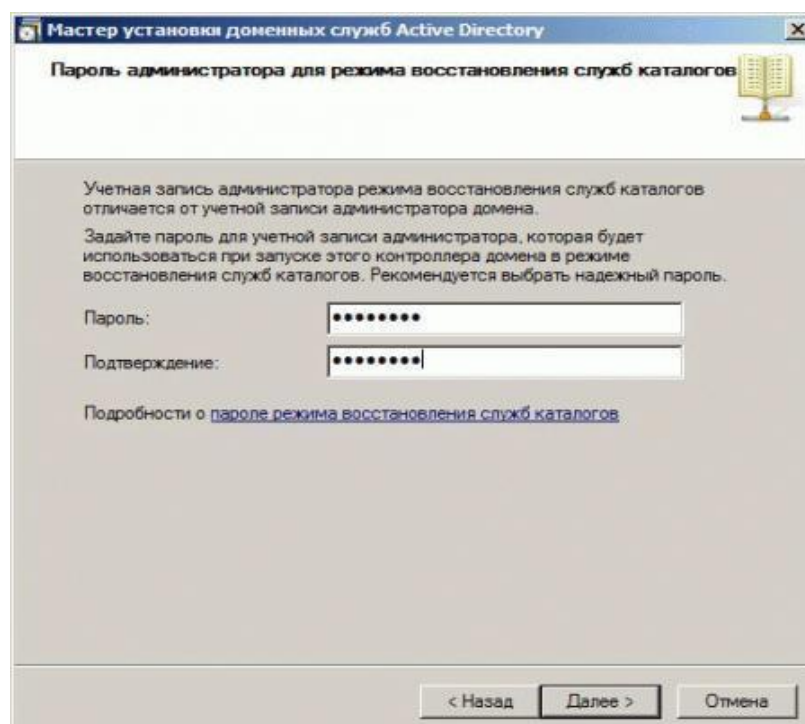


Рисунок 11 – Вікно введення паролю адміністратора режиму відновлення служб каталогів

Так як з цього моменту вже нічого змінити або виправити буде не можливо і якщо десь допущена помилка, то необхідно перевірити всі введені дані.

По завершенні роботи майстра необхідно перезавантажити сервер. Було налаштовано перший контролер домену, який також виконує роль DNS-сервера для мережі. Даний сервер буде містити записи про всі об'єкти вашого домену, при запиті записів, що відносяться до інших доменів, які він не зможе дозволити, вони будуть передані вищим серверам, т.зв. серверів пересилки.

За замовчуванням в якості серверів пересилки вказується адреса DNS-сервера з властивостей мережевого підключення, щоб згодом уникнути різного

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

роду збоїв в роботі мережі слід явно вказати доступні сервера в зовнішній мережі. Для цього необхідно відкрити оснащення DNS в диспетчері сервера і обрати сервера пересилання для свого сервера. Також необхідно вказати не менше двох доступних зовнішніх серверів, це можуть бути як сервера провайдера, так і публічні DNS-служби (рисунок 12).

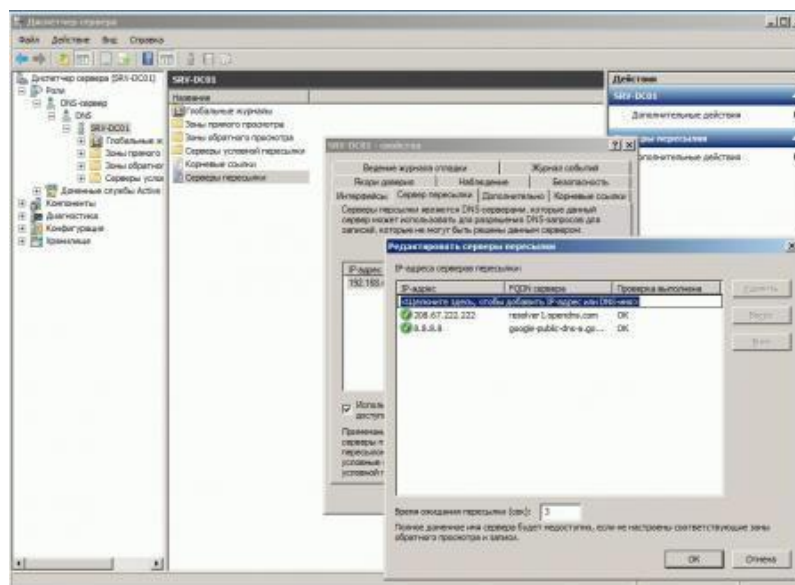


Рисунок 12 – Вікно сервера пересилання DNS

Необхідно перевірити, що у властивостях мережевого підключення контролера домену, який є DNS-сервером, як адресу DNS має бути вказано 127.0.0.1, будь-які інші варіанти записи є помилковими.

Створивши перший контролер домену, необхідно почати розгортання другого контролеру, без цього структура AD не вважається повноцінною і відмовостійкою. Як DNS-сервер потрібно вказати адресу першого контролера і ввести сервер в домен.

Після перезавантаження необхідно увійти доменним адміністратором і встановити роль Доменні служби Active Directory, після чого також запустити майстер. Принципових відмінностей в налаштуванні другого контролера немає. Обов'язково вказуємо, що це додавання нового контролеру в існуючий домен (рисунок 13).

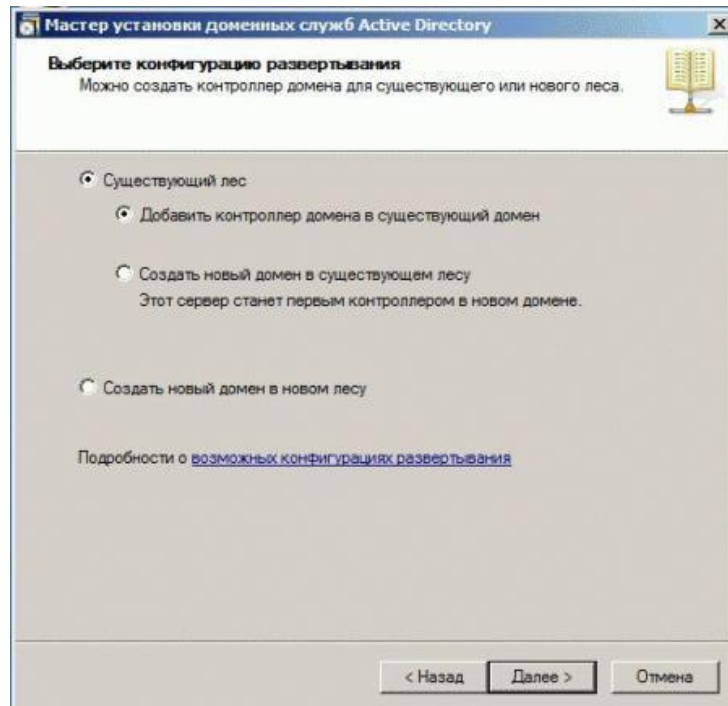
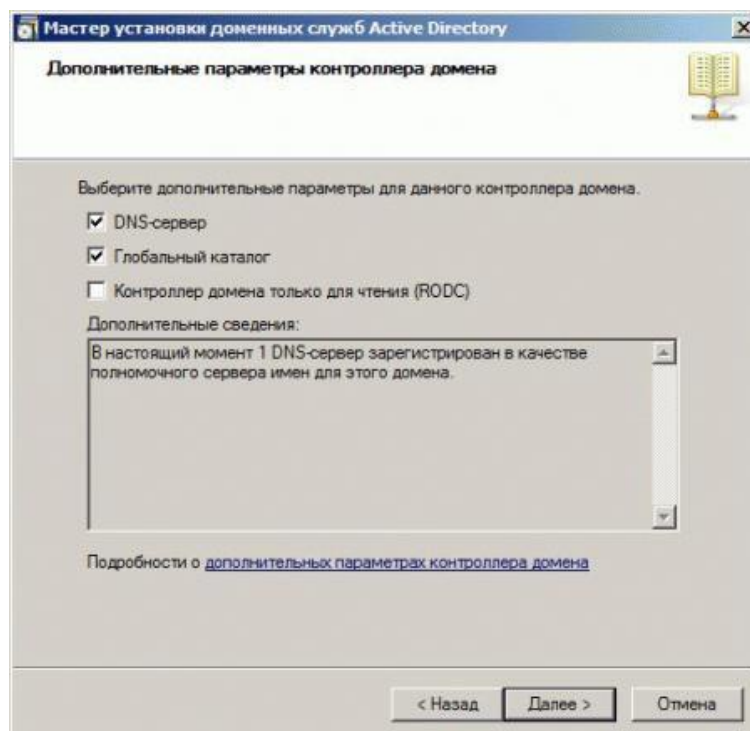


