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: «Проєкт захищеного корпоративного файлового сховища з використанням NAS-технологій»

Виконала: студентка 4-го курсу групи КБ-22-2
спеціальності 125 «Кіберберзпека»
_____ Анастасія ШИПОВИЧ
Керівник: доцент кафедри КІ та КБ, к.т.н.
_____ Олексій ШЕЛУХА
Рецензент: доцент кафедри КІ та КБ, к.т.н., доцент
_____ Юрій РОССІНСЬКИЙ

Житомир - 2026

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
02 лютого 2026 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студент: Шипович Анастасія Іванівна
Тема роботи: «Проєкт захищеного корпоративного файлового сховища з використанням NAS-технологій»
затверджена Наказом університету від від 2 лютого 2026 р. №58/с
Термін здачі студентом закінченої роботи 08 червня 2026 р.

Вихідні дані роботи: процеси резервного копіювання та відновлення інформації в корпоративному мережному середовищі; принципи побудови та функціонування корпоративного файлового сховища; модель розмежування доступу Zero Trust, засоби моніторингу стану мережі та аналізу подій безпеки.

Обладнання та програмне забезпечення:

1. Доменна інфраструктура (Active Directory, DNS, DHCP тощо);
2. Віддалене сховище NAS-SERVER і Windows Server Backup;
3. Робочі станції Windows та Linux.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ольга ДЯЧУК	02.02.2026	02.02.2026
2	Ольга ДЯЧУК	02.02.2026	02.02.2026
3	Ольга ДЯЧУК	02.02.2026	02.02.2026

Студентка _____ Анастасія ШИПОВИЧ

Керівник _____ Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання та аналіз предметної області дослідження	02.02.2026 - 09.02.2026	Виконано
2	Дослідження принципів організації захищених файлових сховищ	10.02.2026 - 23.02.2026	Виконано
3	Аналіз технологій забезпечення безпеки та надійності зберігання даних	24.02.2026 - 09.03.2026	Виконано
4	Обґрунтування вибору програмних та технічних засобів реалізації	10.03.2026 - 16.03.2026	Виконано
5	Проєктування та розгортання віртуальної корпоративної інфраструктури	17.03.2026 - 06.04.2026	Виконано
6	Налаштування доменної інфраструктури та керування доступом користувачів	07.04.2026 - 20.04.2026	Виконано
7	Реалізація захищеного файлового сховища та політик доступу	21.04.2026 - 04.05.2026	Виконано
8	Забезпечення відмовостійкості, резервного копіювання та моніторингу системи	05.05.2026 - 18.05.2026	Виконано
9	Підключення робочих станцій та тестування роботи розробленої системи	19.05.2026 - 31.05.2026	Виконано
10	Оцінка ефективності реалізованої системи та формування висновків	01.06.2026 - 05.06.2026	Виконано
11	Оформлення пояснювальної записки	06.06.2026 - 08.06.2026	Виконано

Студентка _____ Анастасія ШИПОВИЧ

Керівник _____ Олексій ШЕЛУХА

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра на тему: «Проєкт захищеного корпоративного файлового сховища з використанням NAS-технологій».

У межах кваліфікаційної роботи було розроблено та реалізовано проєкт віртуальної інфраструктури корпоративноого файлового сховища.

Пояснювальна записка до кваліфікаційної роботи містить 104 сторінок, 79 рисунків, 6 таблиць, список використаних джерел із 38 найменувань розміщених на 4 сторінках.

Метою кваліфікаційної роботи є розробка та реалізація захищеного файлового сховища з використанням технологій централізованого керування доступом, резервного копіювання та моніторингу для забезпечення надійного зберігання інформації в корпоративній мережі.

У першому розділі кваліфікаційної роботи представлено аналіз сучасних засобів та підходів до організації безпечної корпоративної мережної інфраструктури, зокрема файлових сховищ. Розглянуто особливості функціонування корпоративної мережі, що ґрунтується на централізованому використанні серверних ресурсів і робочих станцій користувачів, технології мережного зберігання даних NAS, методи забезпечення відмовостійкості із використанням RAID 1, механізмів резервного копіювання, а також підходи до контролю доступу на основі ACL та концепції Zero Trust.

У другому розділі виконано проєктування архітектури захищеного корпоративного файлового сховища. Розроблено модель серверних та корпоративних компонентів корпоративної мережі з використанням віртуального середовища Oracle VM VirtualBox. Визначено структуру інфраструктури, яка включає контролер домену DC-SERVER, файловий сервер FILE-SERVER, резервне сховище NAS-SERVER, а також робочі станції Windows та Linux.

					ККІКБ.КР.Б – 125 – 13 – ПЗ	
Змн.	Арк.	№ докум.	Підпис	Дата		
Розроб.		Шипович А.І.		26.06.26	Проєкт захищеного корпоративного файлового сховища з використанням NAS-технологій	Літ. / Арк. 4 / Аркушів 104
Керівник		Шелуха О.О.		26.06.26		
Реценз.		Россінський Ю.М.		26.06.26		ФІКТ, Гр. КБ-22-2
Н. контр.		Шелуха О.О.		26.06.26		
Затверд.		Єфіменко А.А.		26.06.26		

У третьому розділі висвітлено процес розгортання розробленого рішення та практичної реалізації захищеного файлового сховища. Було налаштовано доменну інфраструктуру на основі Active Directory, DNS та DHCP, створено користувачів і групи доступу, реалізовано файловий сервер із використанням SMB та розмежуванням прав доступу за допомогою ACL відповідно до принципів Zero Trust. Для забезпечення відмовостійкості даних було налаштовано RAID 1, а резервне копіювання організовано із використанням Windows Server Backup зі збереженням копій на NAS-SERVER через мережне сховище. Резервування даних виконується у заданий момент часу відповідно до налаштованого процесу створення резервних копій. Також виконано підключення корпоративних станцій Windows та Linux до корпоративної мережі й перевірено доступ до файлових ресурсів. Для контролю стану інфраструктури впроваджено систему моніторингу PRTG Network Monitor, яка забезпечує спостереження за доступністю серверів, станом ресурсів та параметрами роботи мережних вузлів.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА МЕРЕЖА, ФАЙЛОВЕ СХОВИЩЕ, NAS, ACTIVE DIRECTORY, ZERO TRUST, RAID 1, РЕЗЕРВНЕ КОПІЮВАННЯ.

ANNOTATION

Bachelor's final qualification work on the topic: "Project of a secure corporate file storage using NAS technologies".

As part of the qualification work, a project of a virtual infrastructure of a corporate file storage was developed and implemented.

The explanatory note to the qualification work contains 104 pages, 79 figures, 6 tables, a list of used sources with 38 names placed on 4 pages.

The purpose of the qualification work is to develop and implement a secure file storage using centralized access control technologies, backup and monitoring to ensure reliable storage of information in a corporate network.

The first section of the qualification work presents an analysis of modern tools and approaches to organizing a secure corporate network infrastructure, in particular file storage. The features of the functioning of a corporate network based on the centralized use of server resources and user workstations, NAS network storage technologies, methods for ensuring fault tolerance using RAID 1, backup mechanisms, as well as approaches to access control based on ACL and the Zero Trust concept are considered.

In the second section, the architecture of a secure corporate file storage is designed. A model of server and corporate components of a corporate network is developed using the Oracle VM VirtualBox virtual environment. The infrastructure structure is determined, which includes the DC-SERVER domain controller, the FILE-SERVER file server, the NAS-SERVER backup storage, as well as Windows and Linux workstations.

The third section highlights the process of deploying the developed solution and the practical implementation of a secure file storage. A domain infrastructure based on Active Directory, DNS and DHCP was configured, users and access groups were created, and a file server using SMB and delimitation of access rights using ACL was implemented in accordance with the principles of Zero Trust. To ensure data fault tolerance, RAID 1 was configured, and backup was organized using Windows Server Backup with copies saved on NAS-SERVER via network storage. Data backup is performed at a specified time in accordance with the configured backup process. Corporate Windows and Linux stations were also connected to the corporate network and

access to file resources was checked. To monitor the state of the infrastructure, the PRTG Network Monitor monitoring system was implemented, which provides monitoring of server availability, resource status, and network node operation parameters.

KEYWORDS: CORPORATE NETWORK, FILE STORAGE SYSTEM, NAS, ACTIVE DIRECTORY, ZERO TRUST, RAID 1, BACKUP.

ЗМІСТ

ВСТУП 10
РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ ТА ПІДХОДІВ ДО ЗАХИСТУ КОРПОРАТИВНИХ ФАЙЛОВИХ СХОВИЩ 12
1.1 Аналіз проблематики побудови безпечної корпоративної системи зберігання даних 12
1.2 Методи забезпечення безпеки корпоративного файлового сховища 13
1.3 Аналіз застосування NAS-технологій для створення корпоративного файлового сховища 23
1.4 Постановка технічного завдання дослідження 28
Висновок до першого розділу 30
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА МОДЕЛЮВАННЯ ЗАХИЩЕНОГО ФАЙЛОВОГО СХОВИЩА 32
2.1 Розробка архітектури корпоративної мережі 32
2.2 Розробка моделі файлового сховища 34
2.3 Проєктування моделі захищеного файлового сховища 38
2.3 Архітектура програмного забезпечення захищеного файлового сховища 41
Висновик до другого розділу 45
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАХИЩЕНОГО ФАЙЛОВОГО СХОВИЩА 48
3.1 Розгортання віртуальної інфраструктури корпоративної мережі 48
3.2 Налаштування доменної інфраструктури та мережних сервісів 52
3.3 Реалізація файлового сховища та політик доступу 60
3.4 Забезпечення відмовостійкості та резервного копіювання 75
3.5 Підключення корпоративних робочих станцій (Windows та Linux) та тестування системи 87
3.6 Моніторинг та аналіз роботи корпоративної інфраструктури 92
Висновок до третього розділу 97
ВИСНОВКИ 99
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 101

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD - Active Directory, служба каталогів для централізованого керування користувачами та ресурсами домену.

ACL - Access Control List, список контролю доступу до файлів і папок.

DC - Domain Controller, контролер домену.

DHCP - Dynamic Host Configuration Protocol, протокол автоматичного призначення мережних параметрів.

DNS - Domain Name System, система доменних імен.

FS - File Server, файловий сервер.

LTS - Long Term Support, версія програмного забезпечення з довгостроковою підтримкою.

NAS - Network Attached Storage, мережне сховище даних.

NTFS - New Technology File System, файлова система Windows.

PRTG - PRTG Network Monitor, система моніторингу мережної інфраструктури.

RAID - Redundant Array of Independent Disks, технологія підвищення надійності зберігання даних.

RBAC - Role-Based Access Control, модель контролю доступу на основі ролей.

SMB - Server Message Block, протокол спільного доступу до файлів.

VM - Virtual Machine, віртуальна машина.

WMI - Windows Management Instrumentation, технологія моніторингу та керування компонентами Windows.

OU - Organizational Unit, організаційний підрозділ Active Directory.

GPO - Group Policy Object, об’єкт групової політики.

SNMP - Simple Network Management Protocol, протокол моніторингу мережних пристроїв.

IP - Internet Protocol, протокол адресації в комп’ютерних мережах.

OS - Operating System, операційна система.

Zero Trust - концепція безпеки, що передбачає перевірку кожного користувача та кожного запиту на доступ.

ВСТУП

Актуальність теми. У сучасних умовах цифровізації діяльності підприємств та організацій особливого значення набуває забезпечення безпечного зберігання корпоративних даних. Корпоративні файлові сховища використовуються для централізованого зберігання документів, службової інформації та інших інформаційних ресурсів, доступ до яких повинні мати лише авторизовані користувачі. Водночас зростання кількості кіберзагроз, випадків несанкціонованого доступу, помилок користувачів та ризиків втрати даних внаслідок апаратних збоїв вимагає впровадження сучасних засобів захисту інформації.

Для забезпечення безпеки корпоративних даних застосовуються технології централізованого управління доступом на базі Active Directory, механізми розмежування прав доступу ACL, модель безпеки Zero Trust, засоби резервного копіювання та технології підвищення відмовостійкості систем зберігання даних. Важливим елементом також є моніторинг стану мережної інфраструктури, який дозволяє своєчасно виявляти та усувати потенційні проблеми.

У зв’язку з цим розробка захищеного корпоративного файлового сховища з використанням сучасних технологій зберігання даних, контролю доступу, резервного копіювання та моніторингу є актуальним завданням.

Метою кваліфікаційної роботи є розробка проєкту захищеного корпоративного файлового сховища з використанням технологій NAS для забезпечення безпечного зберігання корпоративних даних, централізованого управління доступом, відмовостійкості, резервного копіювання та моніторингу мережної інфраструктури.

Для досягнення поставленої мети було поставлено та вирішено такі завдання:

- проаналізувати сучасні методи та технології побудови захищених корпоративних файлових сховищ і дослідити засоби забезпечення інформаційної безпек;

- розробити модель і архітектуру захищеного корпоративного файлового сховища з урахуванням вимог щодо контролю доступу, відмовостійкості та резервного копіювання;
- виконати практичну реалізацію, налаштування та тестування розробленої системи у віртуальному середовищі корпоративної мережі.

Об’єктом дослідження є процеси зберігання, обробки та захисту інформації в мережній інфраструктурі організації.

Предметом дослідження є методи та засоби побудови захищених корпоративних файлових сховищ, технології NAS, RAID 1, механізми контролю доступу ACL, модель безпеки Zero Trust, засоби резервного копіювання та моніторингу мережної інфраструктури.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеного корпоративного файлового сховища на базі Windows Server із використанням Active Directory, SMB, технологій NAS, RAID 1, Windows Server Backup та системи моніторингу PRTG Network Monitor. Реалізоване рішення забезпечує централізоване управління доступом до корпоративних ресурсів, підвищення відмовостійкості зберігання даних, резервне копіювання та контроль стану мережної інфраструктури.

Практичне значення отриманих результатів полягає у можливості використання розробленого проєкту як основи для створення захищених корпоративних файлових сховищ у невеликих та середніх організаціях, де необхідно забезпечити безпечне зберігання даних, централізоване управління доступом, резервне копіювання та моніторинг інформаційної інфраструктури.

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ ТА ПІДХОДІВ ДО ЗАХИСТУ КОРПОРАТИВНИХ ФАЙЛОВИХ СХОВИЩ

1.1 Аналіз проблематики побудови безпечної корпоративної системи зберігання даних

Корпоративні інформаційні системи відіграють важливу роль у забезпеченні ефективної діяльності сучасних підприємств, установ та організацій. Значна частина корпоративної інформації зберігається в електронному вигляді та потребує надійних механізмів захисту від несанкціонованого доступу, втрати або пошкодження даних [1]. Зі збільшенням обсягів цифрової інформації та зростанням кількості кіберзагроз особливої актуальності набуває питання побудови безпечних корпоративних систем зберігання даних.

Сучасні файлові сервери є важливими елементами корпоративної інфраструктури, оскільки забезпечують централізоване зберігання та спільний доступ до документів і службової інформації. Разом із цим вони залишаються одними з основних об’єктів атак з боку зловмисників. Несанкціонований доступ до файлових ресурсів може призвести до витоку конфіденційної інформації, порушення роботи організації та значних фінансових втрат [2].

Однією з ключових проблем є організація ефективного контролю доступу до інформаційних ресурсів. Неправильно налаштовані права доступу можуть надавати користувачам надмірні привілеї та створювати передумови для внутрішніх загроз. Для централізованого керування користувачами, групами та ресурсами широко застосовується служба Active Directory, а для деталізованого розмежування доступу використовуються списки контролю доступу ACL (Access Control Lists) [3].

Додатковим напрямом підвищення рівня безпеки є використання концепції Zero Trust, відповідно до якої жоден користувач або пристрій не вважається довіреним за замовчуванням. Кожен запит на доступ повинен проходити перевірку незалежно від місця розташування користувача чи пристрою. Такий підхід

дозволяє зменшити ризики несанкціонованого доступу до корпоративних ресурсів [4].

Окрім забезпечення безпеки, важливим завданням є підтримання доступності та цілісності даних. Вихід з ладу жорстких дисків, програмні збої або помилки користувачів можуть призвести до втрати важливої інформації. Для підвищення відмовостійкості систем зберігання застосовуються RAID-масиви, зокрема RAID 1, який забезпечує дзеркальне копіювання даних між двома накопичувачами та дозволяє зберегти працездатність системи навіть у разі відмови одного з дисків [5].

Додатковим рівнем захисту є резервне копіювання даних на окремі мережні сховища. Використання NAS-серверів дозволяє створювати резервні копії критично важливої інформації та забезпечувати її відновлення у випадку аварійних ситуацій, випадкового видалення файлів або впливу шкідливого програмного забезпечення.

Для забезпечення стабільної роботи корпоративної інфраструктури також необхідно здійснювати постійний моніторинг серверів та мережних ресурсів. Системи моніторингу дозволяють контролювати доступність вузлів мережі, навантаження на процесор, використання оперативної пам’яті та дискового простору, що сприяє своєчасному виявленню потенційних проблем та запобіганню відмовам у роботі сервісів [5].

Таким чином, побудова безпечної корпоративної системи зберігання даних потребує комплексного підходу, який поєднує механізми контролю доступу, забезпечення відмовостійкості, резервного копіювання та моніторингу інфраструктури. Для реалізації таких рішень доцільно використовувати сучасні технології Active Directory, ACL, Zero Trust, RAID 1, NAS та системи моніторингу мережних ресурсів.

1.2 Методи забезпечення безпеки корпоративного файлового сховища

Для забезпечення безпеки корпоративного файлового сховища необхідно застосовувати комплексний підхід, який охоплює механізми контролю доступу,

забезпечення надійності зберігання даних, резервного копіювання та моніторингу інформаційної інфраструктури. Використання сучасних технологій дозволяє мінімізувати ризики несанкціонованого доступу, втрати інформації та порушення працездатності корпоративної мережі [6].

Одним із ключових напрямів забезпечення безпеки є контроль доступу до інформаційних ресурсів. Для цього використовуються різні моделі управління доступом, серед яких найбільш поширеними є DAC (Discretionary Access Control), RBAC (Role-Based Access Control) та концепція Zero Trust [7].

Дискреційна модель управління доступом (DAC, Discretionary Access Control) є однією з найстаріших і найпоширеніших моделей для забезпечення інформаційної безпеки. Її основний принцип полягає в тому, що власник ресурсу самостійно визначає права доступу інших користувачів до цього ресурсу. Цей підхід дозволяє власнику мати повноваження на створення, зміни та видалення дозволів для окремих облікових записів або груп користувачів.

Зазвичай реалізація DAC здійснюється через списки контролю доступу (ACL), які містять перелік користувачів та відповідних дозволених дій над об’єктами. Такі дії можуть включати читання, запис, виконання, модифікацію або видалення файлів і каталогів. У файлових системах Windows механізм ACL інтегрований у NTFS, що забезпечує можливість гнучкого налаштування прав доступу на рівні окремих файлів і папок.

Перевагою дискреційної моделі є її висока гнучкість: власники інформаційних ресурсів можуть швидко змінювати дозволи відповідно до потреб організації без залучення системних адміністраторів. Це особливо важливо для малих підприємств з обмеженою кількістю користувачів і ресурсів.

Ще одним плюсом DAC є простота впровадження та зрозумілість адміністрування. Більшість сучасних операційних систем вже містять вбудовані засоби для реалізації цієї моделі, що дозволяє використовувати її без додаткового програмного забезпечення.

Проте дискреційне управління доступом має значні недоліки. Основною проблемою є те, що безпека системи залежить від дій власника ресурсу.

Неправильне надання прав доступу або низький рівень обізнаності користувача можуть призвести до несанкціонованого розповсюдження інформації. Велику складність становить також адміністрування великої кількості індивідуальних дозволів у великих корпоративних мережах.

Іншою проблемою DAC є ризик неконтрольованого розповсюдження привілеїв між користувачами. Оскільки власник об’єкта може делегувати доступ іншим особам, це може призвести до втрати контролю над конфіденційною інформацією. Тому сучасні корпоративні системи все частіше поєднують DAC із централізованими механізмами управління доступом.

Рольова модель управління доступом (RBAC, Role-Based Access Control) передбачає, що дозволи призначаються не конкретним користувачам, а визначеним ролям, які відповідають функціональним обов’язкам співробітників організації [28]. Користувач отримує доступ до ресурсів через включення до певної ролі, і всі права автоматично успадковуються.

Основна концепція RBAC полягає у розділенні користувачів та їх дозволів за допомогою проміжного рівня ролей. Наприклад, в корпоративній мережі можуть бути такі ролі як «Адміністратор», «Працівник відділу кадрів», «Бухгалтер», «Керівник підрозділу» або «Звичайний користувач». Кожній з цих ролей заздалегідь надаються необхідні права доступу до інформаційних ресурсів.

Впровадження ролей значно полегшує адміністрування інформаційної системи. При прийомі нового працівника достатньо додати його до відповідної групи, після чого він автоматично отримує потрібний набір дозволів. У разі зміни посадових обов’язків достатньо перевести користувача в іншу роль без потреби вручну налаштовувати доступ до кожного окремого ресурсу.

Важливою перевагою RBAC є реалізація принципу мінімальних привілеїв (Least Privilege Principle). Це означає, що кожен працівник отримує лише ті права, які необхідні для виконання його службових завдань. Такий підхід суттєво знижує ризик випадкового чи навмисного пошкодження інформації.

Крім того, рольова модель добре масштабується і є придатною для організацій з великою кількістю користувачів. Централізоване управління ролями

зменшує адміністративне навантаження та забезпечує єдину політику безпеки у всій мережевій інфраструктурі.

Проте RBAC має свої обмеження. Однією з головних проблем є явище «вибуху ролей» (Role Explosion), яке виникає при збільшенні кількості підрозділів та функціональних обов'язків і потребує створення великої кількості спеціалізованих ролей. Це ускладнює адміністрування та може призводити до дублювання прав доступу.

Ще одним недоліком є недостатня гнучкість у ситуаціях, коли доступ до інформації залежить від додаткових факторів, таких як місцезнаходження користувача, час доби, тип пристрою або поточний рівень ризику. У таких випадках виникає потреба впроваджувати більш сучасні концепції інформаційної безпеки.

У рамках даного проекту рольова модель реалізується за допомогою Active Directory через використання груп безпеки. Для різних категорій працівників створено окремі групи з призначеними правами доступу до відповідних мережевих ресурсів. Цей підхід забезпечує централізоване управління дозволами та спрощує адміністрування корпоративної файлової інфраструктури.

Концепція Zero Trust (нульової довіри) є одним із найсучасніших підходів до забезпечення інформаційної безпеки та базується на принципі «ніколи не довіряй, завжди перевіряй» (Never Trust, Always Verify) [10]. На відміну від традиційних моделей, які передбачають високий рівень довіри до користувачів усередині корпоративної мережі, Zero Trust розглядає будь-який запит на доступ як потенційно небезпечний і вимагає його додаткової перевірки.