Рисунок 13 – Створення існуючого серверу в існуючий домен

Так як при відсутності глобального каталогу домен може виявитися непрацездатним, то рекомендується мати як мінімум два глобальних каталогу і додатково додавати глобальні каталоги в кожен новий домен або сайт AD (рисунок 14)



Інші налаштування повністю ідентичні. В ході розгортання другого контролера, в процесі якого виконані налаштування відповідних служб і проведена реплікація з першим контролером.

The screenshot shows the Windows XP Start menu search interface. The search query is 'Администрирование'. The results are displayed in a list on the right, with the 'Администрирование' folder highlighted. The left pane shows the search scope, including 'Все программы' (All programs) and 'Найти программы и файлы' (Find programs and files). The bottom of the window shows the Windows taskbar with the Start button and several open applications.

3.2. Налаштування ДНСР

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россинский Ю.М				40
Змн.	Арк.	№ докум.	Підпис	Дата		

На відміну від DNS або AD, DHCP не дозволяє створити два повноцінних сервера і репліціювати дані між ними. Єдиний DHCP-сервер здатний доставити чимало проблем системному адміністратору, сервер з цією роллю навіть на профілактику вивести проблемно, не кажучи вже про збої.

Зазвичай DHCP-сервер суміщають з роутером, в простих мережах даний підхід виправданий, в структурі AD рекомендовано поєднати ролі контролера домену та DHCP-сервера. Для створення відмовостійкої схеми знадобилося два DHCP-сервера, між якими необхідно розділити пул адрес області. Рекомендується співвідношення 80/20, але можна відношення ставити будь-яке (рисунок 16).

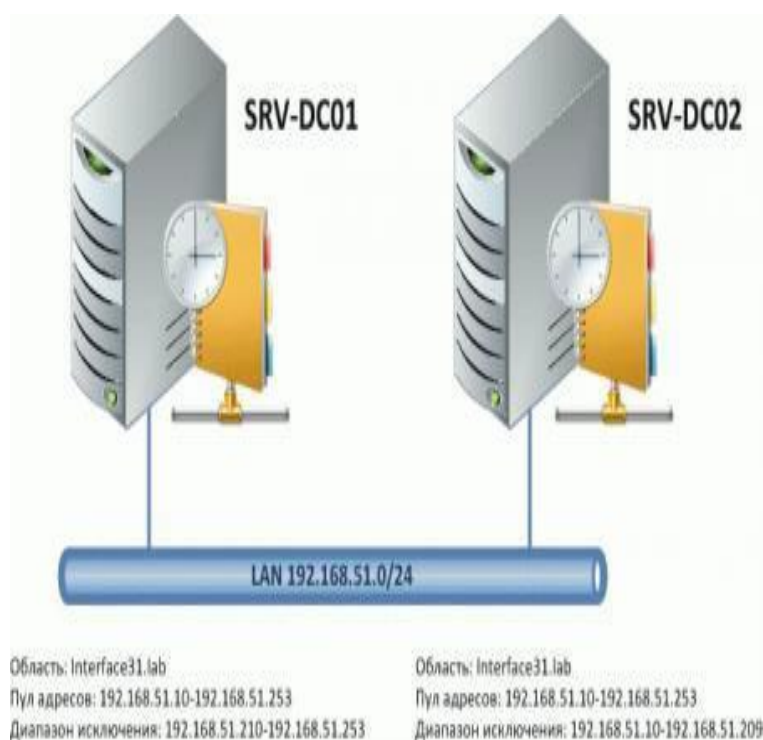


Рисунок 16 – Схема підключення DHCP серверів

Однак перед тим як розподілити пул адреси, варто зробити схему розподілу адрес у мережі.

В даній мережі , дотримуємося такої схеми показаної на рисунок 17.



Рисунок 17 – Схема розподілу адрес пулу

Основною перевагою даного підходу є те, що зустрівши IP-адресу 192.168.51.203 можна знати точно , що це один з мережевих принтерів, а 192.168.51.51 - Wi-Fi обладнання.

З урахуванням даної схеми було відділення пул DHCP-адрес і поділ його в співвідношенні 80/20. У даному випадку це діапазони до і після адреси (включно) 192.168.51.210.

Блок адрес 1-10 - не використовується, так як правило багато мережевих пристроїв налаштовані на використання адреси 192.168.x.1 за замовчуванням і мережеві злоумисники при спробі підключитися до мережі використовують адреси з цього діапазону. Особливо це актуально для мереж діапазонів 192.168.0.0 і 192.168.1.0, тому краще вибрати для корпоративної мережі інший діапазон.

На першому контролері домену запускаємо Диспетчер сервера і додаємо роль DHCP-сервера (рисунок 18):

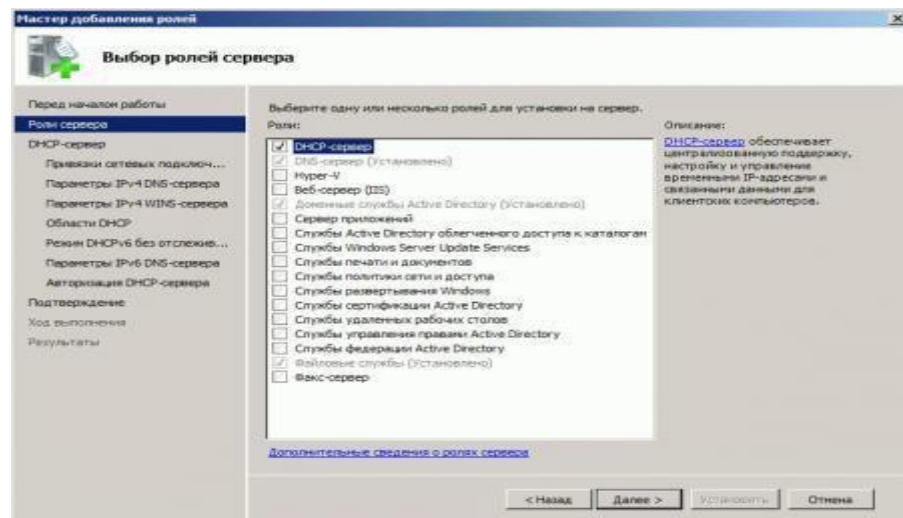


Рисунок 18 – Створення ролі DHCP-сервера

Як батьківський домен вказано домен AD, як DNS-серверів адреса контролера домену (рисунок 19).

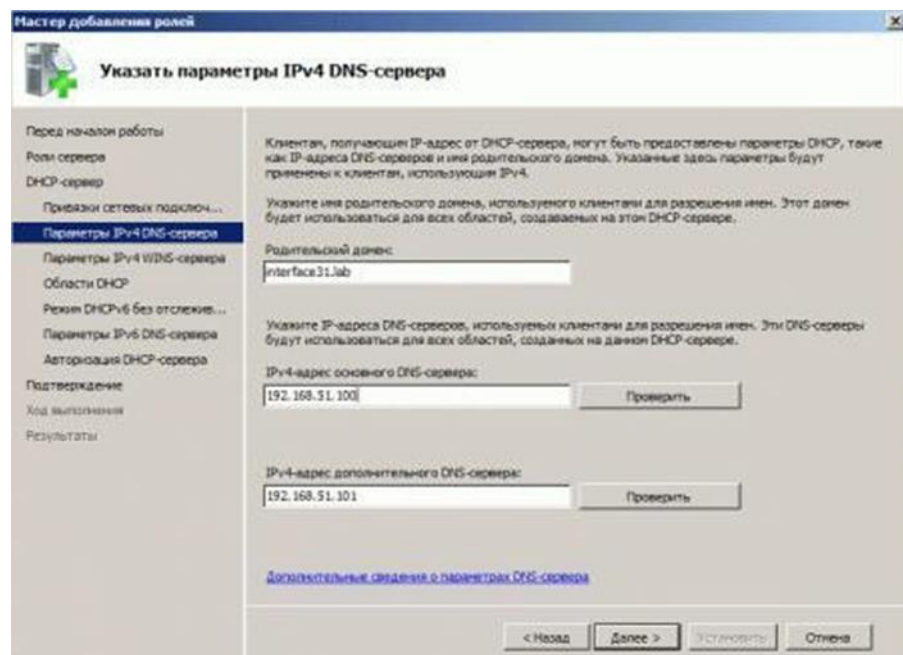


Рисунок 19 – Налаштування IPv4 DNS-сервера

Наступним кроком додаємо область, в налаштуваннях необхідно вказати повний діапазон адрес: 192.168.51.10-.192.168.51.253 (рисунок 20).

		Гусев В.С.			ККИКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

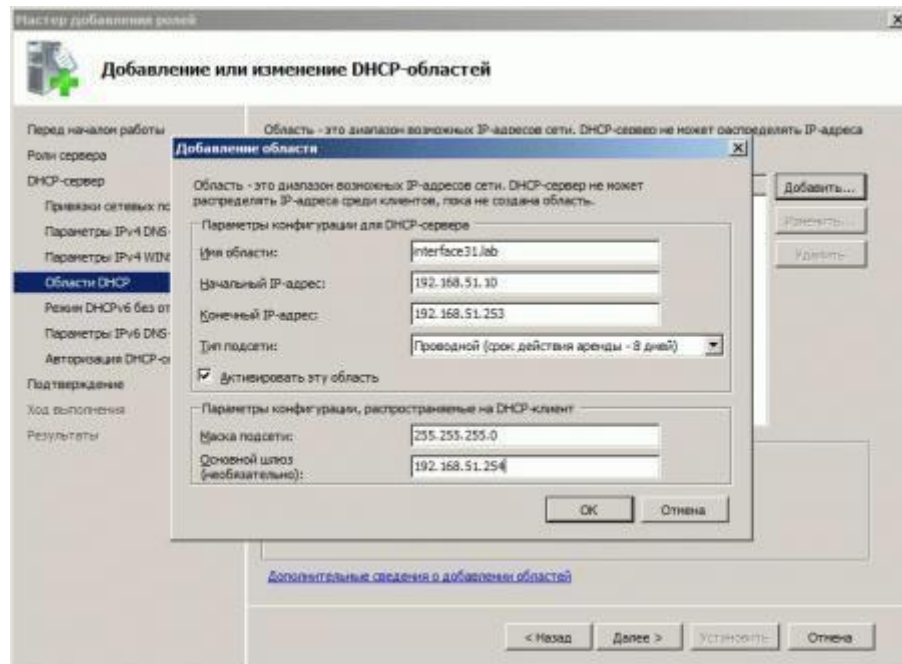


Рисунок 20 – Налаштування повного діапазону адрес

Потім DHCP-сервер потрібно авторизувати в AD, увійшли в систему як адміністратор домена додаткових дій не потрібно, інакше потрібно вказати облікові дані доменного адміністратора (рисунок 21).

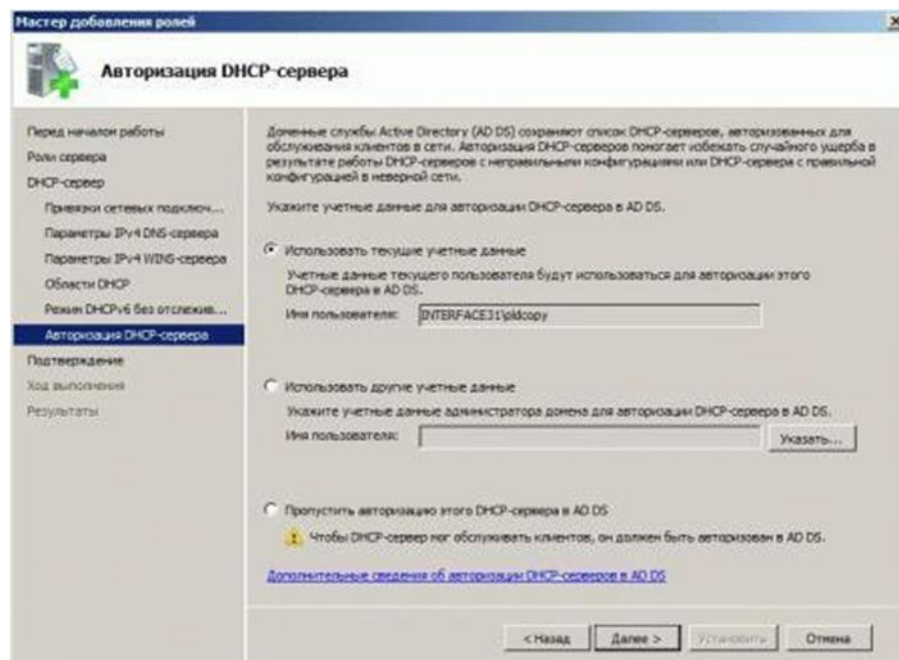


Рисунок 21 – Авторизація DHCP-сервера

Необхідно перевірити всі введені дані і встановити роль DHCP-сервера, перейти в оснастку управління цією роллю і задати діапазони виключення (рисунок 22).