Основною ідеєю цієї концепції є відмова від поділу мережі на безпечний внутрішній та небезпечний зовнішній сегменти. Усі користувачі, пристрої та програмні компоненти проходять процедури автентифікації та авторизації незалежно від їхнього місцезнаходження.

Архітектура Zero Trust ґрунтується на кількох ключових принципах. Першим із них є принцип мінімальних привілеїв, відповідно до якого користувач отримує лише той рівень доступу, який необхідний для виконання його поточних завдань. Другим принципом є постійна перевірка особи користувача та стану пристрою

перед наданням доступу до ресурсів. Третім принципом виступає мікросегментація мережі, яка дозволяє обмежити поширення потенційних атак усередині інфраструктури.

Суттєвою перевагою Zero Trust є ефективний захист від внутрішніх загроз. Навіть якщо обліковий запис користувача буде скомпрометований, зловмисник не отримає автоматичного доступу до всієї корпоративної мережі, оскільки кожен наступний запит потребуватиме додаткової перевірки.

Додатковою перевагою є підвищення контролю над інформаційними потоками та можливість централізованого моніторингу всіх операцій доступу до ресурсів. Це дозволяє своєчасно виявляти аномальну активність та оперативно реагувати на потенційні інциденти інформаційної безпеки.

Разом із тим впровадження концепції Zero Trust потребує значних організаційних та технічних ресурсів. Необхідно забезпечити централізовану систему автентифікації, механізми багатофакторної перевірки, засоби моніторингу мережевої активності та ефективне управління політиками доступу. Крім того, впровадження такої архітектури може супроводжуватися збільшенням навантаження на адміністраторів і потребує високого рівня автоматизації процесів.

У межах даного проєкту принципи Zero Trust реалізуються через використання Active Directory, рольового розподілу прав доступу та механізмів ACL. Кожний користувач отримує лише необхідний набір дозволів, а доступ до корпоративних ресурсів здійснюється виключно після успішної автентифікації та перевірки членства у відповідних групах безпеки.

Проведений аналіз показує, що DAC забезпечує гнучке управління окремими ресурсами, RBAC дозволяє ефективно адмініструвати великі організації завдяки централізації ролей, а концепція Zero Trust підвищує рівень захисту шляхом постійної перевірки всіх суб’єктів доступу. Для побудови захищеного корпоративного файлового сховища доцільним є комбіноване використання RBAC, ACL та принципів Zero Trust, оскільки саме таке поєднання забезпечує баланс між гнучкістю адміністрування, масштабованістю системи та високим рівнем інформаційної безпеки.

Важливим елементом захисту корпоративних даних є забезпечення відмовостійкості системи зберігання. Для цього використовуються технології RAID (Redundant Array of Independent Disks), які дозволяють об'єднати декілька фізичних накопичувачів у єдину систему зберігання даних [11].

У даному проєкті використовується RAID 1, який реалізує принцип дзеркалювання даних. Усі дані одночасно записуються на два диски, що дозволяє зберегти працездатність файлового сховища навіть у разі виходу з ладу одного з накопичувачів. RAID 1 характеризується високою надійністю, простотою реалізації та швидким відновленням після апаратних збоїв [12].

Для обґрунтування вибору RAID 1 доцільно порівняти його характеристики з RAID 5, який також широко використовується у корпоративних системах зберігання даних [13][38].

Таблиця 1.1

Порівняльна характеристика RAID 1 та RAID 5

Характеристика	**RAID 1 (Mirror)**	**RAID 5 (Parity)**
Мінімальна кількість дисків	2	3
Принцип роботи	Повне дублювання даних на кожному диску	Чергування даних з використанням парності
Відмовостійкість	Витримує відмову одного диска	Витримує відмову одного диска
Швидкість читання	Висока завдяки можливості паралельного зчитування даних із дзеркальних дисків	Висока завдяки розподілу даних між декількома дисками
Швидкість запису	Висока, оскільки запис виконується одночасно на два диски без додаткових обчислень	Середня, оскільки під час запису необхідно обчислювати та записувати інформацію парності

Продовження таблиці 1.1

Характеристика	RAID 1 (Mirror)	RAID 5 (Parity)
Використання дискового простору	50% від загального обсягу	(N−1)/N від загального обсягу
Складність реалізації	Низька (налаштування передбачає створення дзеркальної копії між двома дисками без додаткових обчислень)	Середня (потребує налаштування парності та використання щонайменше трьох дисків)
Швидкість відновлення	Висока (відновлення виконується шляхом копіювання даних із працездатного дзеркального диска)	Нижча, особливо при великих обсягах даних (необхідне відновлення інформації на основі даних та блоків парності з усіх дисків масиву)
Ризик втрати даних під час відновлення	Низький (дані повністю зберігаються на другому диску та залишаються доступними після відмови одного накопичувача)	Вищий (у процесі відновлення значно зростає навантаження на всі диски масиву, що підвищує ризик відмови ще одного диска та втрати даних)
Доцільність використання	Критично важливі дані та невеликі сервери	Великі сховища з потребою економії дискового простору

Поряд із застосуванням RAID-масивів важливим є резервне копіювання даних. RAID не може замінити резервне копіювання, оскільки не забезпечує захист від випадкового видалення файлів, помилок користувачів, шкідливого програмного забезпечення або логічних пошкоджень. Тому в сучасних корпоративних інформаційних системах механізми резервування дисків та резервного копіювання використовуються разом і взаємодоповнюють один одного.

Існує кілька основних рівнів RAID, кожен з яких має свої переваги та недоліки. RAID 0 пропонує високу продуктивність завдяки розподілу даних між кількома накопичувачами, але не забезпечує жодної надійності: збій будь-якого диска призводить до втрати всієї інформації. З цієї причини використання RAID 0

є недоцільним для корпоративних файлових сховищ, де пріоритетом є надійність зберігання даних.

RAID 1 реалізує технологію дзеркалювання (mirroring), що дозволяє одночасно записувати інформацію на два фізичних накопичувачі. Якщо один з дисків виходить з ладу, система продовжує працювати без втрати даних, використовуючи його копію. Перевагами RAID 1 є висока надійність, простота налаштування, швидке відновлення після відмови та відсутність складних обчислень паритету. Основний недолік полягає в тому, що лише 50% загального дискового простору використовується через повне дублювання інформації.

RAID 5 використовує механізм чергування даних з розподіленим паритетом і вимагає щонайменше трьох накопичувачів. Цей підхід дозволяє більш ефективно використовувати дисковий простір та допускає вихід одного диска без втрати інформації. Однак процес відновлення після збою є тривалим і може створювати значне навантаження на систему. Крім того, під час реконструкції масиву ризик втрати даних підвищується у разі виходу ще одного накопичувача з ладу.

RAID 6 є вдосконаленою версією RAID 5 і передбачає використання подвійного паритету, що дозволяє системі залишатися працездатною навіть при одночасному виході з ладу двох дисків. Проте для реалізації цього підходу потрібно щонайменше чотири накопичувачі, а також спостерігається зниження швидкості запису через додаткові обчислення паритетної інформації.

RAID 10 поєднує принципи RAID 1 і RAID 0, забезпечуючи як високу продуктивність, так і відмовостійкість. Для його впровадження необхідно принаймні чотири диски; при цьому ефективний обсяг сховища становить лише половину сумарної місткості накопичувачів. Це робить його доцільним переважно для великих високонавантажених корпоративних систем.

Порівняльний аналіз різних рівнів RAID свідчить про те, що найдоцільнішим вибором для реалізації даного проєкту є RAID 1 через кілька факторів: по-перше, проєкт виконується у віртуалізованому середовищі й не потребує надвисокої продуктивності; по-друге, основним пріоритетом є забезпечення надійності та збереження корпоративних даних замість максимального використання дискового

простору; по-третє, RAID 1 характеризується легкістю адміністрування та швидким відновленням після збою одного накопичувача—це особливо важливо для невеликих корпоративних інфраструктур.

Отже, впровадження RAID 1 у поєднанні із системою резервного копіювання на віддалений NAS-сервер дозволяє досягти якості відмовостійкості файлового сховища так і можливості відновлення даних у випадку логічних помилок або дій шкідливого програмного забезпечення чи випадкового видалення інформації. Комплексне застосування цих механізмів формує необхідний рівень надійності та інформаційної безпеки для корпоративної системи зберігання даних.

Для додаткового захисту інформації застосовуються механізми резервного копіювання, які дозволяють відновити дані в разі їх втрати, пошкодження або несанкціонованого видалення. Резервні копії зберігаються на окремих пристроях або у мережевих сховищах NAS (Network Attached Storage), що гарантує фізичне відділення резервних даних від основної файлової структури.

Сучасні системи резервного копіювання пропонують кілька ключових методів: повне, інкрементне та диференційне резервування. Повне резервування передбачає створення копії всіх даних, що спрощує процес відновлення, але вимагає значної кількості дискового простору та часу. Інкрементне резервування фіксує лише ті файли, які були змінені з моменту останнього резервування, що допомагає зменшити витрати ресурсів, проте ускладнює процедуру відновлення. Диференційне резервування займає проміжну позицію між двома зазначеними підходами, оскільки зберігає всі зміни після останньої повної копії та забезпечує швидше відновлення за умов дещо більших витрат дискового простору.

У рамках реалізації системи резервування було розглянуто кілька програмних рішень, серед яких Windows Server Backup, IBM Storage Protect та вбудовані механізми NAS-систем. IBM Storage Protect має високу масштабованість і розширені можливості централізованого управління резервними копіями; однак його адміністрування є складнішим і він більше підходить для великих корпоративних середовищ. Засоби резервування NAS забезпечують просту

інтеграцію зі сховищами даних, проте їх функціональність значною мірою залежить від виробника обладнання.

В рамках цього проекту обрано Windows Server Backup через його інтеграцію в операційну систему Windows Server. Цей інструмент підтримує автоматичне створення повних і інкрементних резервних копій без потреби у додатковому програмному забезпеченні та легко взаємодіє з мережевими ресурсами через протокол SMB. Використання цього рішення сприяє спрощенню адміністрування системи, скороченню витрат на впровадження та забезпеченню належного рівня надійності для корпоративного файлового сховища середнього масштабу.

Резервні копії планується зберігати на окремому NAS-сервері для фізичного розділення їх від основного файлового сервера. Такий підхід підвищує стійкість системи до апаратних збоїв, помилок користувачів і шкідливого ПЗ та дозволяє швидко відновити працездатність інформаційної інфраструктури після аварійних ситуацій.[14]

Не менш важливим компонентом безпечної корпоративної інфраструктури є система моніторингу. Моніторинг забезпечує постійний контроль стану серверів, мережних пристроїв та сервісів, дозволяючи своєчасно виявляти несправності або аномальну активність [15].

У даному проєкті для моніторингу використовується система PRTG Network Monitor, яка забезпечує контроль доступності мережних вузлів, навантаження на процесор, використання оперативної пам’яті, стану дискової підсистеми та інших параметрів функціонування інфраструктури. Використання систем моніторингу дозволяє скоротити час реагування на інциденти та підвищити загальну надійність корпоративної мережі [5].

Додатковою вимогою до сучасних корпоративних файлових сховищ є забезпечення кросплатформеного доступу. Для взаємодії між корпоративними станціями під керуванням різних операційних систем широко використовується протокол SMB (Server Message Block), який забезпечує спільний доступ до файлів, папок та мережних ресурсів [16].

Таким чином, забезпечення безпеки корпоративного файлового сховища потребує комплексного використання технологій контролю доступу, моделей RBAC і Zero Trust, механізмів відмовостійкості RAID 1, резервного копіювання на NAS-сховище, систем моніторингу PRTG Network Monitor та протоколу SMB для організації безпечного доступу до ресурсів корпоративної мережі.

1.3 Аналіз застосування NAS-технологій для створення корпоративного файлового сховища

Сучасні корпоративні інформаційні системи потребують надійних засобів централізованого зберігання даних, які забезпечують безпечний доступ користувачів до інформаційних ресурсів, підтримують резервне копіювання та дозволяють швидко відновлювати працездатність системи після збоїв. Одним із найбільш поширених рішень для організації таких систем є технологія NAS (Network Attached Storage), яка широко застосовується як у невеликих організаціях, так і у великих корпоративних середовищах.

NAS (Network Attached Storage) являє собою спеціалізований мережевий пристрій або сервер, призначений для централізованого зберігання та спільного використання файлів через локальну мережу. На відміну від традиційних файлових серверів, NAS-системи оптимізовані саме для роботи з файловими операціями та забезпечують високу доступність даних, підтримку резервування й зручні механізми адміністрування.

Основною перевагою NAS є можливість відокремлення функцій зберігання даних від інших сервісів корпоративної інфраструктури. Це дозволяє знизити навантаження на основні сервери, підвищити рівень відмовостійкості системи та забезпечити додатковий рівень захисту резервних копій. У корпоративному середовищі NAS найчастіше використовується для організації централізованого сховища документів, архівів, мультимедійних матеріалів та резервних копій критично важливих даних.

Функціонування NAS базується на використанні стандартних мережевих протоколів доступу до файлів, серед яких найбільш поширеними є SMB/CIFS для середовищ Windows, NFS для Linux та Unix-систем, а також FTP і WebDAV для віддаленого доступу. У рамках даної роботи основним механізмом взаємодії між файловим сервером та резервним сховищем обрано протокол SMB, який забезпечує повну сумісність із доменною інфраструктурою Windows Server та підтримує сучасні механізми автентифікації і шифрування переданих даних.

Залежно від способу реалізації корпоративні файлові сховища можуть будуватися на основі трьох основних підходів:

- використання окремих апаратних NAS-пристроїв;
- розгортання програмного NAS-сервера на базі серверної операційної системи;
- застосування хмарних файлових сховищ.

Таблиця 1.2

Порівняння підходів до організації корпоративних файлових сховищ

Критерій	**Апаратний NAS (Synology/QNAP)**	**Програмний NAS (Windows Server + SMB)**	**Хмарне файлове сховище**
Початкові витрати	20 000-60 000 грн за пристрій без дисків	Використовується наявний сервер або віртуальна машина	Відсутні, оплата за підпискою
Вартість зберігання 1 ТБ	Одноразова після придбання дисків	Одноразова після придбання дисків	120-300 грн/міс. за 1 ТБ
Максимальний обсяг зберігання	20-200 ТБ залежно від кількості відсіків	Обмежується можливостями ОС та обладнання (до сотень ТБ)	Практично необмежений

Продовження таблиці 1.2

Критерій	**Апаратний NAS (Synology/QNAP)**	**Програмний NAS (Windows Server + SMB)**	**Хмарне файлове сховище**
Інтеграція з Active Directory	Підтримується через LDAP/AD	Повна нативна інтеграція	Залежить від провайдера та тарифу
Підтримка SMB	SMBv2/v3	SMBv1/v2/v3	Переважно через шлюзи або синхронізаційні клієнти
Налаштування ACL	Обмежене інтерфейсом виробника	Повна підтримка NTFS ACL	Власні механізми доступу провайдера
Підтримка RAID	RAID 0, 1, 5, 6, 10	Windows Storage Spaces, RAID 1	Не використовується користувачем
Залежність від Інтернету	Не потребує	Не потребує	Постійне підключення є обов’язковим
Швидкість доступу в локальній мережі	1-10 Гбіт/с	1-10 Гбіт/с	Обмежується каналом Інтернет
Резервне копіювання	Вбудовані засоби виробника	Windows Server Backup, Veeam, Acronis	Засоби провайдера
Рівень адміністрування	Через веб-інтерфейс	Через Windows Server Manager, PowerShell, GPO	Через веб-панель провайдера

Продовження таблиці 1.2

Критерій	**Апаратний NAS (Synology/QNAP)**	**Програмний NAS (Windows Server + SMB)**	**Хмарне файлове сховище**
Контроль над даними	Повний фізичний контроль	Повний фізичний контроль	Дані розміщуються у стороннього постачальника
Відповідність моделі проєкту	Часткова	Повна	Часткова

Аналіз показує, що апаратні NAS-системи забезпечують високу надійність і простоту адміністрування, однак потребують значних фінансових витрат на придбання спеціалізованого обладнання. Хмарні файлові сервіси характеризуються практично необмеженою масштабованістю та мінімальними початковими витратами, проте створюють залежність від зовнішнього провайдера й постійного доступу до мережі Інтернет.

Найбільш доцільним для реалізації даного проєкту є використання програмного NAS на базі Windows Server. Такий підхід забезпечує повну інтеграцію зі службами Active Directory, підтримку NTFS ACL, використання протоколу SMB, можливість реалізації RAID 1 та застосування вбудованих засобів резервного копіювання. Крім того, програмний NAS легко розгортається у віртуалізованому середовищі Oracle VM VirtualBox, що відповідає вимогам даної кваліфікаційної роботи та дозволяє моделювати реальну корпоративну інфраструктуру без додаткових витрат на фізичне обладнання.

Для мінімізації зазначених ризиків рекомендується застосовувати комплекс заходів захисту, серед яких:

- використання централізованої автентифікації через Active Directory;

- впровадження принципу найменших привілеїв;
- налаштування списків контролю доступу (ACL);
- застосування RAID-масивів для підвищення відмовостійкості;
- регулярне створення резервних копій;
- ведення журналів аудиту та моніторинг подій безпеки;
- сегментація мережі та ізоляція резервного сховища від основних сервісів.

Особливо важливим є питання вибору механізму резервування даних. У корпоративних середовищах поширені три основні підходи: локальне резервне копіювання, резервування на віддалений NAS-сервер та хмарне резервне копіювання. Їх порівняння наведене у таблиці 1.3.

Таблиця 1.3

Порівняння способів резервного копіювання корпоративних даних

Спосіб резервування	**Основні переваги**	**Основні недоліки**
Локальне резервування на тому самому сервері	Час відновлення 5-10 хв; відсутність додаткових мережевих ресурсів	Не забезпечує захист від фізичного пошкодження обладнання та шкідливого ПЗ
Резервування на NAS-сервер	Фізичне відокремлення копій; підтримка автоматизованого резервування через SMB	Потребує виділеного сервера та додаткового адміністрування
Хмарне резервування	Географічне рознесення даних; практично необмежений обсяг зберігання	Залежність від Інтернет-з'єднання та політик стороннього постачальника послуг

Проведене порівняння демонструє, що окремий NAS-сервер є найбільш оптимальним рішенням для створення безпечного корпоративного файлового

сховища. На відміну від локального резервування, цей метод забезпечує фізичне ізолювання резервних копій від головного файлового сервера. У порівнянні з хмарними сервісами, він також дозволяє повністю контролювати розміщення та обробку корпоративних даних.

У рамках цього проєкту NAS-сервер слугуватиме як окреме резервне сховище, де будуть зберігатися резервні копії даних, створені за допомогою Windows Server Backup. Така архітектура надає додатковий рівень стійкості до відмов, дозволяючи швидко відновлювати інформацію після збоїв і відповідаючи сучасним вимогам інформаційної безпеки корпоративних систем.

Таким чином, результати аналізу підтверджують доцільність впровадження NAS-технологій у процесі створення корпоративних файлових сховищ. Порівняння різних підходів показало, що програмна реалізація NAS на базі серверної операційної системи забезпечує найкраще співвідношення між функціональністю, вартістю та рівнем захисту. Відтак, у подальшій роботі для організації резервного копіювання й відновлення інформації буде використано окремий NAS-сервер, інтегрований у корпоративну мережеву інфраструктуру.

1.4 Постановка технічного завдання дослідження

На основі аналізу сучасних підходів до побудови корпоративних інформаційних систем визначено теоретичну мету дослідження - розробку моделі захищеного корпоративного файлового сховища [17]. Дане завдання передбачає формування IT-інфраструктури, яка забезпечує надійне зберігання даних, централізоване управління доступом та стійкість до внутрішніх і зовнішніх загроз.

Метою роботи є створення комплексного рішення захищеного корпоративного файлового сховища, що відповідає сучасним вимогам інформаційної безпеки, надійності та керованості. Реалізація проєкту охоплює як побудову серверної інфраструктури, так і впровадження технологічних механізмів захисту, резервування та моніторингу даних [18].

Система повинна забезпечувати захист від несанкціонованого доступу шляхом централізованої автентифікації, багаторівневого розмежування прав доступу та застосування політик безпеки. Використання підходу Zero Trust передбачає перевірку кожного запиту незалежно від місцезнаходження користувача та мінімізацію наданих прав доступу [10].

Важливою складовою є забезпечення відмовостійкості, яка гарантує збереження даних у разі апаратних або програмних збоїв. Для цього застосовується технологія RAID 1, що базується на дзеркалюванні даних між фізичними накопичувачами та дозволяє продовжувати роботу системи при виході з ладу одного з дисків [19].

Окрему роль відіграє резервне копіювання даних, яке реалізується із використанням віддаленого мережного сховища NAS. Такий підхід дозволяє зберігати резервні копії поза межами основного сервера та забезпечує можливість відновлення інформації у випадку критичних збоїв або втрати даних.

Також передбачається впровадження системи моніторингу та аудиту стану інфраструктури, що дозволяє здійснювати контроль доступності серверів, навантаження на ресурси та своєчасне виявлення інцидентів безпеки. Це підвищує загальний рівень керованості та стабільності системи [20].

Додатково система повинна забезпечувати кросплатформений доступ до файлового сховища для пристроїв із різними операційними системами, зокрема Windows та Linux, із використанням мережного протоколу SMB [21].

Об’єктом дослідження є корпоративна мережа як середовище функціонування інформаційних ресурсів організації, що включає серверну інфраструктуру, робочі станції та мережні сервіси.Предметом дослідження є захищене корпоративне файлове сховище та методи забезпечення його безпеки, включаючи контроль доступу, відмовостійкість, резервне копіювання та моніторинг.

Отже, сформульоване технічне завдання визначає ключові напрямки дослідження та створює основу для подальшого проєктування та реалізації системи захищеного корпоративного файлового сховища.

Висновок до першого розділу

У результаті аналізу встановлено, що питання захисту корпоративних файлових сховищ є багатокомпонентною задачею, яка охоплює контроль доступу, забезпечення відмовостійкості, резервне копіювання та моніторинг інфраструктури. Виявлено, що традиційні підходи до організації файлових систем не забезпечують достатнього рівня захисту в умовах сучасних кіберзагроз, зокрема через відсутність централізованого управління та обмежених механізмів контролю доступу.

Під час аналізу технологій контролю доступу розглянуто моделі DAC, RBAC та Zero Trust. Встановлено, що модель DAC є простою у реалізації, однак має обмеження в масштабованих корпоративних середовищах через складність керування великою кількістю дозволів. Модель RBAC забезпечує більш структурований підхід за рахунок використання ролей, проте потребує чіткої попередньої організації структури користувачів. Найбільш ефективною для даного проєкту визначено концепцію Zero Trust, яка забезпечує перевірку кожного запиту на доступ та реалізацію принципу мінімальних привілеїв.