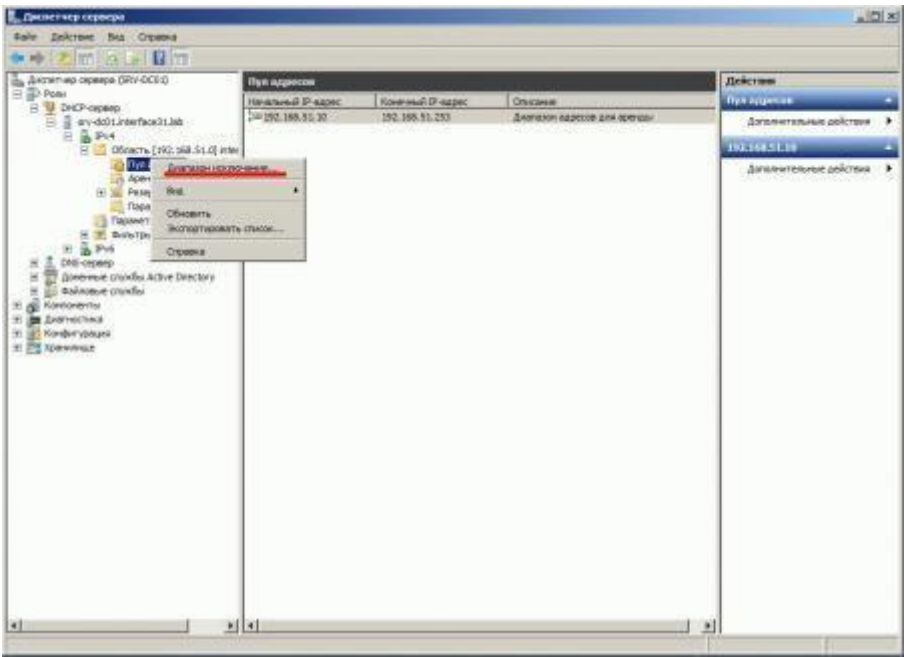


Рисунок 22 – Вікно параметрів серверу

В результаті повинно вийти налаштування зображене на рисунок 23:

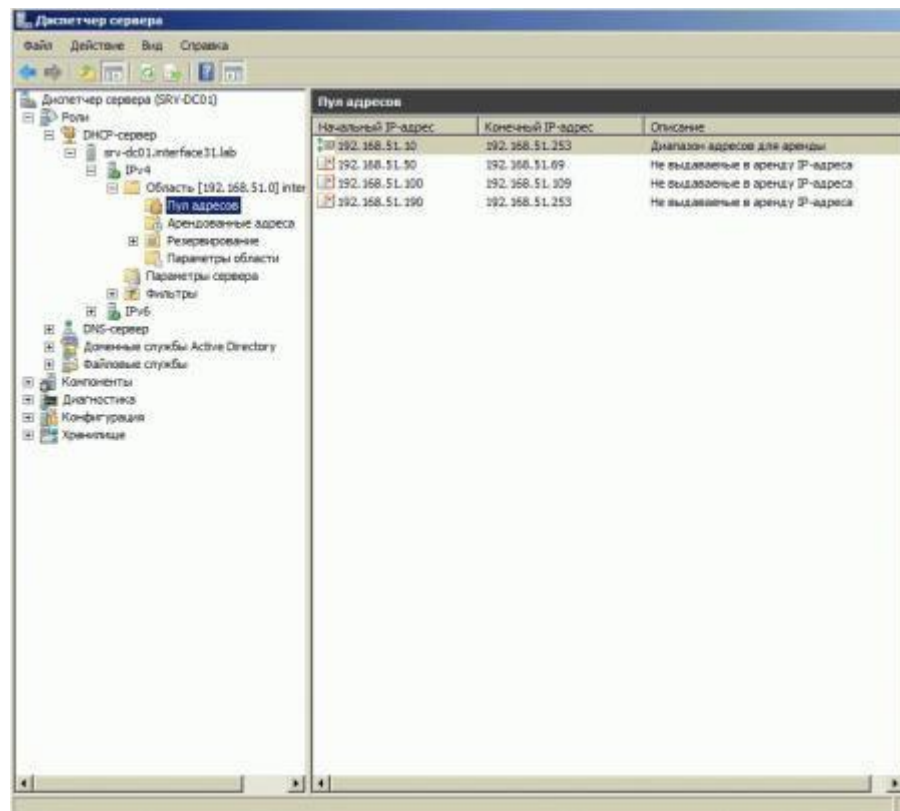


Рисунок 23 – Налаштовані виключені діапазони IP-адрес

Тепер аналогічним чином додаємо і налаштовуємо роль DHCP на другому контролері домену. Налаштуванню області особливої уваги не приділяємо, все одно її доведеться видалити (рисунок 24):

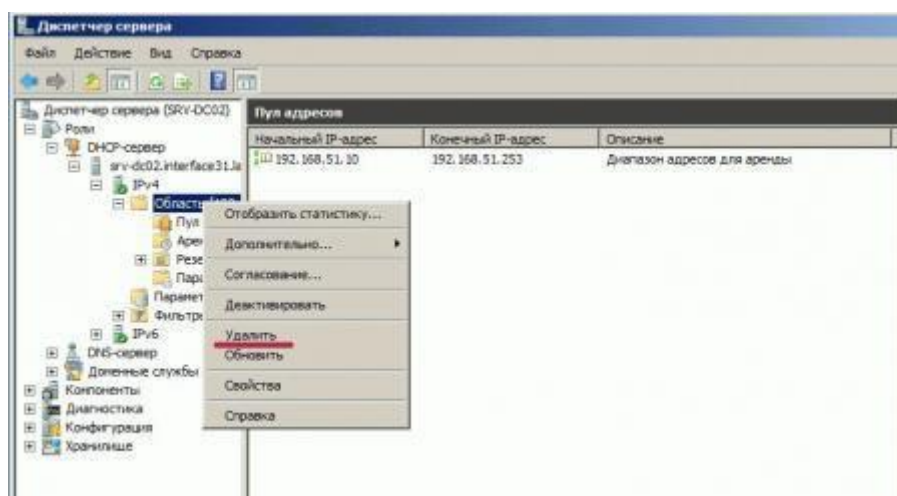


Рисунок 24 – Видалення налаштувань області

На другому контролері домену видаляємо створену область і знову переходимо на перший контролер домену. Необхідно відкрити DHCP-області і обрати Розділені області (рисунок 25).

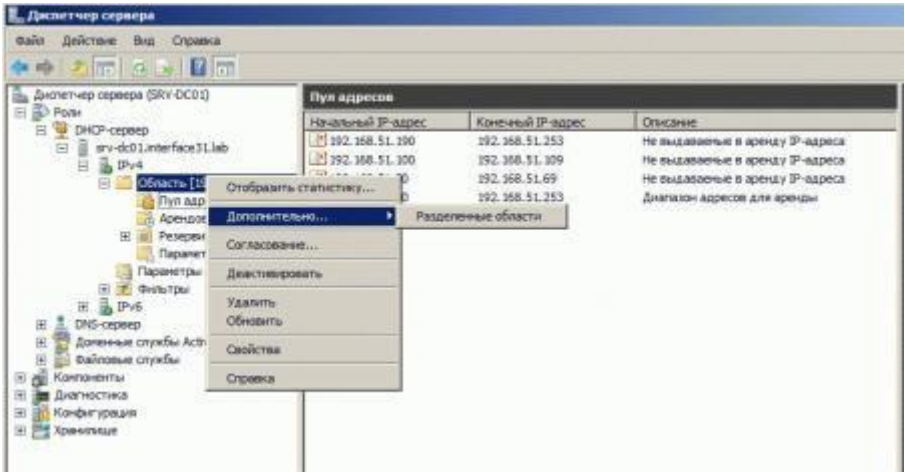


Рисунок 25 – Контекстне меню DHCP-області

У відкритому майстрі конфігурацій потрібно вибрати додатковий (другий) DHCP-сервер (рисунок 26):

Мастер конфигурации с разделенными областями DHCP

Дополнительный DHCP-сервер
 Выберите другой DHCP-сервер, на котором необходимо настроить область в рамках разделения областей.