При аналізі технологій забезпечення надійності зберігання даних було розглянуто підходи RAID 1 та RAID 5. Встановлено, що RAID 1 забезпечує вищий рівень надійності за рахунок дзеркального копіювання даних і швидкого відновлення після відмови диска, однак має меншу ефективність використання дискового простору. RAID 5, у свою чергу, більш ефективний за обсягом використання пам’яті, але характеризується складнішою реалізацією та повільнішим процесом відновлення даних. З огляду на вимоги до надійності та простоти реалізації для даного проєкту обрано RAID 1.

Також розглянуто підходи до резервного копіювання даних. Встановлено, що використання локальних копій на тому ж сервері є недостатньо надійним, тоді як застосування віддаленого NAS-сховища значно підвищує рівень захисту інформації та дозволяє відновити дані у випадку повної відмови основного сервера.

Окремо проаналізовано системи моніторингу інфраструктури. Виявлено, що використання спеціалізованих рішень, таких як PRTG Network Monitor, є більш ефективним порівняно з ручним контролем або стандартними системними засобами, оскільки забезпечує централізований збір даних про стан серверів, навантаження ресурсів та доступність сервісів у режимі наближеному до реального часу.

Таким чином, у ході аналізу визначено оптимальний набір технологій для побудови захищеного корпоративного файлового сховища: Zero Trust для контролю доступу, RAID 1 для забезпечення відмовостійкості, NAS для резервного копіювання та PRTG для моніторингу. Отримані результати формують теоретичну основу для подальшого проєктування та практичної реалізації системи у наступних розділах роботи.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА МОДЕЛЮВАННЯ ЗАХИЩЕНОГО ФАЙЛОВОГО СХОВИЩА

2.1 Розробка архітектури корпоративної мережі

Розробка захищеного корпоративного файлового сховища потребує побудови цілісної мережної інфраструктури, яка забезпечує централізоване керування користувачами, надійне зберігання даних, резервне копіювання та контроль стану системи. Для реалізації поставлених завдань було розроблено архітектуру корпоративної мережі, яка включає серверні та корпоративні компоненти, об'єднані в єдине інформаційне середовище [17]. Загальну структуру розробленої корпоративної мережі наведено на рисунку 2.1.

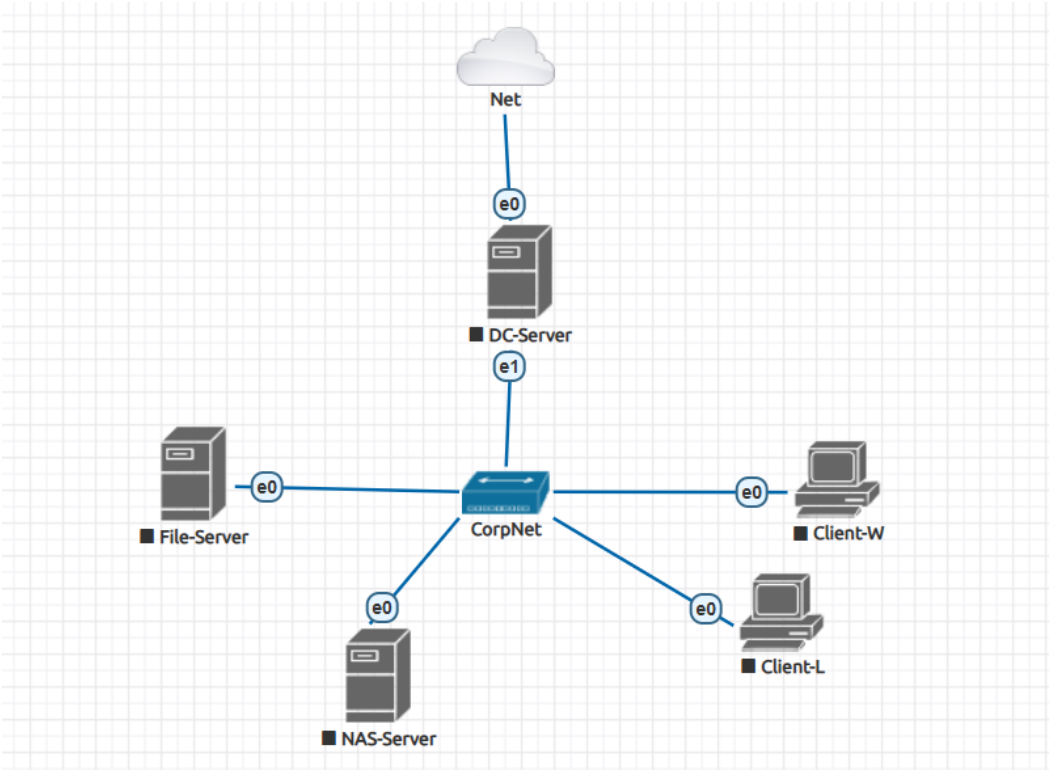


Рисунок 2.1 - Загальна модель корпоративної мережі

Основою архітектури є контролер домену DC-SERVER, який виконує функції централізованого управління користувачами та мережними ресурсами. На сервері розгорнуто служби Active Directory Domain Services, DNS та DHCP, що забезпечують автентифікацію користувачів, централізоване керування обліковими записами, автоматичне призначення мережних параметрів та перетворення

доменних імен у IP-адреси [22]. Використання доменної інфраструктури дозволяє реалізувати єдину систему доступу до ресурсів корпоративної мережі та спрощує адміністрування всієї інфраструктури.

Центральним елементом системи зберігання даних є файловий сервер FILE-SERVER. На ньому розміщуються корпоративні файлові ресурси, до яких користувачі отримують доступ відповідно до призначених прав. Для організації спільного доступу використовується протокол SMB, який підтримується операційними системами Windows та Linux. Контроль доступу до файлів і каталогів реалізується за допомогою списків контролю доступу ACL, що дозволяє детально визначати права окремих користувачів та груп на виконання операцій читання, запису або зміни даних.

Для підвищення надійності зберігання інформації на файловому сервері реалізовано програмний RAID 1. Даний механізм забезпечує дзеркальне копіювання інформації між двома фізичними накопичувачами, що дозволяє зберегти працездатність системи у разі відмови одного з дисків [19]. Використання RAID 1 є доцільним для корпоративного файлового сховища, оскільки забезпечує високий рівень відмовостійкості та не потребує складних процедур відновлення даних.

Додатковий рівень захисту інформації забезпечується NAS-SERVER, який використовується як окреме мережне сховище для резервного копіювання даних. На даний сервер передаються резервні копії корпоративних ресурсів, створені за допомогою Windows Server Backup. Фізичне відокремлення NAS-SERVER від файлового сервера дозволяє зберегти резервні копії навіть у випадку виходу з ладу основного сервера або пошкодження його даних.

Доступ до корпоративних ресурсів здійснюється з корпоративних робочих станцій Client-W та Client-L. Для перевірки кросплатформеності рішення використовуються операційні системи Windows 10 та Ubuntu Linux. Після успішної автентифікації в домені користувачі отримують доступ до файлових ресурсів відповідно до своїх ролей і груп безпеки. Такий підхід відповідає принципам централізованого управління доступом та концепції Zero Trust, відповідно до якої

кожний запит на доступ перевіряється незалежно від місця розташування користувача.

Мережна інфраструктура побудована з використанням двох логічних сегментів. Внутрішній сегмент CorpNet використовується для взаємодії між серверними компонентами та корпоративними станціями, а сегмент NAT забезпечує контрольований доступ до зовнішніх мережних ресурсів та мережі Інтернет. Такий підхід дозволяє ізолювати критично важливі ресурси корпоративної мережі від зовнішнього середовища та зменшує ризик несанкціонованого доступу.

Взаємодія компонентів мережі відбувається за централізованою схемою. Користувач виконує вхід до домену через DC-SERVER, після чого отримує доступ до ресурсів FILE-SERVER відповідно до призначених прав доступу. Дані файлового сервера періодично резервуються на NAS-SERVER, а контроль стану всієї інфраструктури здійснюється системою моніторингу PRTG Network Monitor. Це дозволяє забезпечити безпечне зберігання даних, їх доступність для користувачів та своєчасне виявлення можливих проблем у роботі мережної інфраструктури.

Таким чином, розроблена архітектура корпоративної мережі об’єднує засоби централізованого управління доступом, надійного зберігання інформації, резервного копіювання та моніторингу в єдину систему. Запропонована структура є основою для подальшої практичної реалізації захищеного корпоративного файлового сховища.

2.2 Розробка моделі файлового сховища

У цьому підрозділі представлена розроблена модель корпоративного файлового сховища, що окреслює структуру зберігання даних, взаємозв'язок компонентів системи та механізми забезпечення безпеки інформаційних ресурсів. Модель файлового сховища створена з урахуванням вимог централізованого управління доступом, відмовостійкості, резервного копіювання та моніторингу стану інфраструктури. Основна мета моделі полягає в забезпеченні надійного

зберігання корпоративних даних із можливістю їх безпечного використання користувачами мережі відповідно до визначених прав доступу.

Центральним елементом файлового сховища є сервер FILE-SERVER, який виконує функції централізованого зберігання корпоративної інформації та надає спільний доступ до неї через мережу. Усі файлові ресурси консолідовані на одному сервері, що спрощує адміністрування, контроль доступу та резервне копіювання даних. Взаємодія користувачів із файловим сервером реалізується через доменну інфраструктуру Active Directory, налаштовану на контролері домену DC-SERVER.

Модель передбачає впровадження централізованої системи автентифікації та авторизації для користувачів. Кожен користувач отримує індивідуальний доменний обліковий запис для входу в корпоративну мережу і доступу до файлових ресурсів. Такий підхід дозволяє ефективно управляти користувачами, групами безпеки та політиками доступу, а також швидко блокувати або змінювати права доступу за необхідності.

Для реалізації моделі контролю доступу користувачів розподіляють за функціональними групами відповідно до їхніх службових обов'язків. Кожна група має доступ лише до певних ресурсів файлового сховища. Цей підхід відповідає принципам мінімальних привілей і концепції Zero Trust, згідно з якою жоден користувач або пристрій не отримує автоматичний доступ без перевірки його повноважень.

У межах розробленої моделі були створені облікові записи користувачів і групи безпеки, наведені в таблиці 2.1.

Таблиця 2.1

Облікові записи користувачів домену CORPNET.LOCAL

Користувач	**Група**	**Призначення**
Administrator	Domain Admins	Адміністрування доменної інфраструктури
i.petrenko	IT_Admins	Адміністратор інформаційної системи
o.koval	Employees	Користувач корпоративної мережі
a.melnyk	Employees	Користувач корпоративної мережі
m.shevchuk	Accounting	Працівник бухгалтерського відділу

Для організації зберігання корпоративних даних на файловому сервері були створені спеціалізовані мережні ресурси, що відповідають структурі підприємства. Це забезпечує категоризацію інформації та обмеження доступу лише для визначених груп користувачів.

Таблиця 2.2

Структура мережних ресурсів FILE-SERVER

Мережний ресурс	**Призначення**
IT_Admins	Зберігання адміністративних файлів та службової інформації
Employees	Зберігання робочих документів користувачів
Accounting	Зберігання фінансової та бухгалтерської документації

Доступ до ресурсів реалізовано за допомогою списків контролю доступу ACL. Для кожної групи користувачів визначено набір дозволених операцій із файлами та каталогами. Такий механізм дозволяє контролювати читання, запис, зміну або видалення інформації та мінімізує ризик несанкціонованого доступу до корпоративних даних.

Таблиця 2.3

Розподіл прав доступу ACL до файлових ресурсів

Файловий ресурс	**Група користувачів**	**Надані права доступу**
IT_Admins	IT_Admins	Full Control
Employees	Employees	Modify, Read, Write
Accounting	Accounting	Modify, Read

Особливістю розробленої моделі є здійснення багаторівневого захисту інформації. Перший рівень захисту реалізується через доменну автентифікацію користувачів. Другий рівень забезпечується за допомогою списків контролю доступу (ACL) та груп безпеки в Active Directory. Третій рівень складається з

механізмів, які гарантують цілісність і доступність даних, застосовуючи RAID 1 і резервне копіювання. Такий підхід сприяє зменшенню наслідків зовнішніх атак та внутрішніх помилок користувачів.

Для покращення надійності зберігання інформації у файловому сховищі впроваджена технологія RAID 1, що забезпечує дзеркальне копіювання даних між двома фізичними накопичувачами [23]. Якщо один диск виходить з ладу, всі дані залишаються доступними на іншому носії, що дозволяє уникнути простою системи та втрати інформації.

Додатковий рівень захисту досягається завдяки механізму резервного копіювання. Резервні копії формуються за допомогою Windows Server Backup і зберігаються на окремому мережному сховищі NAS-SERVER. Відокремлене місцезнаходження резервних копій дає змогу відновити дані навіть у разі серйозного пошкодження файлового сервера або втрати основного сховища.

Модель також передбачає підтримку корпоративних операційних систем Windows і Linux. Для організації спільного доступу до даних використовується мережний протокол SMB, який забезпечує кросплатформенну взаємодію між файловим сервером і корпоративними станціями [24]. Це дозволяє використовувати одне файлове сховище незалежно від типу операційної системи користувача.

Для моніторингу працездатності всіх компонентів файлового сховища реалізовано систему на базі PRTG Network Monitor [5]. Ця система забезпечує постійний збір інформації про стан серверів, мережних ресурсів та використання системних ресурсів.

Таблиця 2.4

Сенсори моніторингу у PRTG Network Monitor

Сенсор	**Призначення**
Ping	Контроль доступності мережного пристрою
CPU Load	Моніторинг завантаження процесора

Продовження таблиці 2.4

Memory	Контроль використання оперативної пам’яті
Disk Free	Контроль вільного місця на дисках

Таким чином, розроблена модель файлового сховища об’єднує механізми централізованого управління користувачами, контролю доступу, відмовостійкості, резервного копіювання та моніторингу інфраструктури. Використання Active Directory, ACL, RAID 1, NAS-сховища та системи моніторингу PRTG дозволяє створити комплексне рішення для безпечного зберігання корпоративних даних, що відповідає сучасним вимогам інформаційної безпеки та забезпечує надійну роботу корпоративної мережі.

2.3 Проєктування моделі захищеного файлового сховища

На основі аналізу предметної області та розробленої моделі корпоративної мережі було спроєктовано захищене файлове сховище. Головна мета проєкту - створення централізованого середовища для зберігання корпоративних даних, що гарантує їх конфіденційність, цілісність, доступність та відмовостійкість.

Запропонована архітектура базується на доменній інфраструктурі Microsoft Active Directory, файловому сервері під керуванням Windows Server, мережному сховищі (NAS) для резервного копіювання та системі моніторингу PRTG Network Monitor. Взаємодія між усіма компонентами реалізована через внутрішню корпоративну мережу CorpNet.

Архітектура системи передбачає розподіл функцій між окремими серверами:

- DC-SERVER (Domain Controller) - виконує функції контролера домену в корпоративній мережі, виступаючи ключовим вузлом системи адміністрування. На сервері розгорнуто служби Active Directory Domain Services (AD DS), DNS та DHCP, що забезпечують централізовану автентифікацію й авторизацію користувачів, управління обліковими записами та групами безпеки, динамічне призначення мережних параметрів корпоративним пристроям, а також підтримку цілісності доменної інфраструктури. Впровадження Active Directory дає змогу

реалізувати єдину архітектуру управління доступом до ресурсів корпоративної мережі.

- FILE-SERVER (файловий сервер) забезпечує централізоване зберігання корпоративних даних, організацію спільного доступу до файлів і папок, а також керування правами користувачів. Для налаштування розмежування доступу до мережних ресурсів застосовуються списки контролю доступу (ACL), що базуються на принципах мінімальних привілеїв та концепції Zero Trust. Висока надійність зберігання даних гарантується використанням технології RAID 1, яка реалізує дзеркальне дублювання інформації на фізичних накопичувачах.

- NAS-SERVER (Network Attached Storage Server) - це окремий мережний пристрій, призначений для зберігання резервних копій важливих корпоративних даних та налаштувань серверів.

- Він забезпечує додатковий рівень захисту інформації завдяки фізичному розміщенню резервних копій окремо від основного файлового сховища.

- У випадку виникнення технічних несправностей, помилок з боку користувачів або кібератак, NAS-SERVER дає змогу відновити дані та гарантувати безперервність функціонування інформаційної системи.

- Корпоративні робочі станції Client-W та Client-L функціонують у корпоративній мережі під управлінням операційних систем Windows та Linux відповідно. Їхнє призначення - забезпечення доступу до ресурсів домену, мережних служб та системи зберігання файлів. Після успішної автентифікації користувачі отримують доступ виключно до тих ресурсів, які визначені їхніми ролями та наданими правами доступу. Застосування різноманітних операційних систем дозволяє оцінити міжплатформну сумісність розгорнутої інфраструктури, а також перевірити функціонування файлового сховища за допомогою протоколу SMB.

З метою забезпечення централізованого управління доступом в межах домену налаштовано облікові записи користувачів та групи безпеки за допомогою Active Directory, які наведені в таблиці 2.1.

Керування доступом до файлових ресурсів реалізовано шляхом використання груп безпеки та списків контролю доступу (ACL). Цей метод дає

змогу застосувати принцип мінімальних привілеїв, надаючи користувачам доступ виключно до тих ресурсів, які потрібні для виконання їхніх службових завдань, це наведено в таблиці 2.3.

На файловому сервері функціонує система управління доступом до спільних мережних ресурсів, яка забезпечує їх розподіл між групами користувачів відповідно до принципу найменших привілеїв. Для кожної визначеної категорії користувачів організовано окремі каталоги, для яких встановлено відповідні права доступу. Детальний список мережних ресурсів файлового сервера та їх функціональне призначення представлено у Таблиці 2.2.

Задля забезпечення надійності функціонування файлового сховища на сервері застосовується технологія RAID 1. Це реалізує дзеркальне дублювання інформації на два окремі фізичні накопичувачі, що дозволяє системі зберігати працездатність навіть у випадку виходу з ладу одного з них.

Додатковий рівень захисту інформації забезпечується системою резервного копіювання. Для цього використовується Windows Server Backup, а збереження резервних копій здійснюється на окремий NAS-сервер. Процес резервування даних виконується згідно з попередньо налаштованим графіком, що дає можливість відновити втрачену або пошкоджену інформацію.

Контроль за станом та працездатністю корпоративної інфраструктури здійснюється за допомогою системи PRTG Network Monitor.

Для забезпечення сумісності з різними операційними системами, доступ до файлових ресурсів реалізовано за допомогою протоколу SMB. Це дає змогу користувачам операційних систем Windows та Linux працювати з єдиним централізованим сховищем даних.

За підсумками розробки було створено концепцію захищеного сховища файлів, яка інтегрує механізми централізованого управління доступом, відмовостійкого зберігання інформації, резервного копіювання та контролю інфраструктури. Ця розроблена модель слугує базою для подальшої практичної імплементації системи та її конфігурації у віртуальному середовищі.

2.4 Архітектура програмного забезпечення захищеного файлового сховища

Для реалізації захищеного корпоративного файлового сховища була сформована програмна архітектура, яка забезпечує централізоване керування користувачами, надійне зберігання інформації, резервне копіювання та моніторинг стану інфраструктури. Архітектура побудована у віртуалізованому середовищі та складається з серверних компонентів, робочих станцій і допоміжних сервісів, взаємодія між якими забезпечує безперервне функціонування корпоративної мережі.

Таблиця 2.5

Основні програмні компоненти системи

Компонент	**Програмне забезпечення**	**Призначення**
Платформа віртуалізації	Oracle VM VirtualBox 7.1.4	Створення та керування віртуальним середовищем
Контролер домену	Windows Server 2022 + AD DS	Централізована автентифікація та керування користувачами
DNS-сервер	DNS Server	Перетворення доменних імен у мережеві адреси
DHCP-сервер	DHCP Server	Автоматичне призначення IP-адрес
FILE-SERVER	Windows Server 2022 + NTFS + SMB	Централізоване зберігання корпоративних даних
Система резервування	Windows Server Backup	Автоматичне створення резервних копій
NAS-SERVER	Windows Server (SMB Storage)	Зберігання резервних копій
Робоча станція Windows	Windows 10	Доступ до корпоративних ресурсів

Продовження таблиці 2.5

Робоча станція Linux	Ubuntu 24.04.1 LTS	Перевірка кросплатформеної взаємодії
Система моніторингу	PRTG Network Monitor	Контроль стану серверів і мережевих сервісів

Як платформу віртуалізації було обрано Oracle VM VirtualBox 7.1.4. Вона забезпечує створення та управління віртуальними машинами, необхідними для розгортання серверних і корпоративних компонентів. VirtualBox підтримує ключові мережні режими, дає змогу створювати ізольовані мережні сегменти та надає достатній рівень продуктивності для моделювання корпоративного середовища.

Основу серверної інфраструктури становить операційна система Windows Server 2022, яка застосовується для розміщення сервера управління доменом, сховища файлів та системи резервного копіювання. Вибір цієї ОС пояснюється її вбудованою підтримкою ключових мережних сервісів, таких як Active Directory Domain Services, DNS та DHCP, а також наявністю інтегрованих інструментів для адміністрування та забезпечення безпеки інформації.

Для створення доменної мережі використовується сервер DC-SERVER, на якому встановлені служби Active Directory, DNS та DHCP. Active Directory надає централізоване керування обліковими записами користувачів, групами та правилами безпеки, DNS відповідає за перетворення мережних імен, а DHCP автоматично налаштовує мережні параметри для корпоративних пристроїв.

Файловий сервер призначений для централізованого зберігання даних підприємства та забезпечення доступу до них згідно з встановленими правилами безпеки. В основі файлового сховища лежить файлова система NTFS, яка підтримує механізми розмежування доступу за допомогою списків ACL. Це дає змогу впровадити принцип мінімального рівня доступу, надаючи користувачам доступ виключно до тих ресурсів, що потрібні для виконання їхніх посадових обов'язків.

Для підвищення надійності зберігання інформації на цьому сервері використовується технологія RAID 1, яка забезпечує дублювання даних на двох фізичних дисках. Такий підхід дозволяє підтримувати працездатність системи навіть у випадку відмови одного накопичувача та істотно скорочує час на відновлення функціонування сховища.

Резервування даних здійснюється за допомогою програмного забезпечення Windows Server Backup, що забезпечує автоматизацію формування резервних копій згідно з визначеним графіком. Для зберігання архівних копій застосовується окремий NAS-пристрій, який функціонує як віддалене мережне сховище. Фізичне розділення резервних копій від основного файлового сервера гарантує покращений рівень захисту інформації та можливість її відновлення у випадку критичних подій або відмов.