Дополнительный DHCP-сервер:

Несущий DHCP-сервер:

Имя узла для сервера:

Адрес IPv4 сервера:

Рисунок 26 – Майстер конфігурацій с розділеними областями DHCP

Необхідно вказати пропорції в яких слід розгорнути область. Більш точні налаштування можна задати вручну (рисунок 27).

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Мастер конфигурации с разделенными областями DHCP

Процентное соотношение разделения
Выберите процентное соотношение разделения диапазона IP-адресов между серверами.

Переместите ползунок для выбора процентного соотношения разделения диапазона адресов IPv4 в данной области:

192.168.51.10 192.168.51.253

0 50 100

Процентное соотношение адресов IPv4

	Несущий DHCP-сервер	Добавленный DHCP-сервер
% обслуживаемых адресов IPv4:	80	20

Ниже указан исключаемый диапазон адресов IPv4:

	Несущий DHCP-сервер	Добавленный DHCP-сервер
Начальный адрес IPv4:	192 . 168 . 51 . 205	192 . 168 . 51 . 10
Конечный адрес IPv4:	192 . 168 . 51 . 253	192 . 168 . 51 . 204

Примечание. Существующие исключения соответствующим образом настраиваются на DHCP-серверах.

< Назад Далее > Отмена

Рисунок 27 – Налаштування області DHCP-серверу

Потрібно вказати затримки відповіді серверів, так як перший сервер основний, то було зазначено для другого сервера затримку в 10 мс, це дозволить видавати всі адреси першим сервером, використовуючи другий тільки при відмові першого або заповненні його пулу адрес (рисунок 28).

Мастер конфигурации с разделенными областями DHCP

Задержка предложения DHCP
Укажите значение задержки (в миллисекундах), с которой осуществляется распределение адресов добавленным DHCP-сервером.

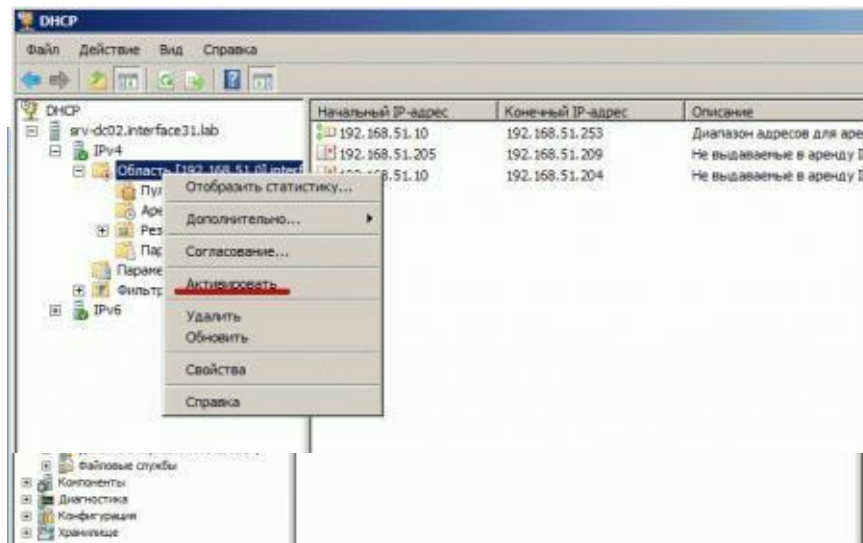
Задержка предложения DHCP в миллисекундах:

	Несущий DHCP-сервер:	Добавленный DHCP-сервер:
	0	10

< Назад Далее > Отмена

Рисунок 28 – Налаштування затримки відповіді DHCP-серверу

Після закінчення роботи майстра область буде розділена і на першому



сервері вона набуде вигляду, як на рисунку 29:

Рисунок 29 – Розділена область DHCP-серверу

На другому сервері, доведеться видалити зайвий діапазон виключення вручну, щоб діапазони не конфліктували (рисунок 30):

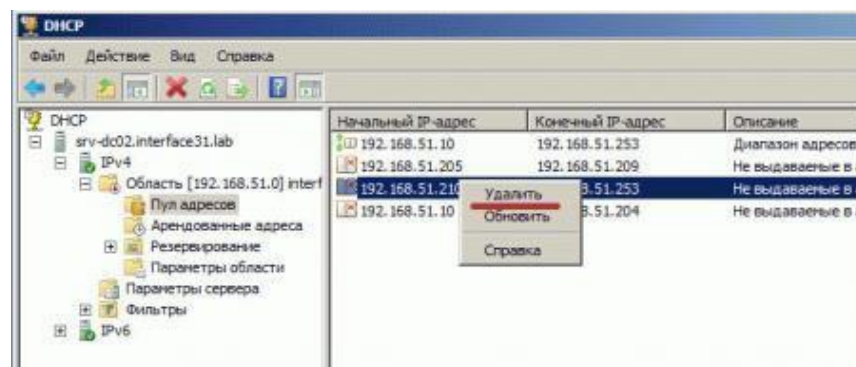


Рисунок 30 – Видалення непотрібного діапазону

Переконавшись що обидва сервера обслуговують непересічні частини області, необхідно активувати область на другому сервері (рисунок 31):

Рисунок 31 – Активування області IP-адресс

У разі відмови або виводу на профілактику основного DHCP-сервера, другий сервер обробить запити клієнтів з орендою адреси яка закінчується (за умовчанням 8 днів), якщо основний сервер вибув на більший термін, то на додатковому DHCP- сервері необхідно розширити пул адрес, в подальшому зробивши даний сервер основним, а інший сервер додатковим.

У будь-якому випадку даний підхід дозволяє забезпечити безперебійне функціонування мережевої інфраструктури незалежно від працездатності окремих вузлів

3.3. Перенесення облікових записів в домен

Отже, є робоча станція за якою працює співробітник, яку потрібно ввести в домен. В першу чергу необхідно переконатися що ПК має бажане ім'я і при необхідності перейменувати комп'ютер, а також перезавантажитися. Необхідно правильно налаштувати мережу, так як в мережі розгорнутий DHCP-сервер, досить встановити автоматичне отримання мережевих параметрів і переконатися в отриманні правильних значень (рисунок 32).