В якості корпорвтивних операційних систем використовуються Windows 10 та Ubuntu 24.04.1 LTS. Наявність двох відмінних платформ дозволяє оцінити функціональність корпоративної мережі в умовах гетерогенного середовища та забезпечити доступ до файлових ресурсів як для користувачів Windows, так і Linux. Взаємодія корпоративних систем з файловим сервером здійснюється за протоколом SMB.

Для забезпечення належного функціонування інфраструктури застосовується система моніторингу PRTG Network Monitor. Вона надає можливість здійснювати консолідований збір відомостей про стан серверного обладнання, рівень завантаження процесора, обсяг використаної оперативної пам'яті, доступність мережних служб та обсяг вільного дискового простору. Окрім цього, задіюються системні журнали Windows (Event Viewer), які дозволяють проводити аудит дій користувачів та аналізувати події, пов'язані з інформаційною безпекою.

Логічну структуру корпоративної мережної інфраструктури, реалізованої у віртуальному середовищі Oracle VM VirtualBox, наведено на рисунку 2.2. Логічна схема взаємодії компонентів корпоративної мережі представлено на рисунку 2.3.

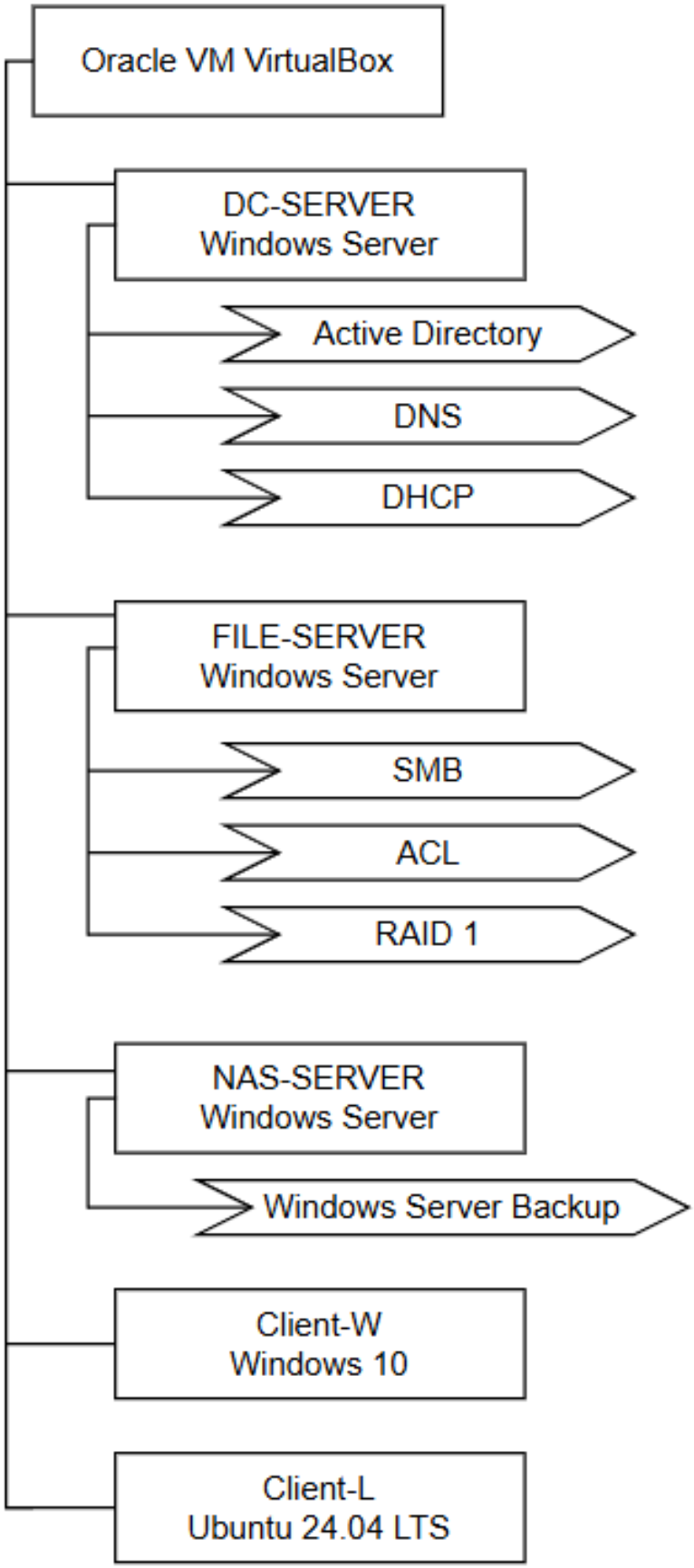


Рисунок 2.2 - Логічна структура корпоративної мережної інфраструктури

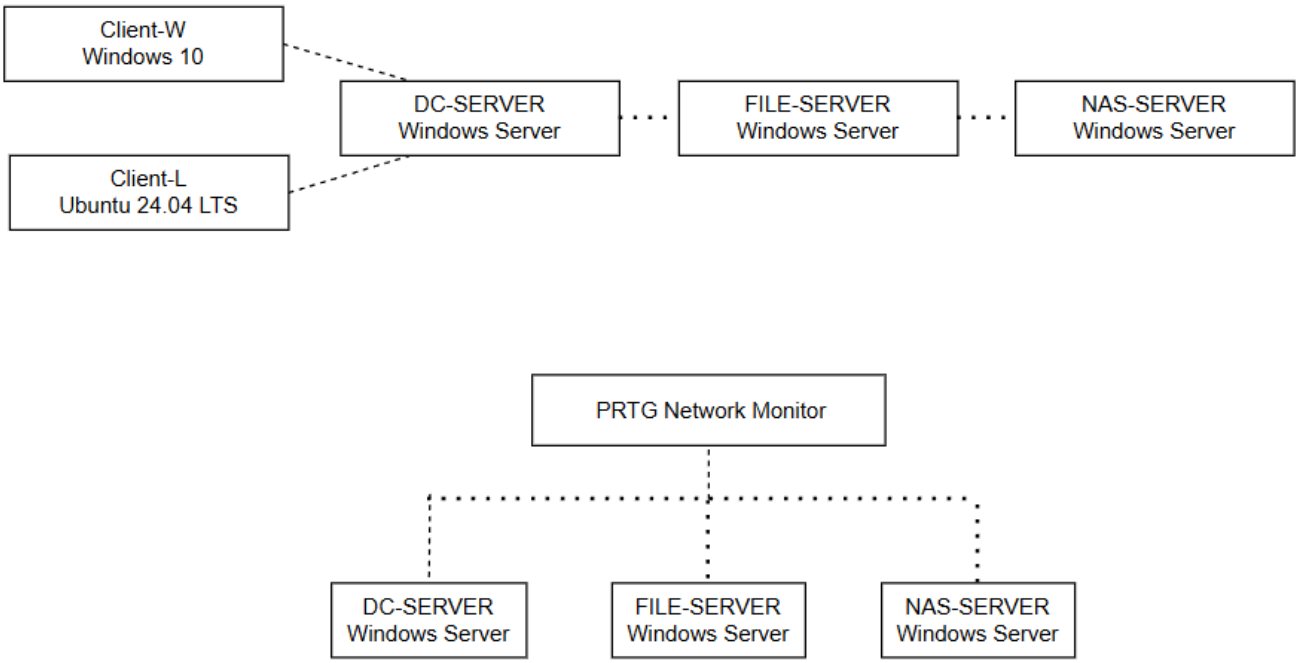


Рисунок 2.3 - Логічна схема взаємодії компонентів корпоративної мережі

Таким чином, обраний набір програмних рішень і технологій повною мірою задовольняє всі необхідні функції проєкту. Сюди входять такі аспекти, як централізоване керування доступом, безпечне зберігання корпоративних даних, можливість резервного копіювання, стійкість до збоїв та постійний контроль за станом IT-інфраструктури. Використання цих підходів дозволяє створити повноцінне та надійне корпоративне файлове сховище в умовах віртуального середовища.

Висновок до другого розділу

У другому розділі було розроблено архітектуру захищеного корпоративного файлового сховища та сформовано модель корпоративної мережі. Ця модель передбачає централізоване розміщення даних, контроль прав доступу, механізми резервного копіювання та інструменти моніторингу системної інфраструктури. Остаточна архітектура системи включає контролер домену (DC-SERVER), файловий сервер (FILE-SERVER), сервер для резервного копіювання (NAS-SERVER) та робочі станції користувачів, що функціонують під управлінням операційних систем Windows і Linux.

Під час проєктування було деталізовано принцип взаємодії між усіма складовими системи. З'ясовано, що застосування доменної служби Active Directory дає змогу централізовано контролювати облікові записи, групи безпеки та політики доступу, що спрощує управління корпоративною мережею та підвищує її безпеку. Для ефективного розмежування доступу до файлів були використані списки контролю доступу (ACL) та реалізовано принцип найменших привілеїв. Такий підхід відповідає концепції "нульової довіри" (Zero Trust) і суттєво зменшує ймовірність несанкціонованого отримання корпоративної інформації.

У контексті розробленої моделі захисту обґрунтовано вибір технології RAID 1 для гарантування відмовостійкості файлового сервера. Аналіз та порівняння RAID 1 з RAID 5 виявило, що хоча RAID 1 менш ефективно використовує дисковий простір, вимагаючи 50% обсягу для дзеркального копіювання даних, він вирізняється простішою імплементацією, швидшим відновленням після несправностей та зниженим ризиком втрати даних при відновленні масиву. Враховуючи критичну важливість забезпечення максимальної надійності корпоративного файлового сховища, RAID 1 було визнано оптимальним рішенням для цього проєкту.

Крім того, було створено модель резервного копіювання даних, що базується на NAS-SERVER та використовує функціонал Windows Server Backup. Цей підхід надає додатковий рівень захисту інформації, дозволяючи відновити дані навіть у випадку повної відмови файлового сервера або пошкодження основного сховища. Розміщення резервних копій на окремому носії підвищує загальну стійкість системи до апаратних несправностей та кіберзагроз.

При виборі програмного забезпечення та середовища для реалізації було встановлено, що Oracle VM VirtualBox дозволяє створити повноцінну корпоративну інфраструктуру у віртуальному просторі, усуваючи потребу у фізичному обладнанні. Для серверних компонентів було обрано Windows Server, який надає підтримку для Active Directory, DNS, DHCP, файлових сервісів та інструментів резервного копіювання. З метою перевірки кросплатформенності

системи, як корпоративну станцію додатково використано Ubuntu 24.04 LTS, яка успішно працює з файловими ресурсами через протокол SMB.

Для забезпечення контролю функціональності та своєчасного виявлення потенційних проблем було інтегровано систему моніторингу PRTG Network Monitor. Аналіз її можливостей показав, що вона дозволяє здійснювати централізований контроль за станом серверів, споживанням ресурсів процесора, оперативної пам'яті, дискового простору, а також доступністю мережних служб у реальному часі.

Таким чином, у підсумку цього розділу було сформовано комплексну архітектуру захищеного корпоративного файлового сховища, аргументовано вибір ключових технологій та розроблено модель їх практичного впровадження. Отримані результати стануть основою для подальшого розгортання, конфігурування та тестування системи у третьому розділі кваліфікаційної роботи.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАХИЩЕНОГО ФАЙЛОВОГО СХОВИЩА

3.1 Розгортання віртуальної інфраструктури корпоративної мережі

На початковому етапі практичної реалізації захищеного файлового сховища було створено віртуальне середовище корпоративної мережі. Для моделювання роботи інформаційної системи підприємства використано платформу віртуалізації Oracle VM VirtualBox, де розгорнуто серверні та корпоративні компоненти мережної інфраструктури, що ілюструється на рисунку 3.1

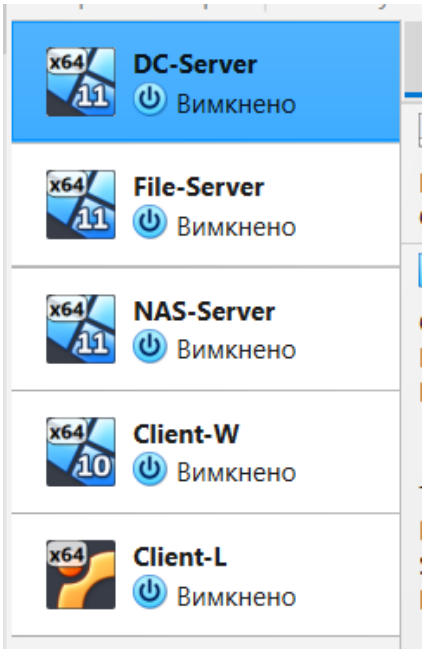


Рисунок 3.1 - Структура розгорнутої мережі в Oracle VM VirtualBox

У рамках тестового середовища було налаштовано кілька віртуальних машин, кожна з яких виконує специфічні функції у корпоративній інфраструктурі. Віртуальна машина DC-SERVER функціонує як контролер домену Active Directory, забезпечуючи централізоване управління користувачами, групами та політиками безпеки. Віртуальна машина File-SERVER виконує завдання файлового сервера, призначеного для зберігання корпоративних даних і організації спільного доступу через протокол SMB. Сервер NAS-SERVER служить віддаленим сховищем для резервного копіювання даних. Корпоративна машина Client-W являє собою робочу станцію на базі Windows, підключену до доменної мережі, тоді як Client-L

використовується як Client-L для перевірки кросплатформенного доступу до файлових ресурсів.

Для забезпечення взаємодії між усіма вузлами було створено ізольований мережний сегмент у VirtualBox типу Internal Network з назвою CorpNet. Використання внутрішньої мережі дозволило організувати обмін даними між віртуальними машинами без доступу до зовнішньої мережі, що моделює корпоративне локальне середовище. Налаштування параметрів внутрішньої мережі для кожного вузла відображено на рисунках 3.2-3.6.

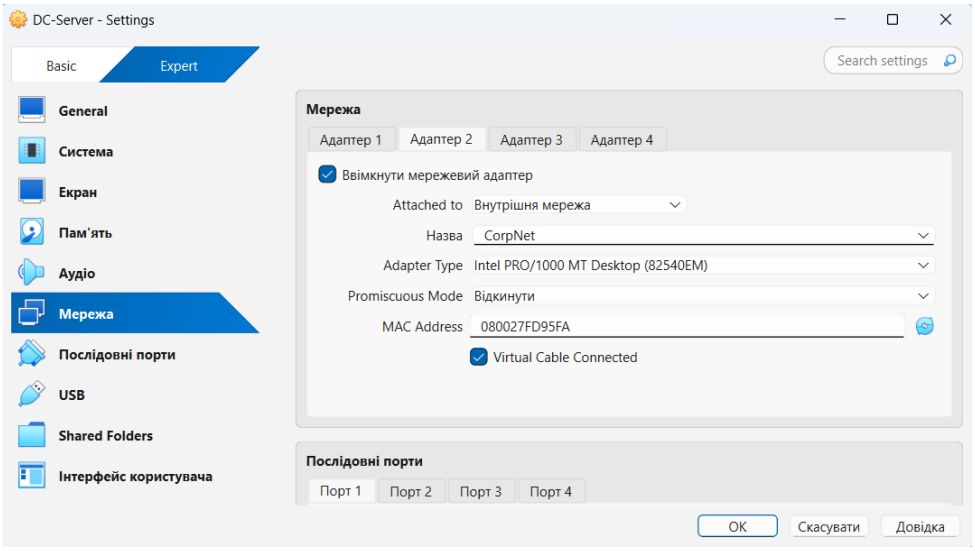


Рисунок 3.2 - Налаштування внутрішньої мережі CorpNet у середовищі VirtualBox для DC-Server

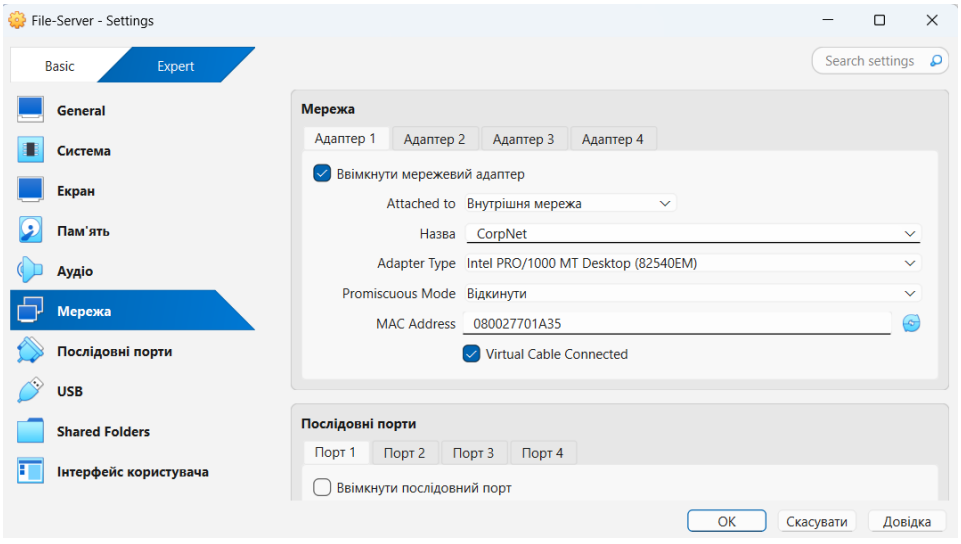


Рисунок 3.3 - Налаштування внутрішньої мережі CorpNet у середовищі VirtualBox для File-Server

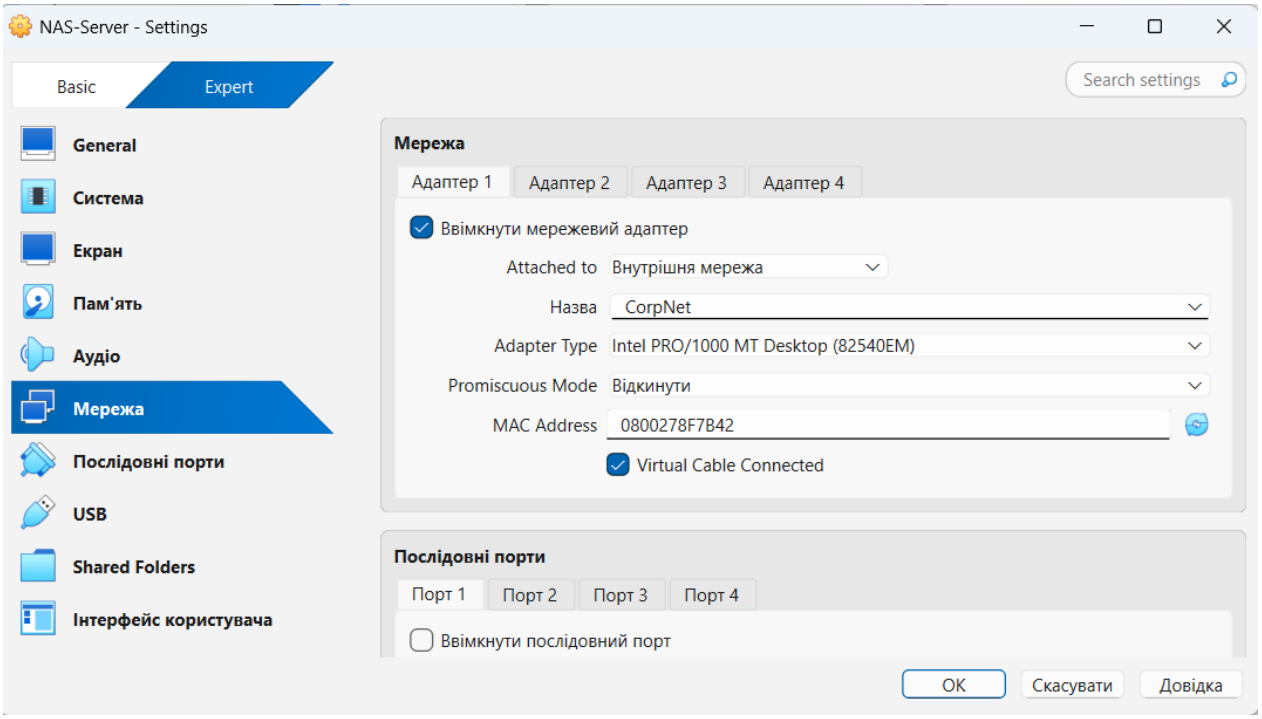


Рисунок 3.4 - Налаштування внутрішньої мережі CorpNet у середовищі VirtualBox для NAS-Server

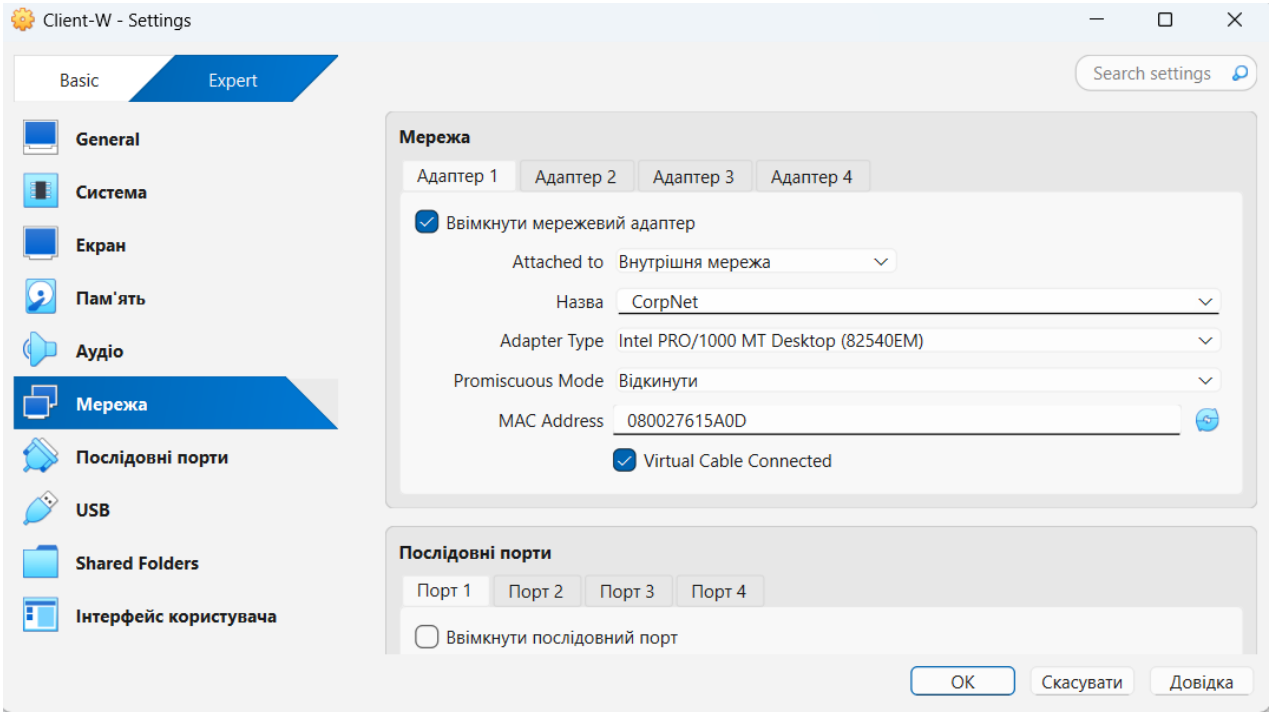


Рисунок 3.5 - Налаштування внутрішньої мережі CorpNet у середовищі VirtualBox для Client-W