		Гусєв В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М				51
Змн.	Арк.	№ докум.	Підпис	Дата		

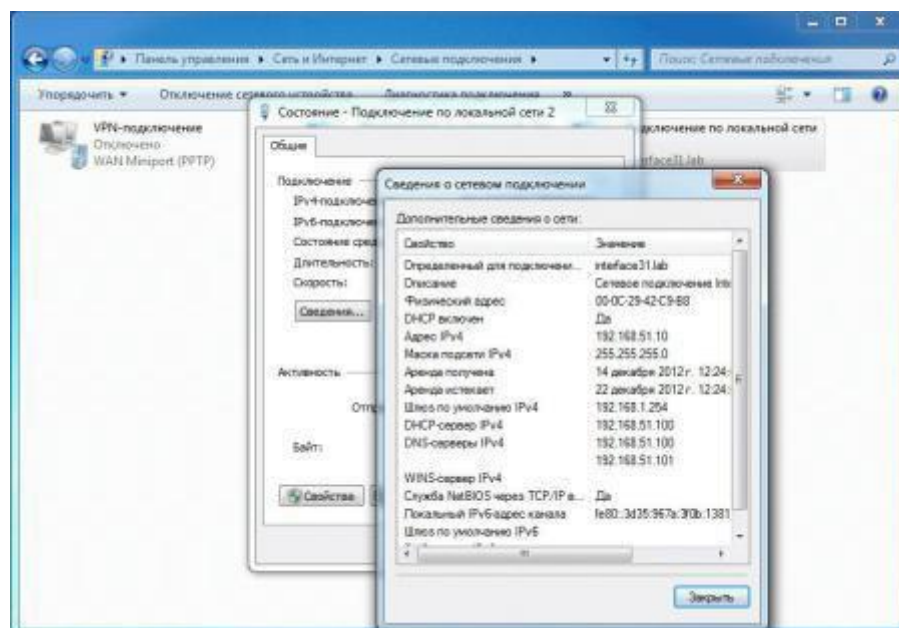


Рисунок 32 – Перевірка мережевих параметрів

Для серверів, які повинні мати статичні мережеві параметри необхідно вказати необхідні значення вручну, особливу увагу слід приділити DNS-серверам, це повинні бути адреси двох будь-яких контролерів домену (які поєднують роль DNS-сервера), в іншому випадку не вийде ввести такий комп'ютер в домен.

Якщо потрібно щоб будь-яка робоча станція мала статичну адресу, то не варто вказувати його вручну, правильно буде використовувати таку функцію DHCP-сервера як резервування. Це дозволить в подальшому змінювати налаштування мережі без необхідності вносити зміни на кожній робочій станції (наприклад поміняти адресу шлюзу). Для резервування потрібно відкрити «оснащення управління DHCP-сервером», перейти в папку «Орендовані адреси» та клацнути на потрібному хості правою кнопкою миші, вибрати «Додати до резервування». Цими діями виділена адреса закріпиться за комп'ютером на постійній основі (рисунок 33).

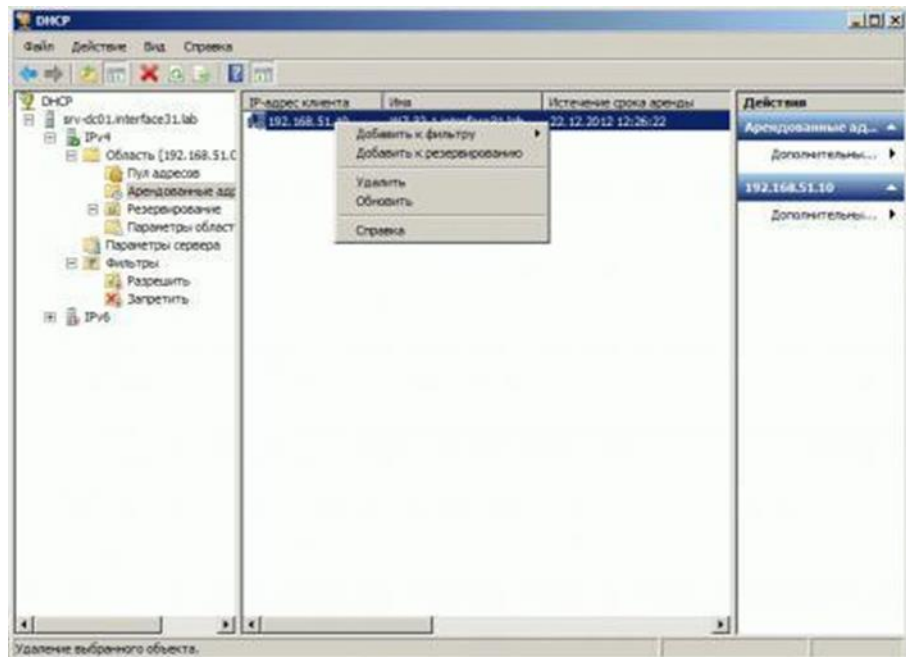


Рисунок 33 – Закріплення IP-адреси за обраною робочою станцією

На даному етапі необхідно включити комп'ютер в домен. Для цього потрібно перейти в «Свойства системы - Имя компьютера» і натиснути кнопку «Изменить», вибрати «Является членом домена» і вказати ім'я домену в який потрібно увійти, натиснути ОК, та вказати ім'я та пароль користувача який має право на включення комп'ютера в домен (за замовчуванням адміністратор домену)(рисунок 34).

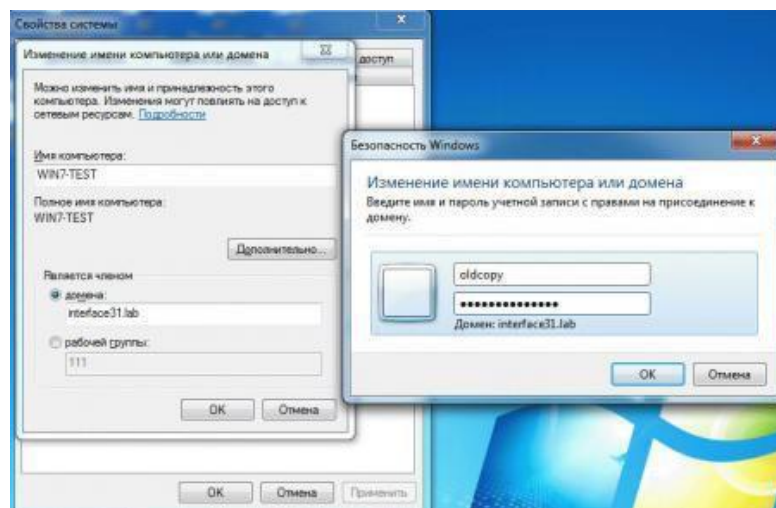


Рисунок 34 – Додавання комп'ютеру в домен

Після перезавантаження можна увійти під доменним обліковим записом, який потрібно попередньо створити на будь-якому з контролерів домену. Для цього потрібно відкрити оснащення «Active Directory - пользователи и компьютеры», перейти в папку «User» і створити там нового користувача (рисунк 35).

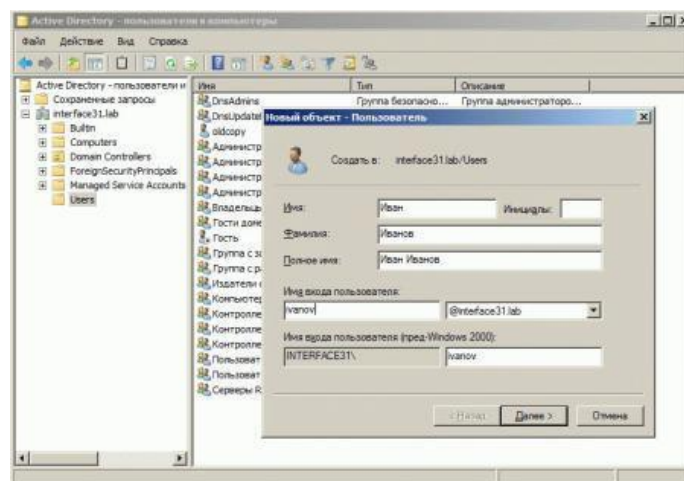


Рисунок 35– Створення нового користувача

В систему можна увійти під ім'ям нового користувача. І переконатися в тому, що працюючи під локальним обліковим записом користувач мав звичним чином розташовані файли, папки і ярлики, програми були відповідним чином налаштовані, крім того мінявся обліковий запис пошти, закладки браузера і т.д. Був отриманий чистий профіль, який необхідно налаштовувати заново (рисунк 36).