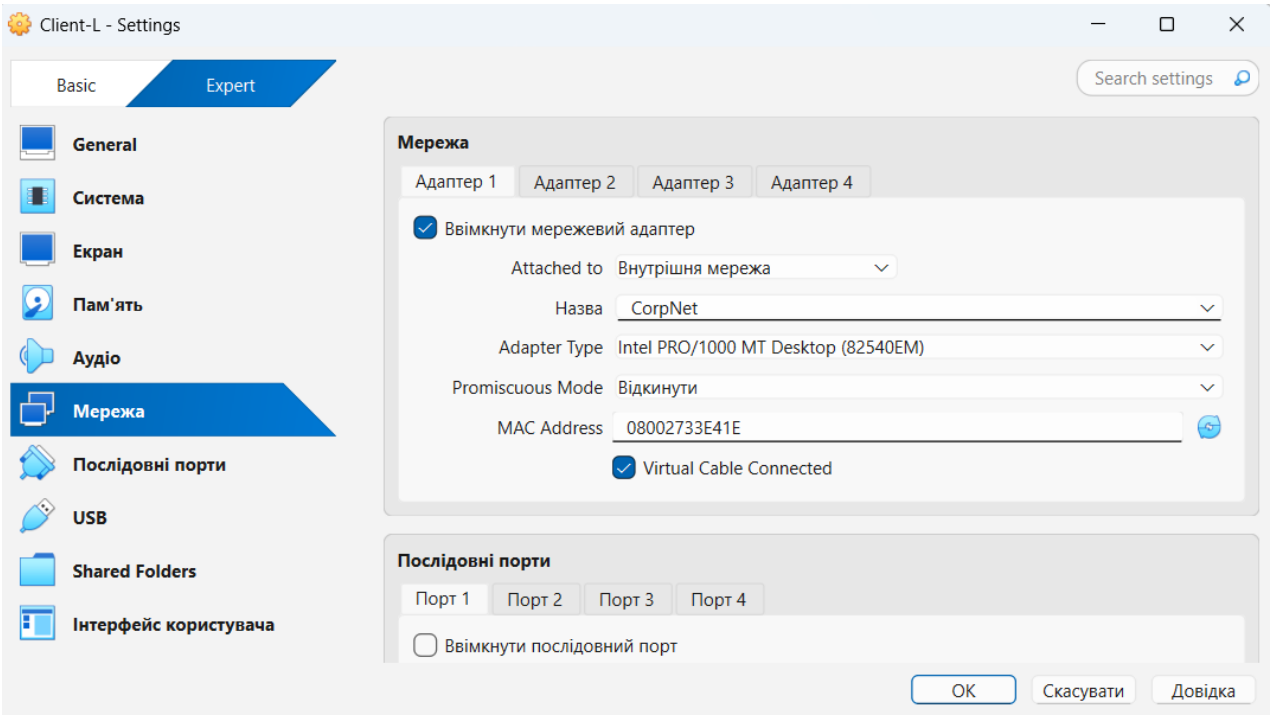


Рисунок 3.6 - Налаштування внутрішньої мережі CorpNet у середовищі VirtualBox для Client-L

Після налаштування мережного середовища була виконана конфігурація основної IP-адресації вузлів. Для корпоративної мережі обрано підмережу 192.168.10.0/24, що надає єдиний адресний простір для всіх компонентів системи.

Розподіл IP-адрес між вузлами представлено у таблиці 3.1. Така схема адресації дозволила створити структуроване та логічно організоване середовище для подальшої настройки служб автентифікації, файлового доступу та моніторингу.

Таблиця 3.1

Розподіл IP-адрес між вузлами

Пристрій	**IP-адреса**
DC-SERVER	192.168.10.1
FILE-SERVER	192.168.10.2
NAS-SERVER	192.168.10.3
Client-W	192.168.10.100
Client-L	192.168.10.101

3.2 Налаштування доменної інфраструктури та мережних сервісів

На сервері DC-SERVER було здійснено розгортання базової доменної інфраструктури корпоративної мережі. На початковому етапі були встановлені необхідні серверні ролі, зокрема Active Directory Domain Services (AD DS), DNS-сервер і DHCP-сервер, що забезпечують централізоване управління користувачами, мережними іменами та автоматичне призначення IP-адрес. Процес установки ролей та їх первісного налаштування ілюструється на рисунку 3.7 - Встановлення серверних ролей AD DS, DNS та DHCP.

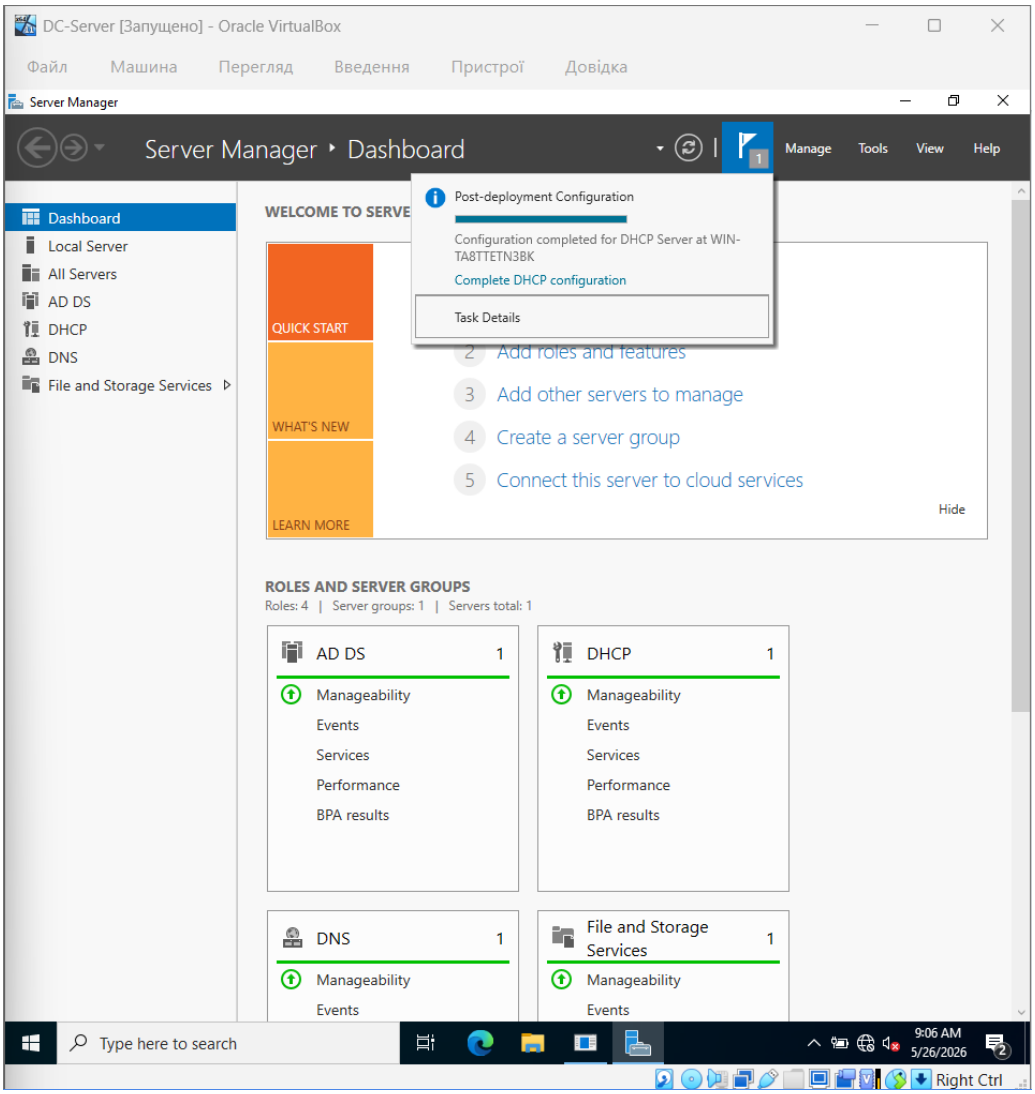


Рисунок.3.7 - Встановлення ролей AD DS, DNS та DHCP

Після активації ролі Active Directory сервер був підвищений до статусу контролера домену. В результаті цього було створено новий домен corpnet.local,

який використовується для централізованої автентифікації користувачів, управління комп'ютерами та регулювання прав доступу до корпоративних ресурсів.

Наступним кроком була настройка служби DHCP, яка відповідає за автоматичне надання мережних параметрів корпоративним пристроям. Створення та конфігурація DHCP-області (Scope) разом із параметрами розподілу адрес відображені на рисунку 3.8; додаткове налаштування параметрів - на рисунку 3.9. Результат роботи служби, що підтверджує успішне автоматичне отримання IP-адреси корпоративним комп'ютером Windows, представлений на рисунку 3.10 - Перевірка отримання IP-адреси через DHCP на Client-W.

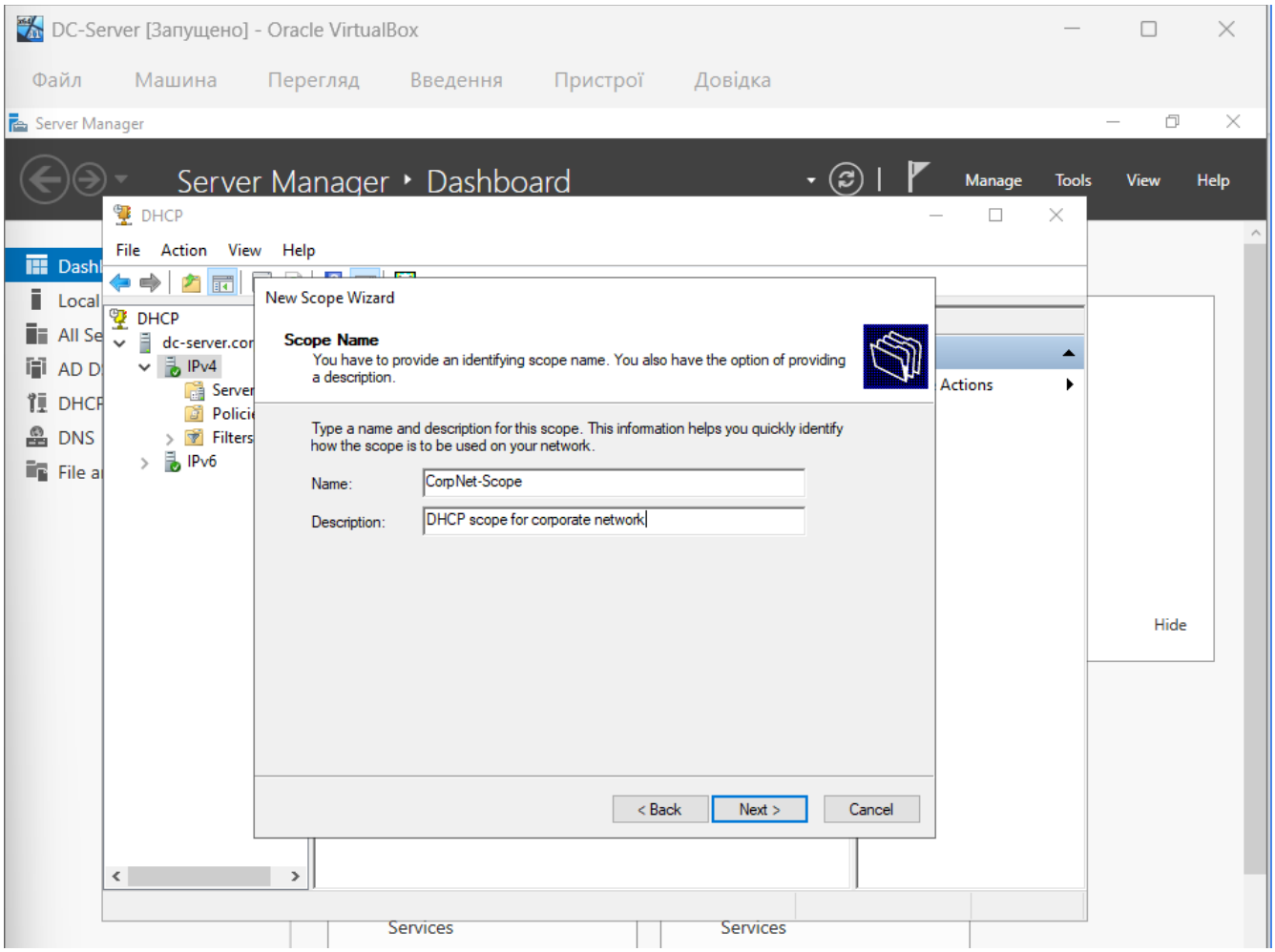


Рисунок 3.8 - Налаштування DHCP

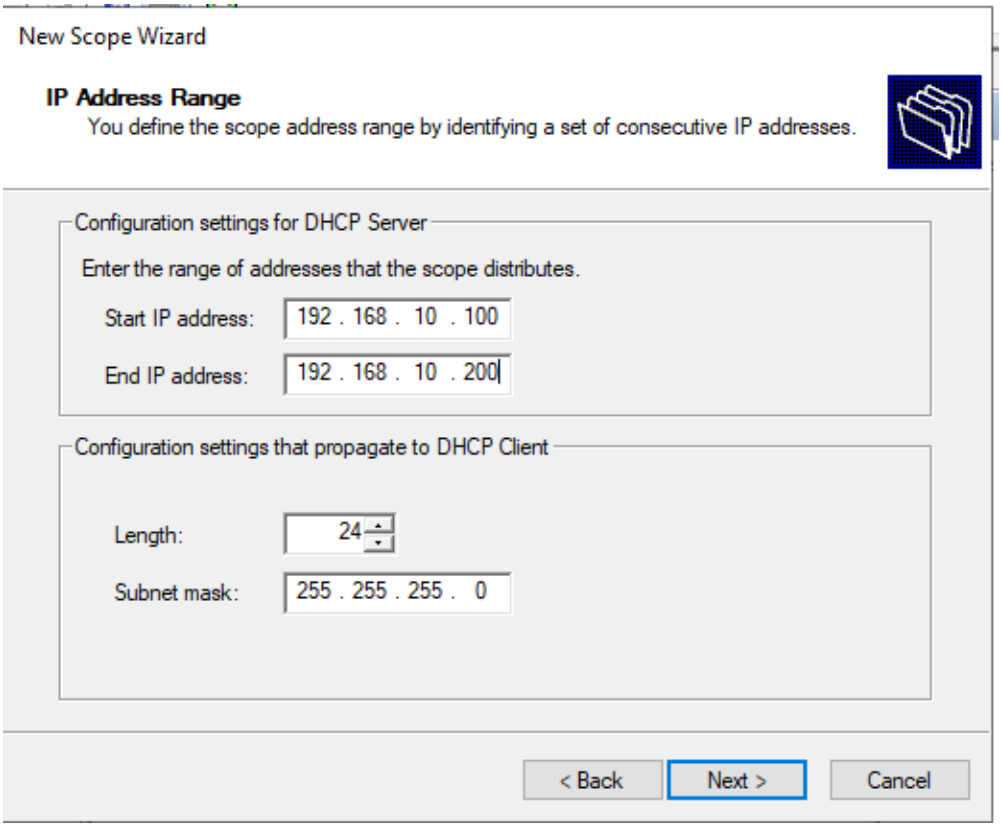


Рисунок 3.9 - Додаткові параметри DHCP-сервера

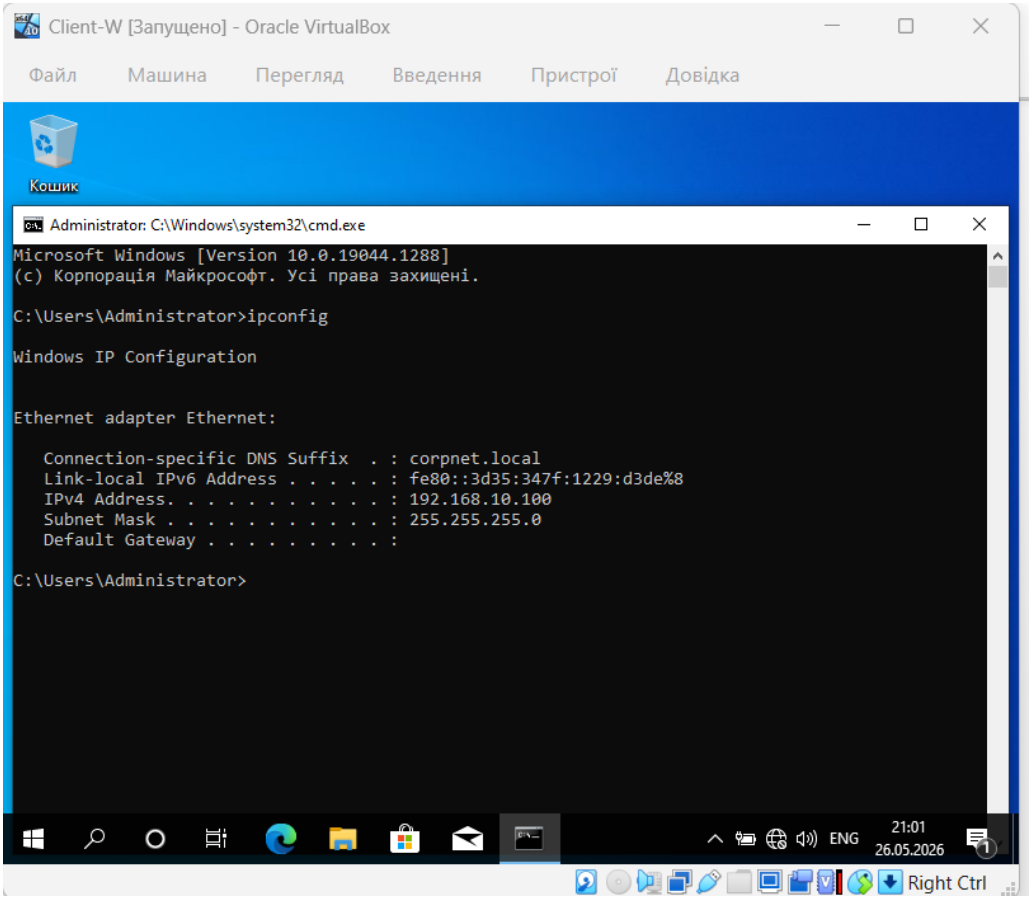


Рисунок 3.10 - Результат перевірки автоматичного отримання IP-адреси Windows Client через DHCP

Після налаштування мережних сервісів була створена структура Active Directory, включаючи організаційні одиниці (OU), групи безпеки та облікові записи користувачів. Процес створення OU для подальшої організації доменної структури показано на рисунку 3.11.

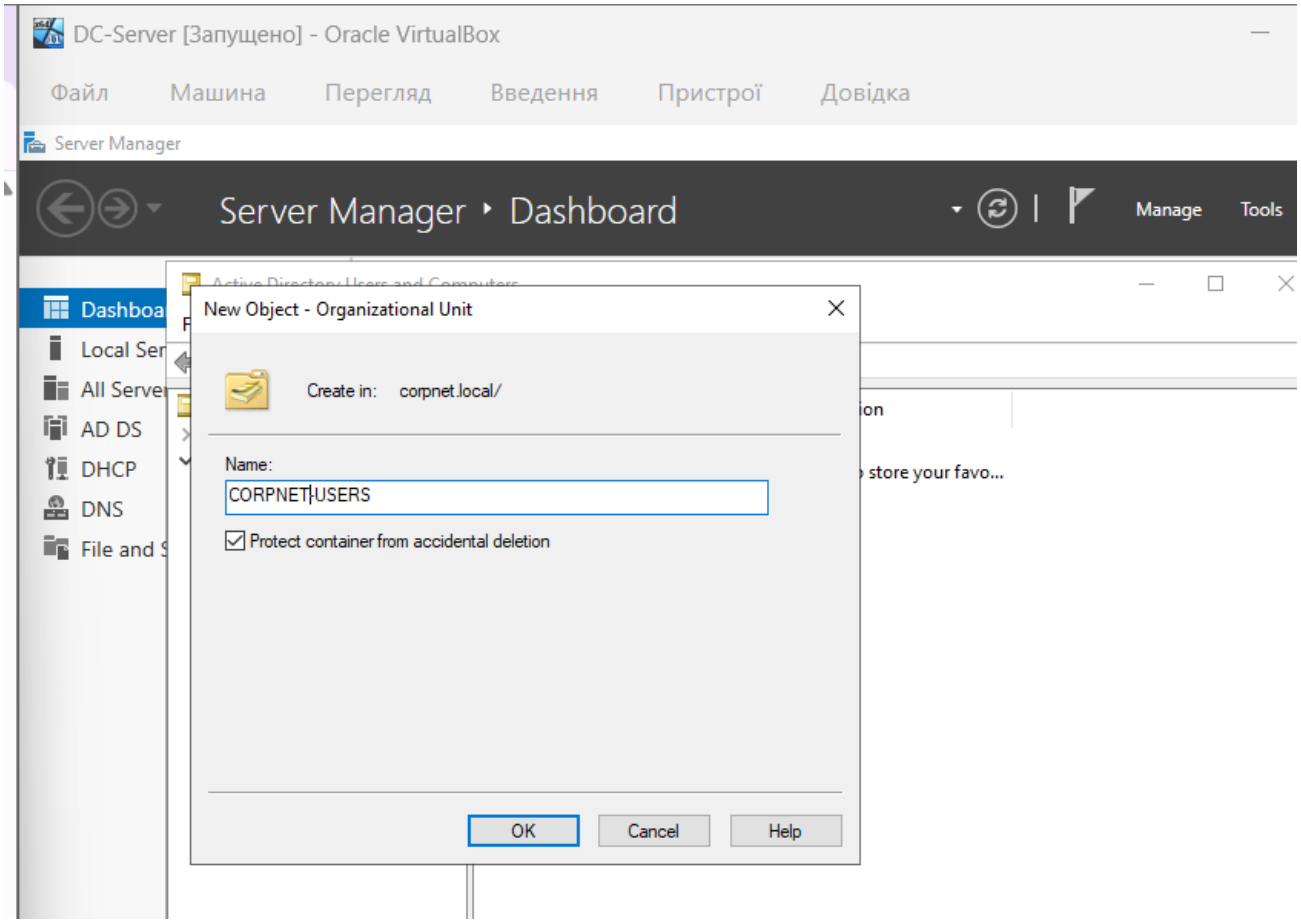


Рисунок 3.11 - Створення Organizational Unit (OU) у Active Directory

Для забезпечення розмежування доступу були сформовані групи безпеки відповідно до ролей користувачів. Цей процес продемонстровано на рисунку 3.12. Результати формування трьох основних груп (IT_Admins, Employees, Accounting) наведені на рисунку 3.13.

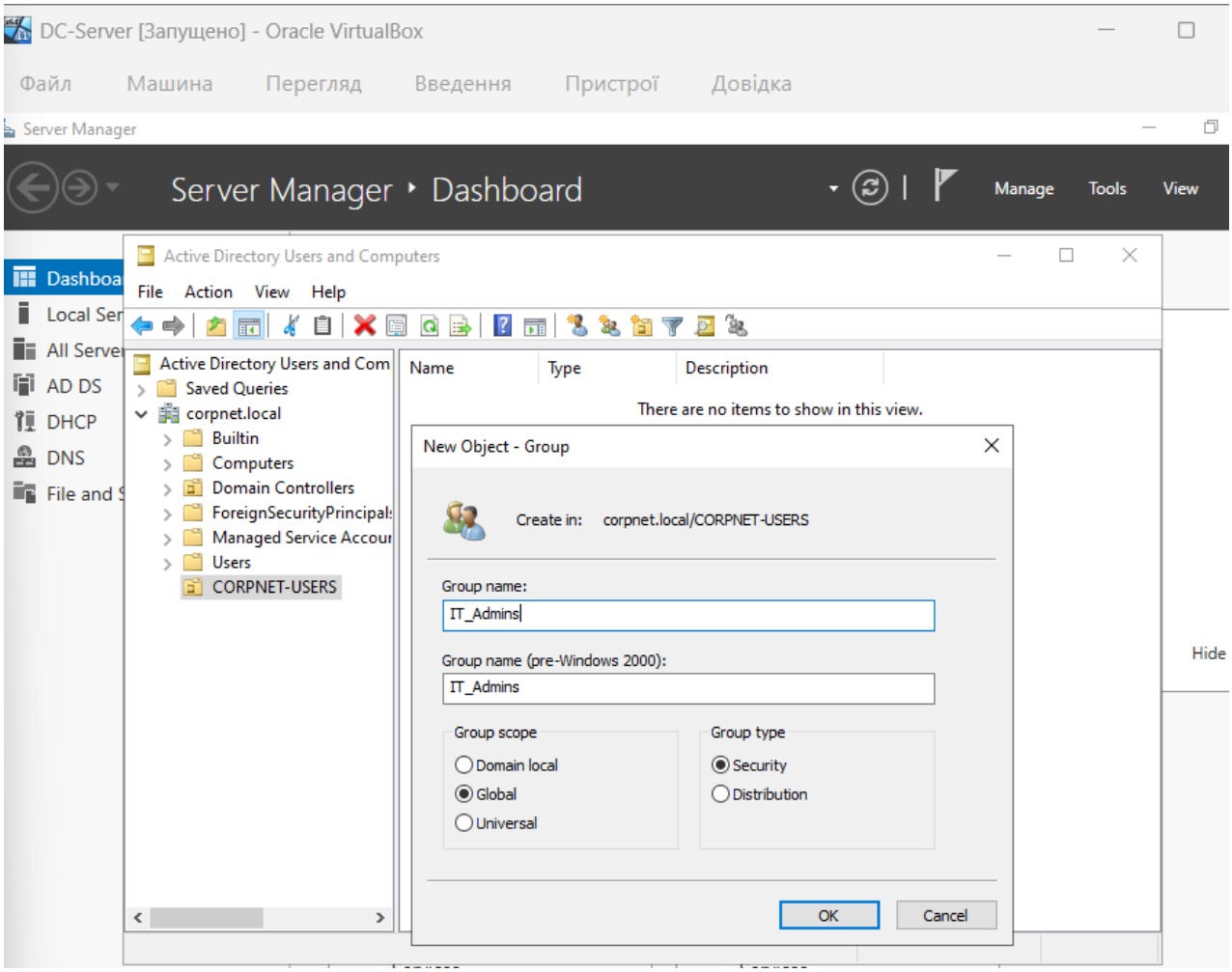


Рисунок 3.12 - Створення груп безпеки Active Directory

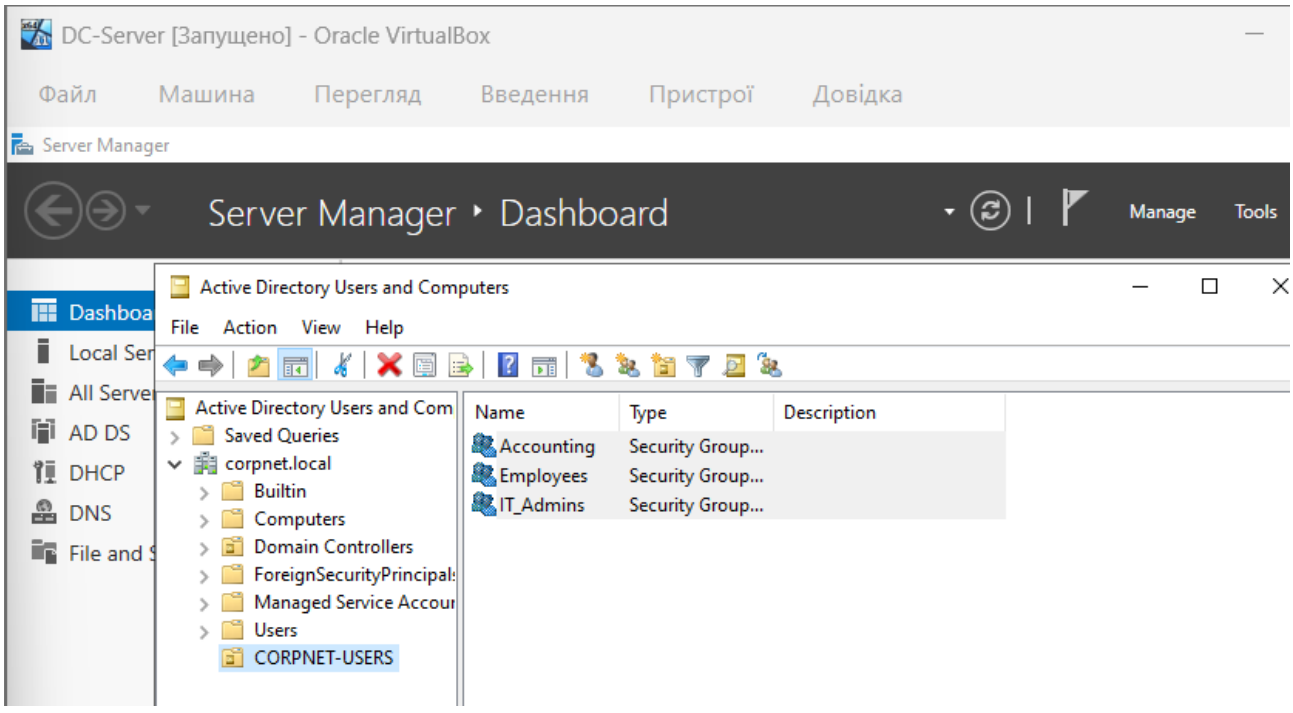


Рисунок 3.13 - Сформовані групи безпеки в домені

Далі було виконано створення облікових записів користувачів домену з їх подальшим розподілом по відповідним групам безпеки. Процес створення нового користувача відображений на рисунку 3.14; кінцевий перелік створених користувачів представлений на рисунку 3.15; приклад додавання користувачів до груп безпеки показано на рисунку 3.16 - 3.17.

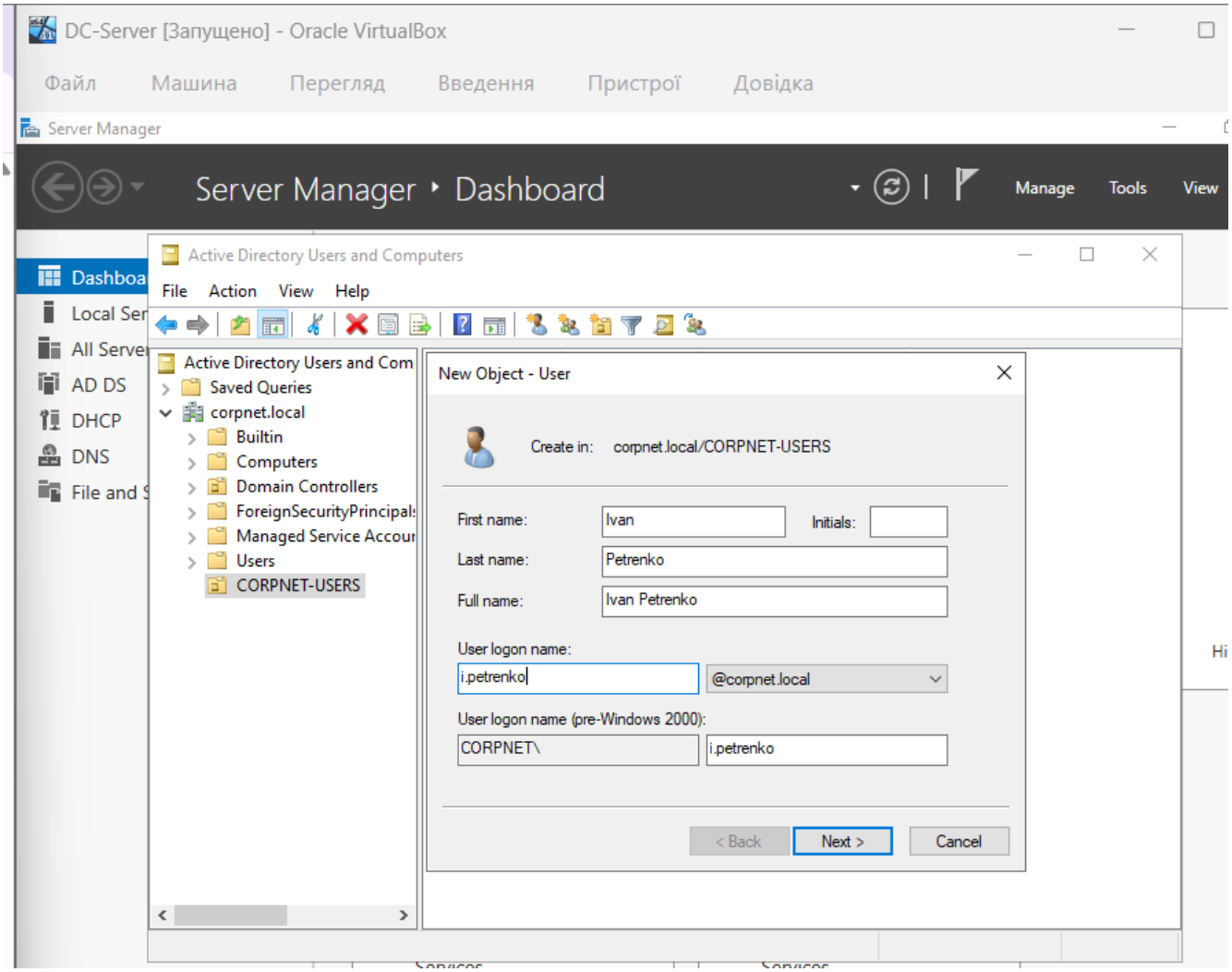


Рисунок 3.14 - Створення нового користувача в Active Directory

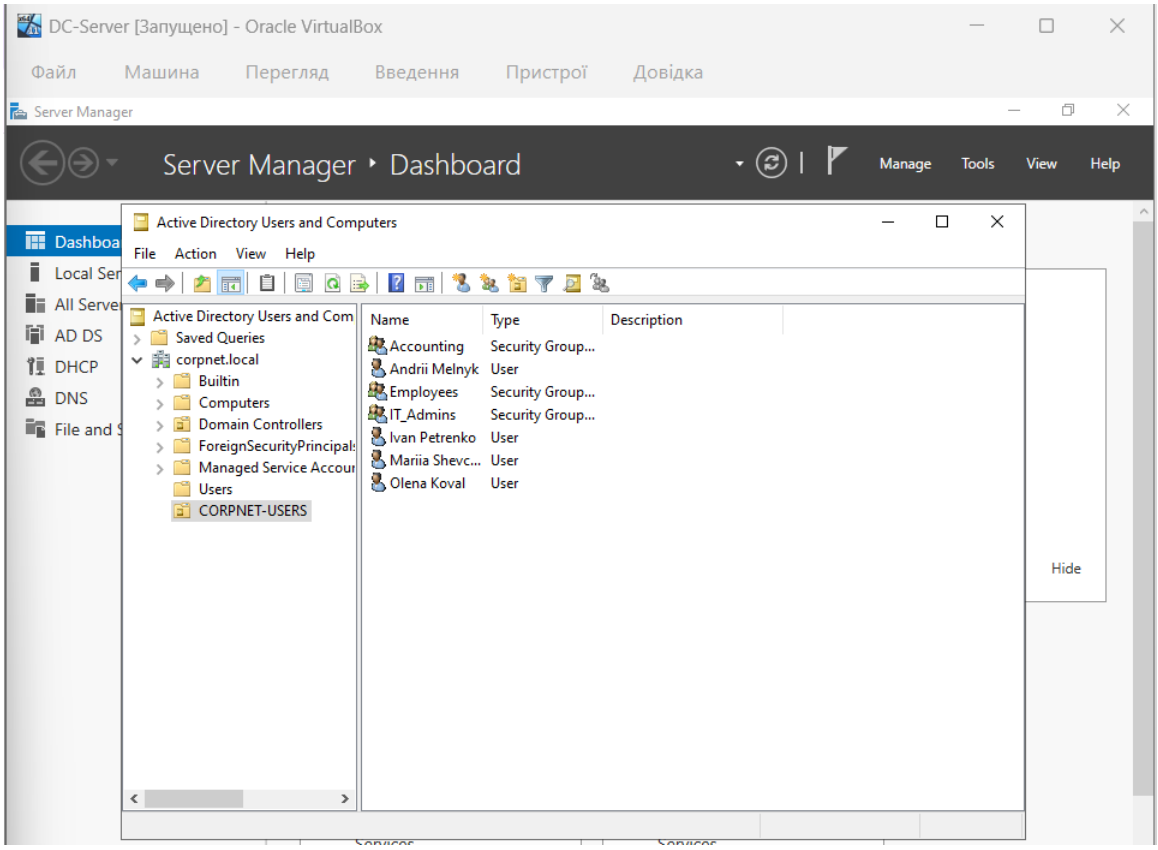


Рисунок 3.15 - Облікові записи користувачів домену

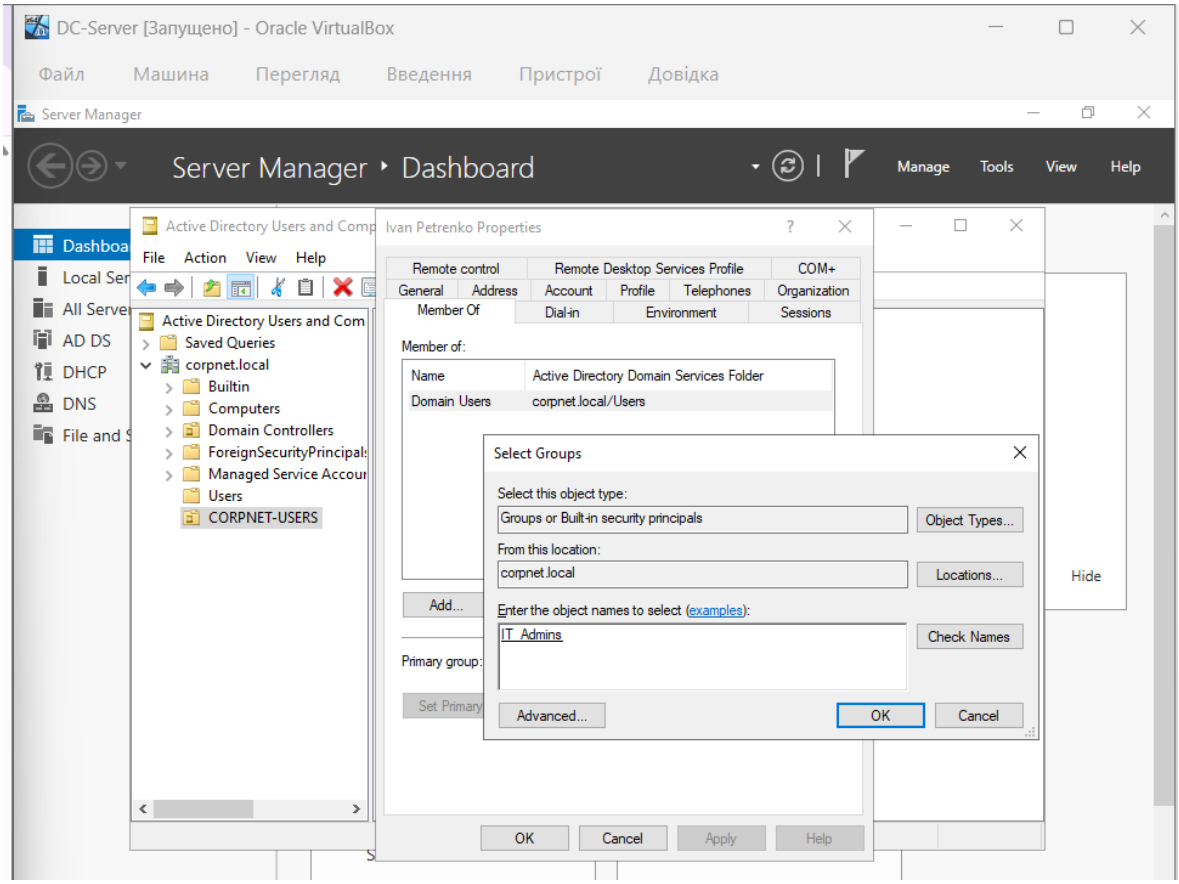


Рисунок 3.16 - Призначення користувачів до груп Active Directory

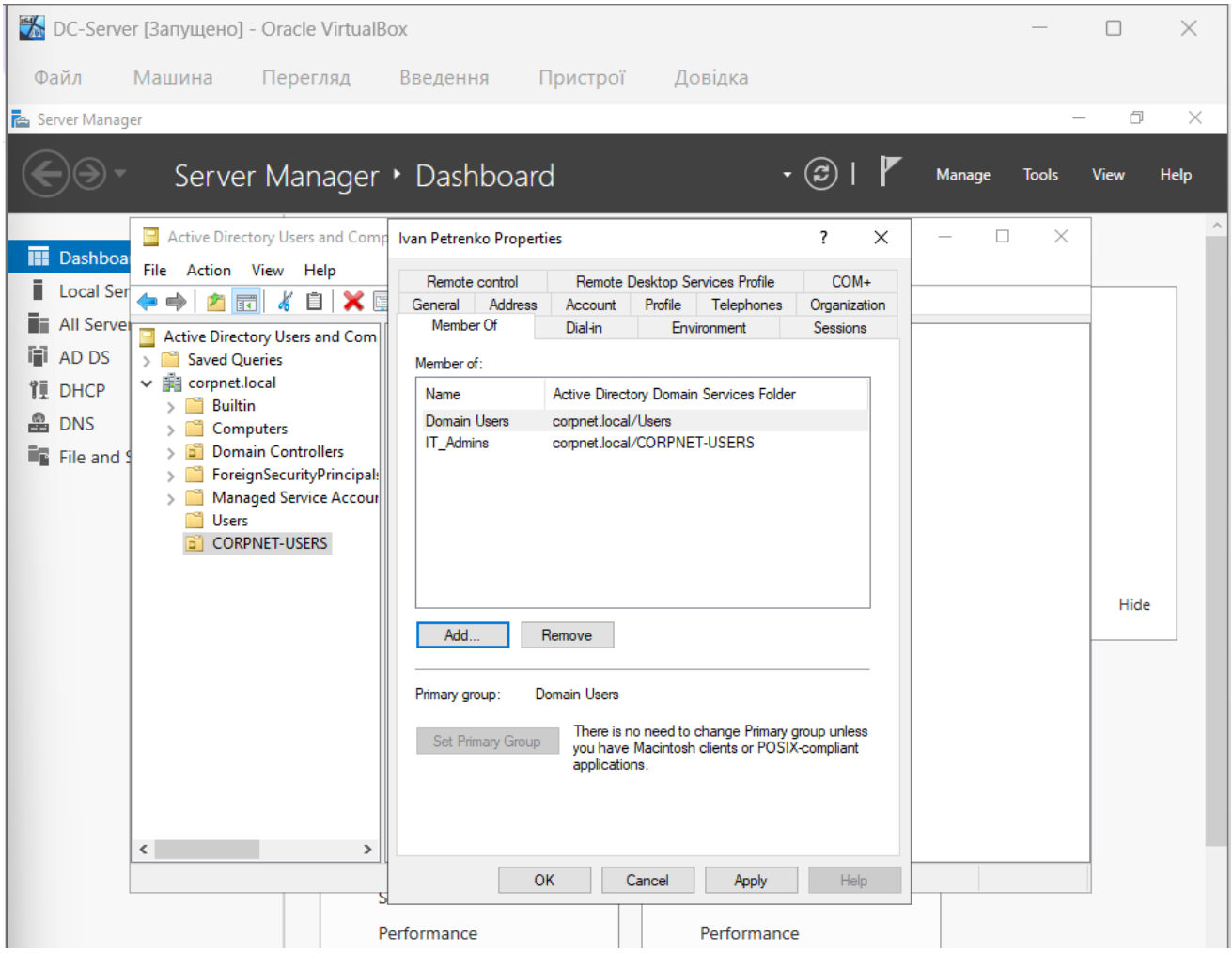


Рисунок 3.17 - Продовження прикладу додавання користувачів у груп Active Directory

Для управління політиками безпеки в домені використовувалися об'єкти групової політики (Group Policy Objects, GPO), які дозволяють централізовано встановлювати правила для користувачів та комп'ютерів. Це забезпечило реалізацію основних налаштувань безпеки, таких як вимоги до складності паролів, їх регулярної зміни, а також обмеження доступу до певних системних ресурсів.

Останнім етапом стало підключення корпоративних машин до доменної інфраструктури. Після успішного приєднання до домену corpnet.local корпоративні пристрої отримали можливість централізованої автентифікації та доступу до ресурсів відповідно до наданих прав, що підтверджує коректність функціонування доменної структури та мережних сервісів.

3.3 Реалізація файлового сховища та політик доступу

Після налаштування доменної інфраструктури було виконано конфігурацію файлового сервера FILE-SERVER, призначеного для централізованого зберігання корпоративної інформації та управління контрольованим доступом користувачів. Цей файловий сервер базується на операційній системі Windows Server і використовує файлову систему NTFS разом із технологією спільного доступу SMB (Server Message Block).