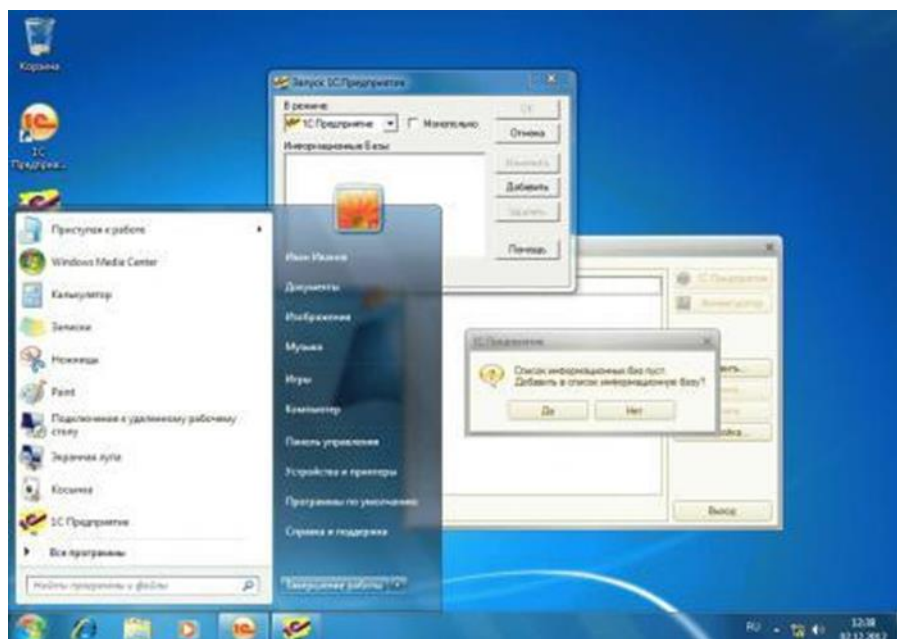


Рисунок 36 – Вигляд тільки-но створеного користувача

На цьому етапі необхідно перенести профіль локального облікового запису в доменний. Для цього було використано інструмент User State Migration Tool, який входить до складу Пакета автоматичної установки Windows (AIK), так як даний пакет немає необхідності встановлювати на всіх ПК, цілком достатньо буде установити на комп'ютер адміністратора або один з серверів. Цей набір утиліт знаходиться в папці C: \ Program Files \ Windows AIK \ Tools \ USMT потрібно скопіювати їх на цільову систему або зробити доступними по мережі (рисунок 37).

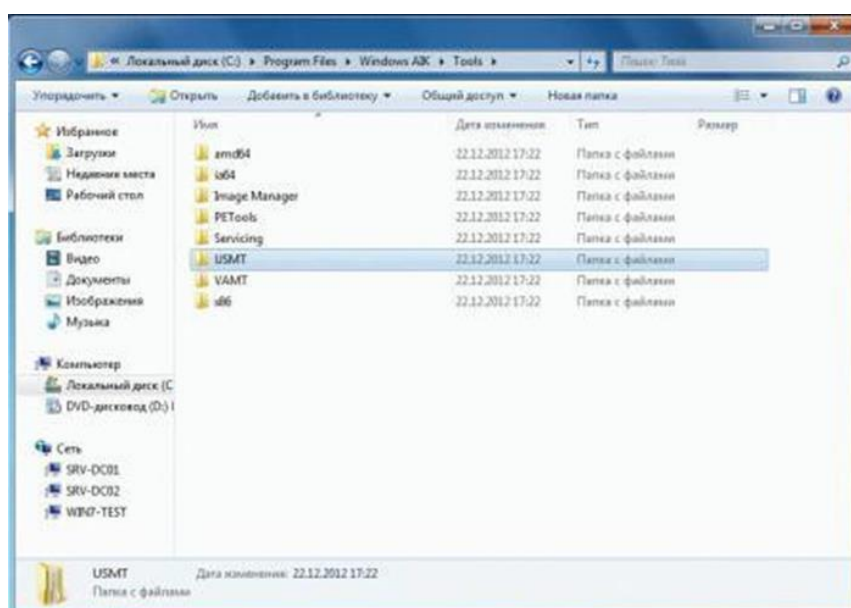


Рисунок 37 – Знаходження набору утіліт

Процес перенесення профілю складається з двох етапів: створення файлу перенесення з даними і параметрами зазначеного користувача і відновлення профілю з файлу перенесення, причому зробити це можна на будь-якому ПК, що дозволяє швидко перенести профіль з одного ПК на інший при заміні комп'ютера. Але необхідно пам'ятати, що можна перенести профіль з 32-х розрядної системи в 64-х розрядну, однак зворотній перенос з 64-х розрядної в 32-х розрядну неможливий.

Для створення файлу перенесення використовувалась утиліта ScanState. У цьому випадку буде переноситись локальний профіль користувача WWW в профіль доменного користувача ivanov. Для створення файлу перенесення необхідно увійти в систему під обліковим записом адміністратора домену, перейти в папку з потрібною версією USMT (32 або 64 біт) і виконати наступну команду: scanstate C: \ Migration \ User /i:miguser.xml /i:migapp.xml / v: 13 / ue: * \ * / ui: WWW /l:C:\Migration\scan.log

Синтаксис команди переводиться як:

- перший аргумент вказує розташування файлу перенесення,
- ключ / i: вказує які правила перенесення слід використовувати,
- ключ / v: задає необхідний рівень деталізації лога,
- поєднання ключів / ue: i / ui: виключає з перенесення всіх користувачів окрім WWW,
- ключ / l: визначає розташування балки.

Результатом виконання команди буде короткий звіт який зображений на рисунку 38:

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М				56
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Администратор: C:\Windows\system32\cmd.exe

C:\Program Files\Windows AIK\Tools\USMT\x86>scanstate C:\Migration\User /i:miguser.xml /i:nigapp.xml /u:13 /ue:* /ui:WUW /l:C:\Migration\scan.log

Log messages are being sent to 'C:\Migration\scan.log'

Starting the migration process
Processing the settings store

Examining the system to discover the migration units
WIN7-TEST\WUW (1 of 2): 100% done
This Computer (2 of 2): 100% done

Selecting migration units

Gathering data
WIN7-TEST\WUW (1 of 2): 100% done
This Computer (2 of 2): 100% done
Commit

Success.