Для збереження даних був створений окремий логічний диск G:, який виключно використовується для корпоративних ресурсів. Структура каталогу складається з трьох основних папок: IT_Admins, Employees та Accounting, що відповідають різним групам користувачів і рівням доступу. Процес формування каталогів на диску G: продемонстровано на рисунку 3.18, а фінальний вигляд створених папок можна побачити на рисунку 3.19.

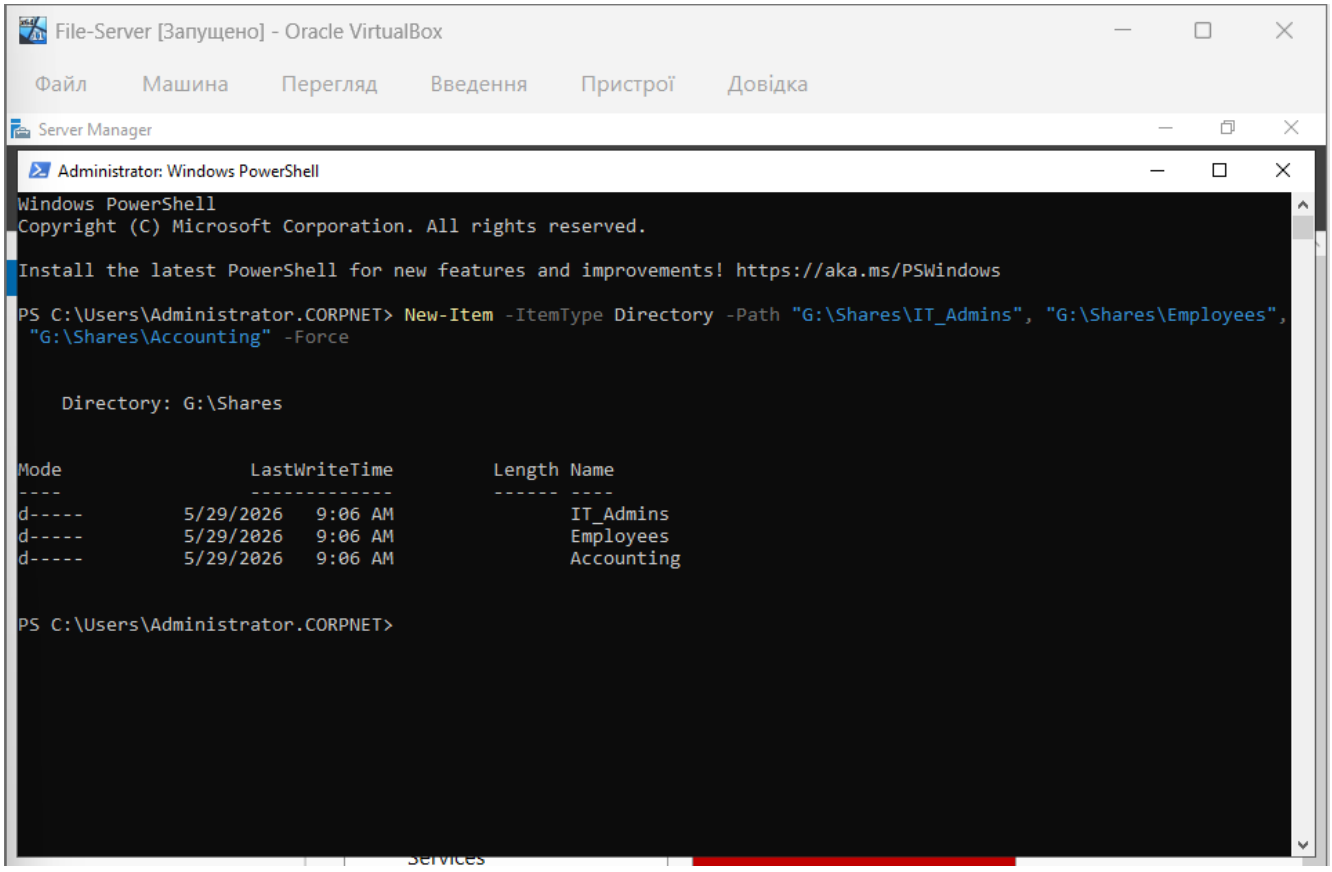


Рисунок 3.18 - Процес створення структури каталогів на диску G

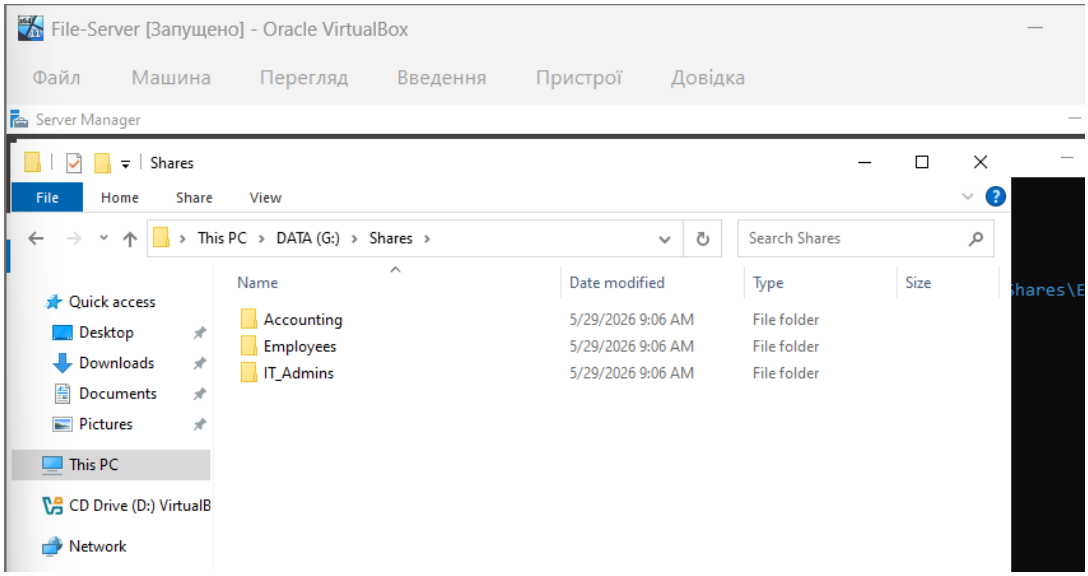


Рисунок 3.19 - Фінальний вигляд створених папок

Доступ користувачів до файлового сховища реалізовано через мережні ресурси SMB (спільні папки). Відповідно до структури системи створено окремі спільні ресурси для кожної групи користувачів, що забезпечує контрольований доступ до корпоративних даних. Загальний процес налаштування спільних папок наведено на рисунку 3.20.

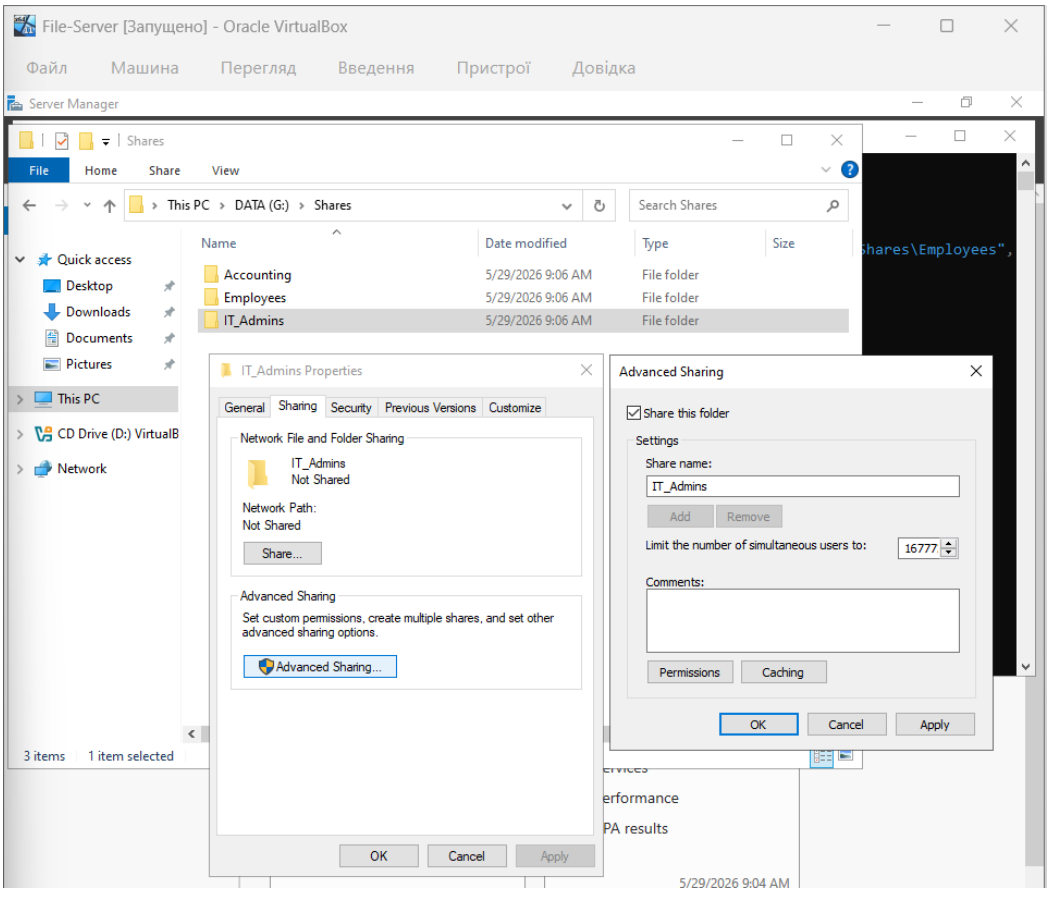


Рисунок 3.20 - Загальний вигляд налаштування спільних папок

Доступ до ресурсів здійснюється через мережні шляхи виду \\FILE-SERVER\IT_Admins, \\FILE-SERVER\Employees та \\FILE-SERVER\Accounting, що забезпечує централізовану взаємодію користувачів із файловим сервером у межах доменної інфраструктури.

Для забезпечення захисту інформації були налаштовані списки контролю доступу (ACL), а також реалізовано принцип Zero Trust, згідно з яким доступ надається лише тим користувачам і групам, які мають відповідні повноваження для виконання своїх службових обов'язків. Налаштування ізоляції ресурсів та відключення успадкування прав доступу показано на рисунку 3.21.

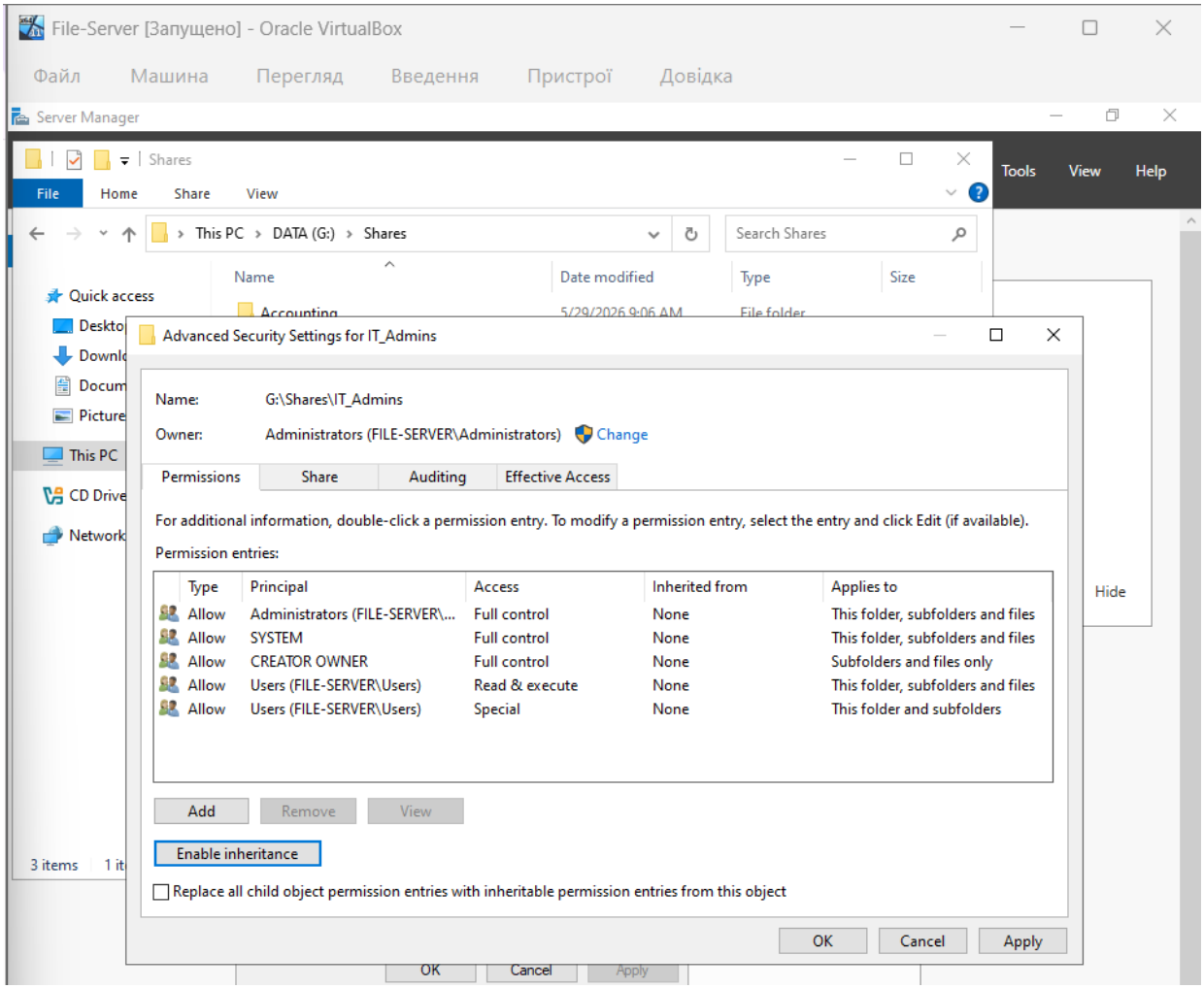


Рисунок 3.21 - Налаштування ізоляції і відключення успадкування прав доступу

Далі були налаштовані права доступу для кожної категорії користувачів. Для папки IT_Admins призначено повні права доступу (Full Control), що надає

адміністраторам повний контроль над файлами, папками та параметрами доступу. Це дозволяє виконувати всі необхідні операції з корпоративними даними, такі як створення, редагування та видалення ресурсів, а також управління дозволами.

Папка Employees отримала обмежені права доступу (Modify, Read, Write, Read & Execute) у відповідності до принципу мінімальних привілеїв. Цей підхід забезпечує можливість роботи з файлами без надання користувачам адміністративних прав або доступу до критичних системних налаштувань, що підвищує рівень інформаційної безпеки.

Для папки Accounting доступ обмежений лише для членів відповідної групи, що дозволяє ізолювати фінансову інформацію від інших користувачів корпоративної мережі. Це створює додатковий рівень захисту конфіденційних даних і зменшує ризик несанкціонованого доступу.

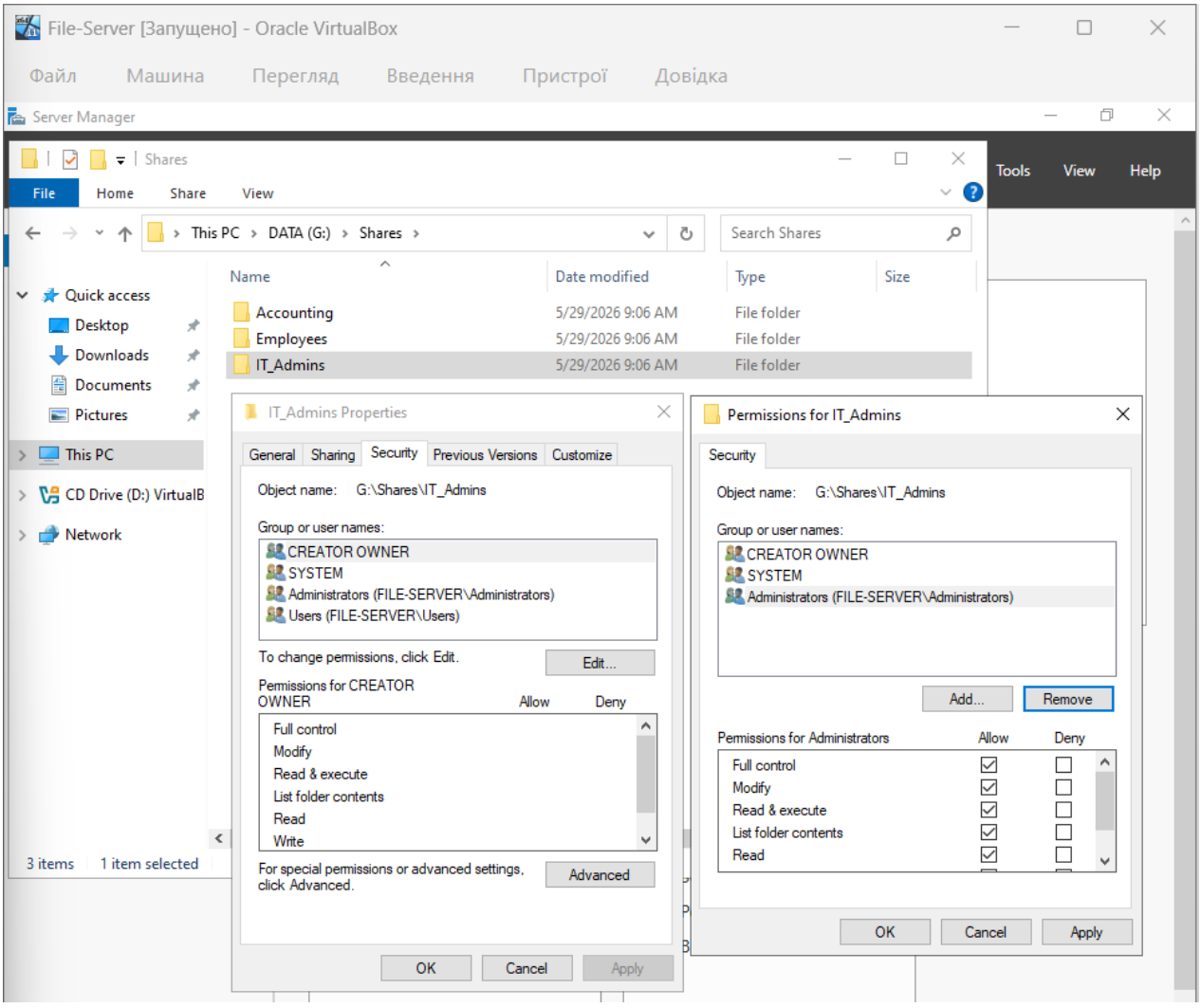


Рисунок 3.22 - Видалення облікового запису користувача (User)