ScanState return code: 0

C:\Program Files\Windows AIK\Tools\USMT\x86>

```

Рисунок 38 – Звіт команди scanstate

Файл перенесення створений, але так як в цю систему вже здійснювався вхід під цільовим користувачем, то необхідно видалити або перейменувати папку з профілем в каталозі C: \ Users і видалити відповідний профілю розділ в гілці реєстру: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ ProfileList (рисунок 39)

Так як в іншому випадку при спробі відновлення профілю буде отримано помилку з кодом 71: LoadState return code: 71.

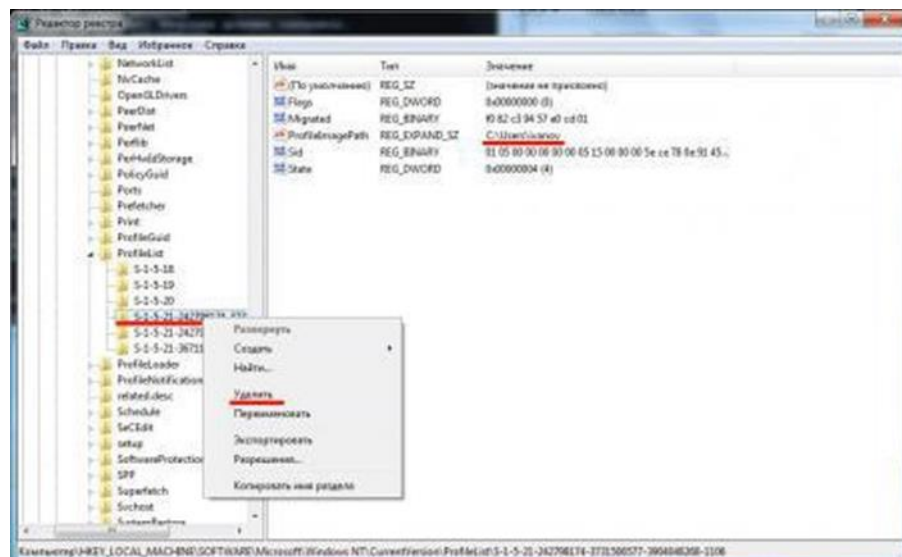


Рисунок 39 – Видалення профілю в редакторі реєстру

Відновлення профілю буде виконано за допомогою утиліти LoadState. Для перенесення профілю необхідно використати наступну команду: loadstate

C: \ Migration \ User /i:miguser.xml /i:migapp.xml / v: 13
/mu:WWW:interface31.lab\ivanov /l:C:\Migration\load.log

Структура команди багато в чому схожа на попередню, однойменні ключі мають аналогічне значення, ключ / mu: вказує вихідний профіль і профіль призначення, доменні облікові записи вказуються як Domain \ User. У цьому випадку профіль локального користувача WWW буде відновлений в профіль користувача interface31.lab \ ivanov (рисунок 40).

```
C:\Program Files\Windows AIK\Tools\USMT\x86>loadstate C:\Migration\User /i:miguser.xml /i:migapp.xml /v:13 /mu:WWW:interface31.lab\ivanov /l:C:\Migration\load.log
Log messages are being sent to 'C:\Migration\load.log'
Starting the migration process
Processing the settings store
Selecting migration units
Examining the system to discover the migration units
  interface31.lab\ivanov (1 of 2): 100% done
  This Computer (2 of 2): 100% done
Applying data
  UIN7-TEST\WWW (1 of 2): 100% done
  This Computer (2 of 2): 100% done
Success.
LoadState return code: 0
C:\Program Files\Windows AIK\Tools\USMT\x86>
```

Рисунок 40 – Звіт команди loadstate

Тепер, увійшовши під доменним обліковим записом користувач виявить звичне робоче оточення, як видно на рисунку 41, переноситься навіть вміст кошика.

Рисунок 42 – Знаходження утиліти moveuser

Для перенесення профілю необхідно увійти на цільовий ПК як адміністратор домена і виконати команду: `moveuser www interface31.lab\ petrov /y` (рисунок 43)

Синтаксис даної утиліти набагато простіше. Ключ `/y` дозволяє перезаписати профіль навідь якщо він існує, тобто можна попередньо виконати вхід доменним користувачем на цю машину, це ніяк не завадить переносу, після перенесення вхід під локальним користувачем буде неможливий, якщо необхідно використовувати локальний профіль, потрібно додатково вказати ключ `/k`.



Рисунок 43 – Виконання команди moveuser

Виконаємо вхід під доменної записом користувача Петров і переконаємося що він може продовжувати роботу в домені зі звичним робочим оточенням (рисунок 44).

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 44 – Робочий стіл користувача після переносу профілю

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В ході виконання дипломної роботи було розглянуто основні методи підвищення функціонування корпоративної мережі. Була побудована модель інформаційно-телекомунікаційної системи (інфраструктури) підприємства з використанням локальних корпоративних доменів, що управляються за допомогою контролеру домену, а саме компонента Active Directory.

Active Directory було обрано як основний інструмент через його широко профільний функціонал, гнучкість та можливість локального налаштування політик для різних вимог користувачів.

Практична значущість роботи полягає в реалізації на практиці заходів з проектування та налагодженню доступу до загальних ресурсів локальної мережі, таким як спільне використання мережевих папок, а також для розділення різних підрозділів всередині корпоративної мережі.

В ході реалізації було виконано наступні дії: аналіз існуючих технологій, підбір апаратно-програмних засобів, налаштування обладнання.

Після виконання даної роботи, було виявлено, що цю мережу можна легко проектувати, просте розширення, висока та стабільна робота сервісів та захист інформації. Дану мережу можна використовувати у будь-яких фірмах від малого великого бізнесу. Простий та зручний інтерфейс дає можливість керувати даними користувачів без прямої взаємодії з ними, що в наш час дуже актуально.

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Windows Server documentation. – URL: <https://docs.microsoft.com/uk-ua/windows-server/>
(date of access: 20.06.2023).
2. Розгортаємо Active Directory усіма можливими методами. URL: –
Режим доступу до ресурсу: <https://habr.com/ru/company/ultravds/blog/480776/>
(date of access: 20.06.2023)
3. Active Directory Security Groups. URL: – Режим доступу до ресурсу:
<https://docs.microsoft.com/uk-ua/windows/security/identity-protection/access-control/active-directory-security-groups>
(date of access: 20.06.2023).
4. Станек У. Microsoft Windows Server 2012 R2: зберігання, безпека, мережеві компоненти. Довідник адміністратора / У. Станек. - СПб.: BHV, 2015. – 416 с
5. Холмс Лі Windows PowerShell. Кишеньковий довідник; ЕКОМ Паблішерз -, 2013. - 160 с.
6. Active Directory, 4th Edition / [B. Desmond, J. Richards, R. Allen та ін.], 2008. – 866 с
7. Оліфер, В. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник / В. Оліфер, Н. Оліфер. - СПб.: Пітер, 2016. - 318 с.
8. Мінас, Марк Windows Server 2012 R2. Повне керівництво. Том 1. встановлювати і налаштовувати сервера, мережі, DNS / Марк Мінас і ін. -2017. - 960 с.
9. PowerShell Documentation. – URL: <https://docs.microsoft.com/en-us/powershell/> (date of access: 20.06.2023)
10. Contributors to Wikimedia projects. Computer forensics - Wikipedia. Wikipedia, the free encyclopedia. URL:
https://en.wikipedia.org/wiki/Computer_forensics

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Россінський Ю.М				63
Змн.	Арк.	№ докум.	Підпис	Дата		

(date of access: 22.06.2023).

11. Autopsy. Data and information recovery - Hacker's Basement. URL:
<https://hacker-basement.com/2023/01/09/vosstanovlenie-dannix-autopsy/>

(date of access: 22.06.2023).

		Гусев В.С.			ККІКБ.КР.Б – 125 – 6 – ПЗ	Арк.
		Росінський Ю.М.				64
Змн.	Арк.	№ докум.	Підпис	Дата		