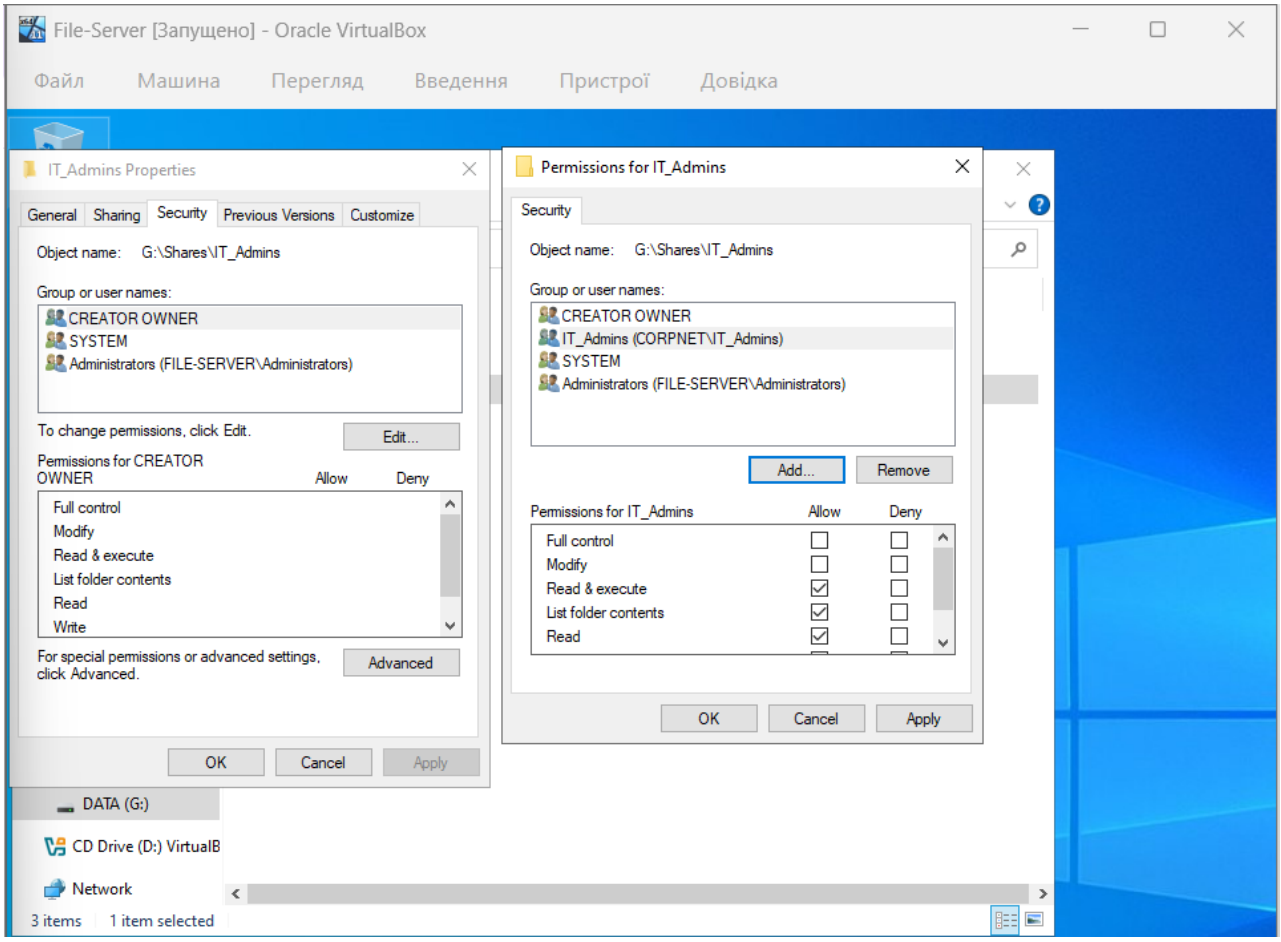


Рисунок 3.23 - Створення групи безпеки IT_Admins

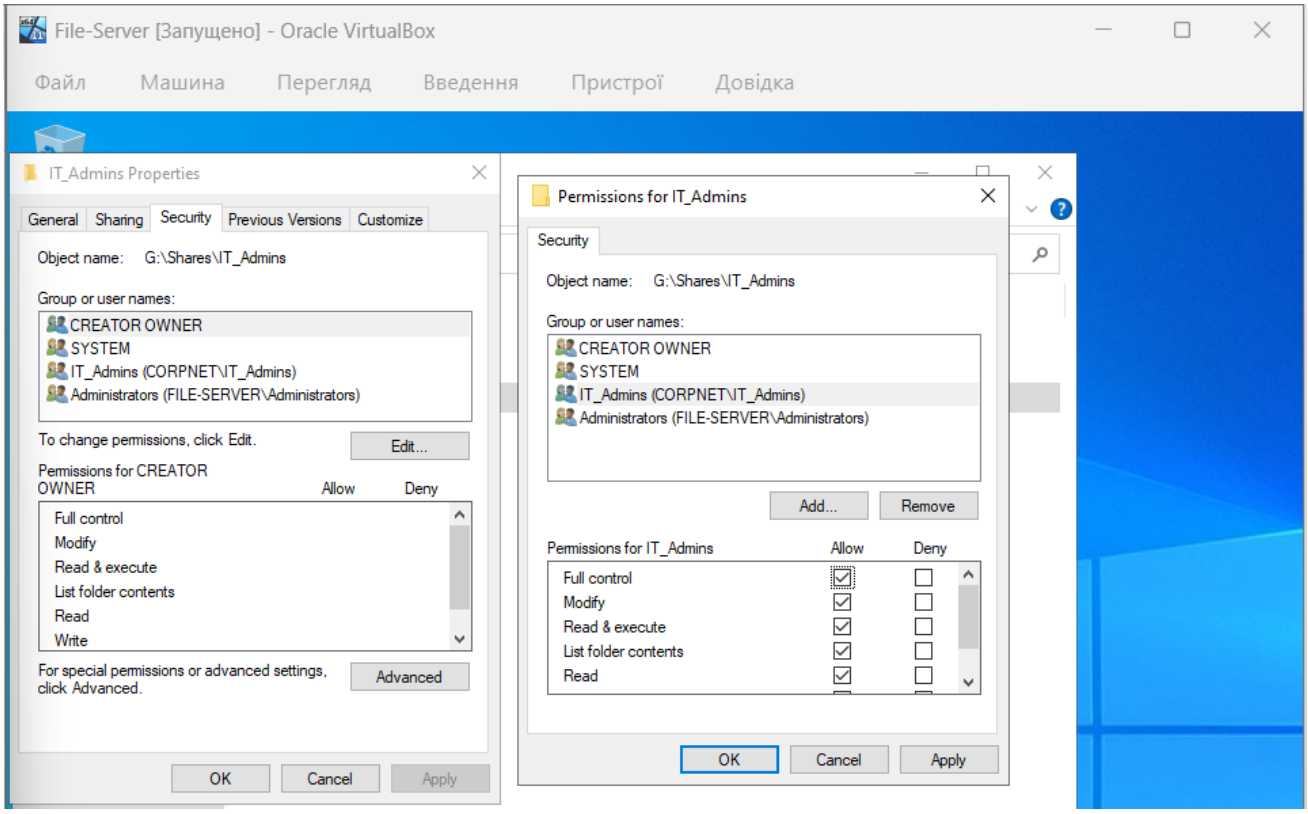


Рисунок 3.24 - Призначення прав доступу для групи IT_Admins

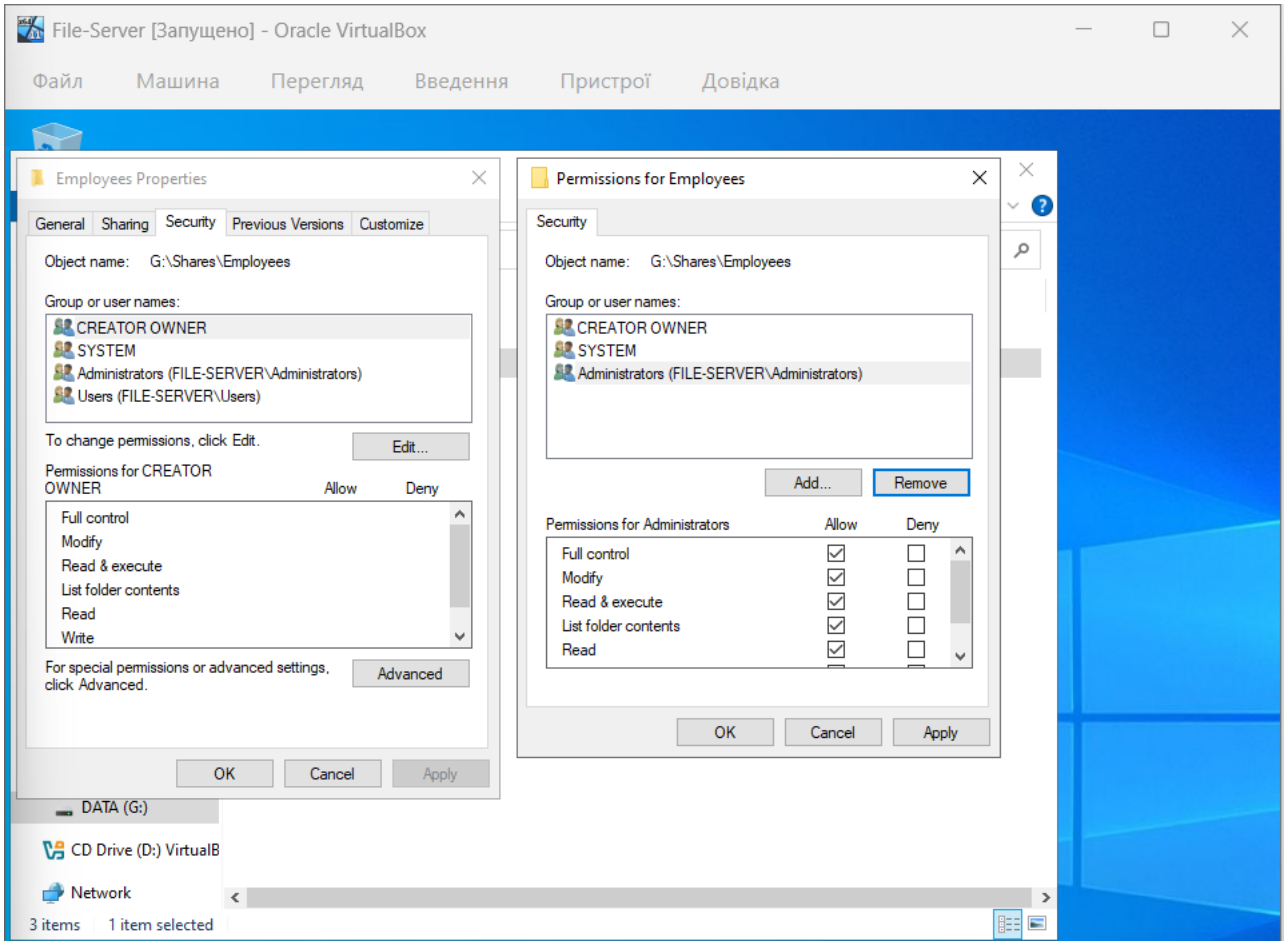


Рисунок 3.25 - Видалення зайвих груп під час налаштування доступу

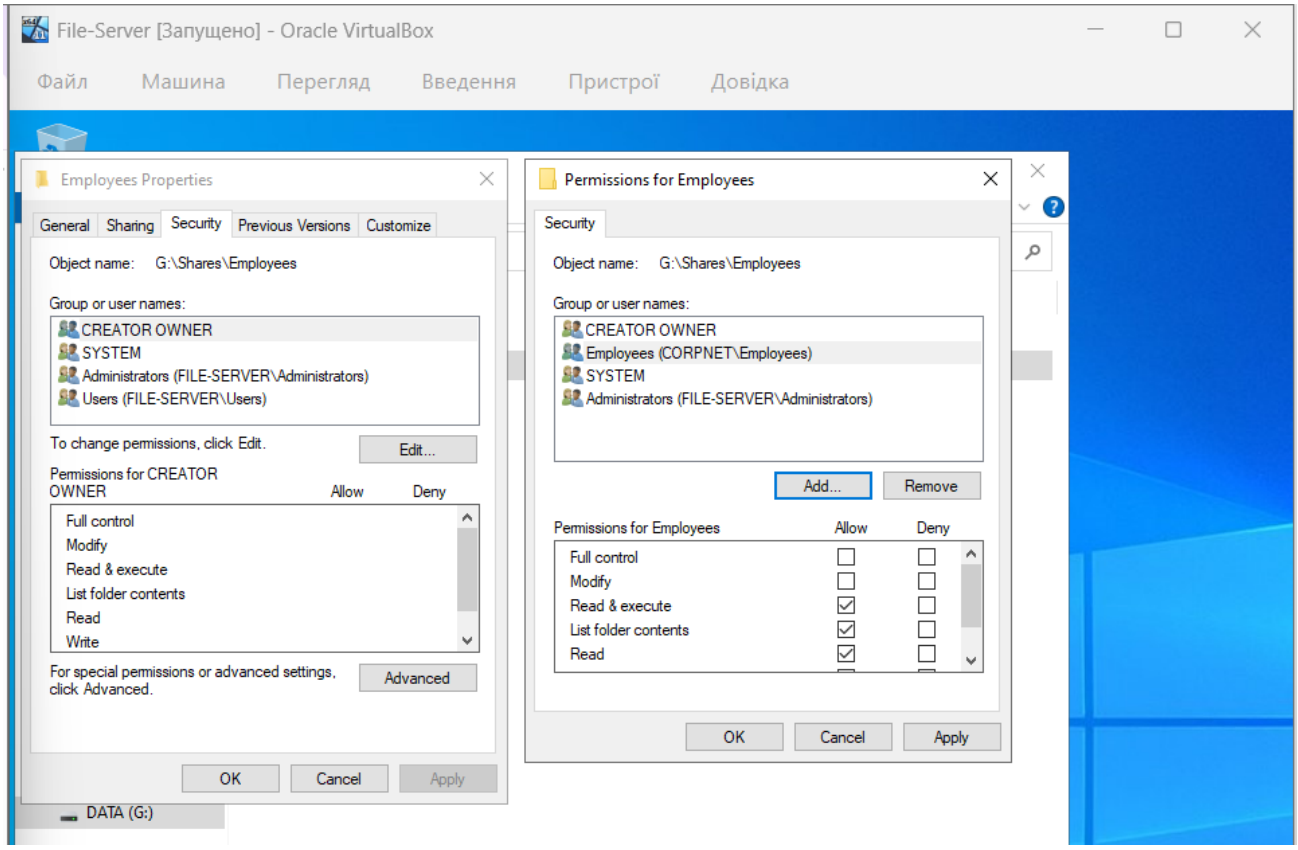


Рисунок 3.26 - Створення групи Employees у Active Directory

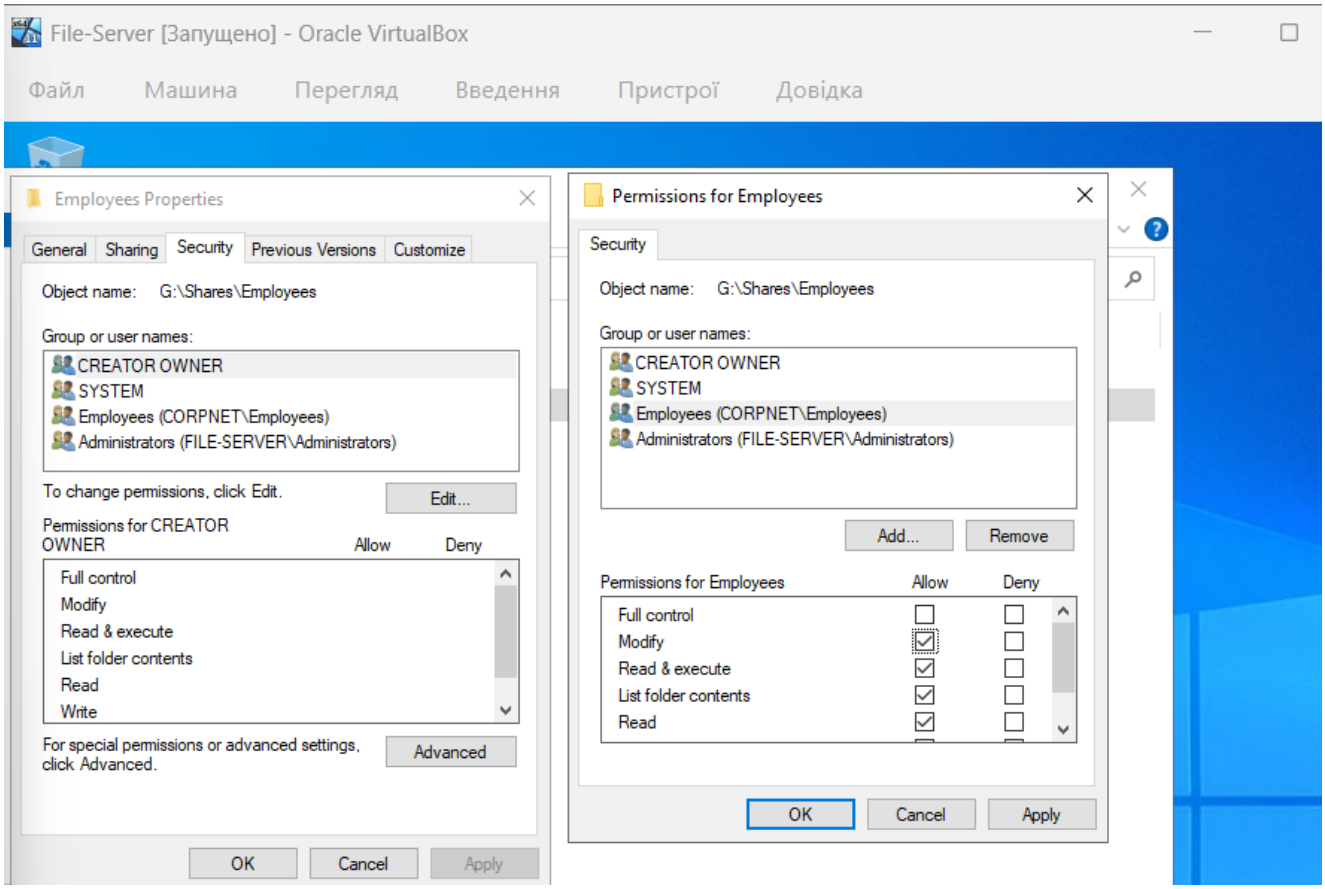


Рисунок 3.27 - Налаштування прав доступу для групи Employees

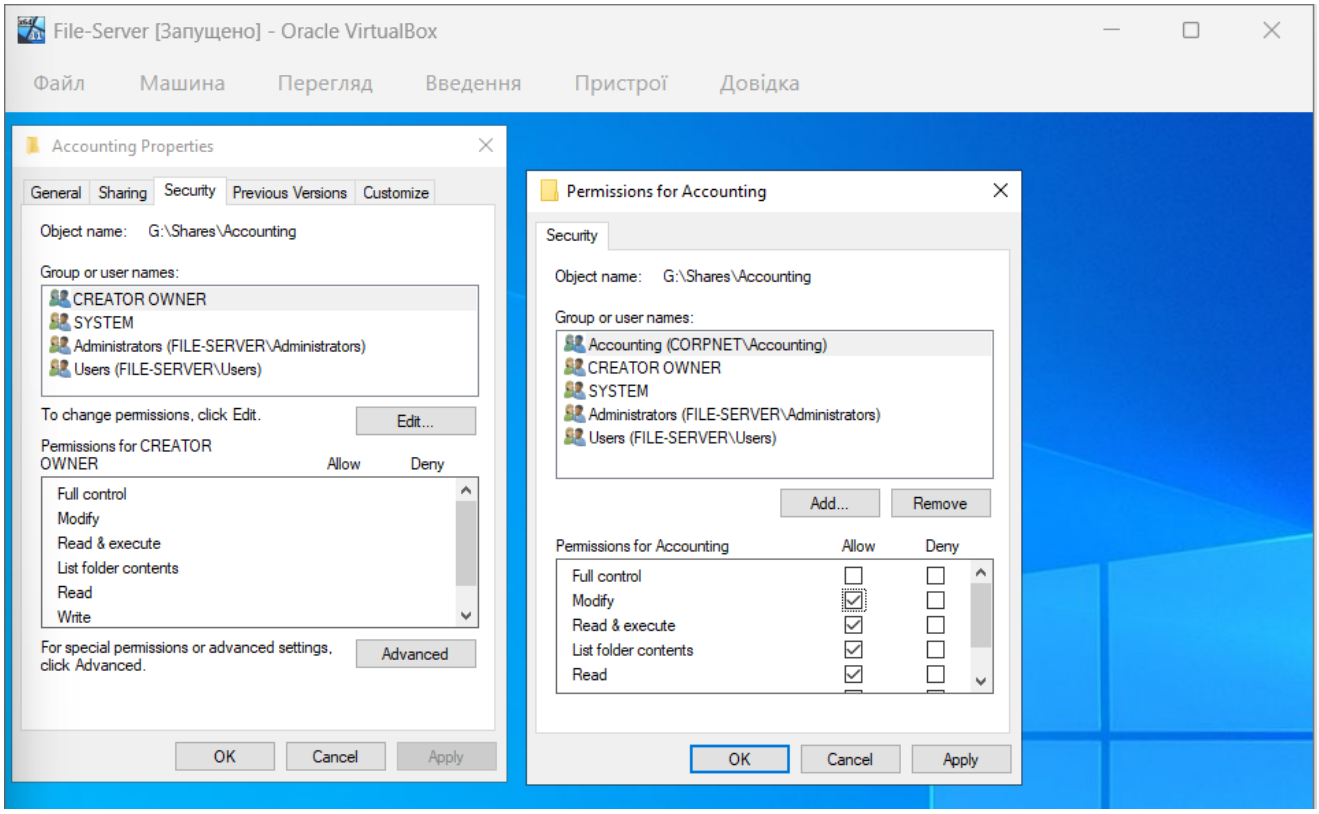


Рисунок 3.28 - Створення групи Accounting та призначення прав доступу

Після завершення налаштування прав доступу була проведена перевірка коректності функціонування системи розмежування доступу. Тестування здійснювалося з корпоративної станції Client-W, яка підключена до домену CORPNET.LOCAL. У процесі тестування виконувались входи користувачів з різних груп та перевірялася їх можливість доступу до відповідних ресурсів файлового сервера.

Отже, налаштована система продемонструвала правильність роботи механізмів розмежування доступу та підтвердила ефективність реалізованої моделі безпеки файлового сховища.

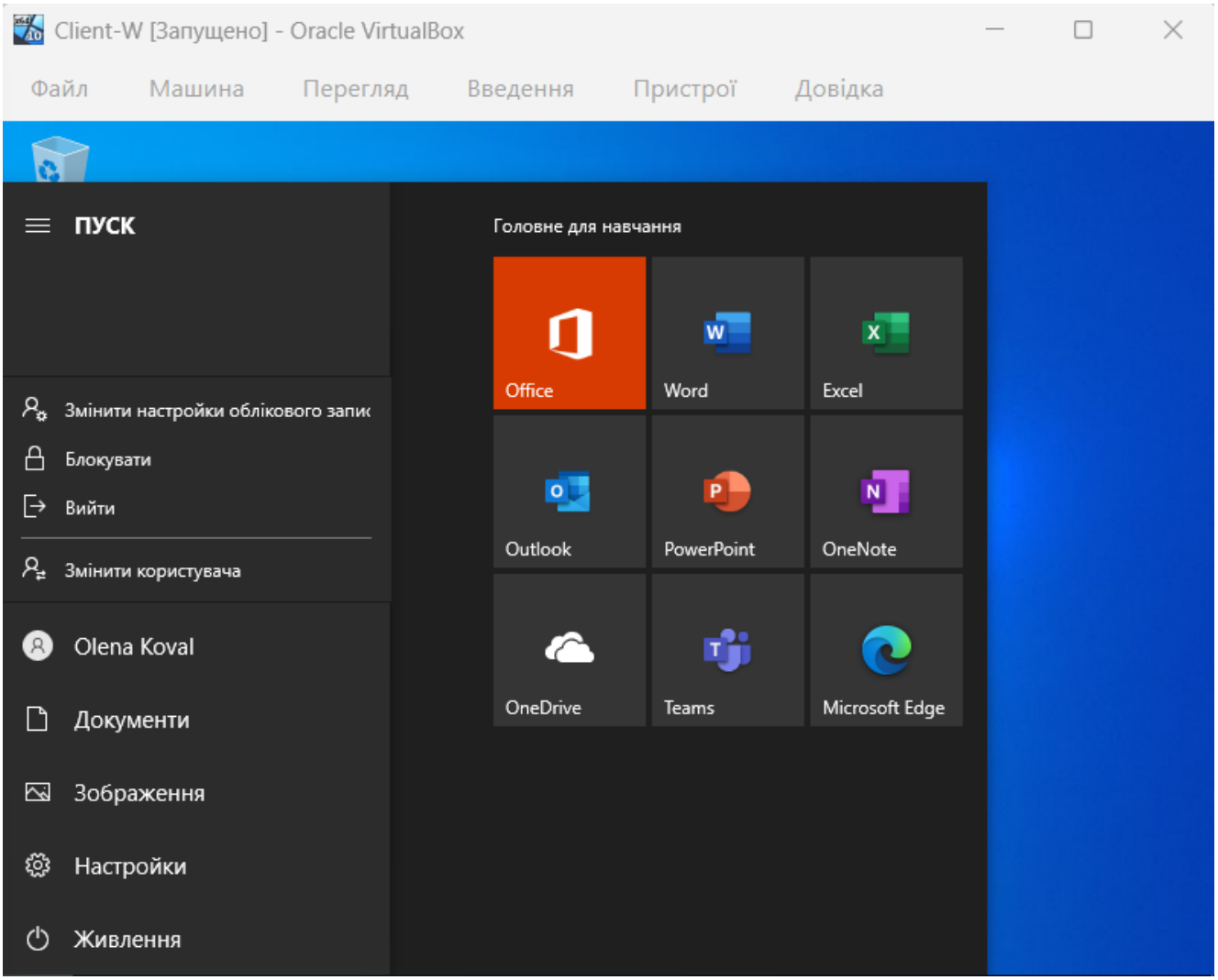


Рисунок 3.29 - Перевірка автентифікації користувача в домені

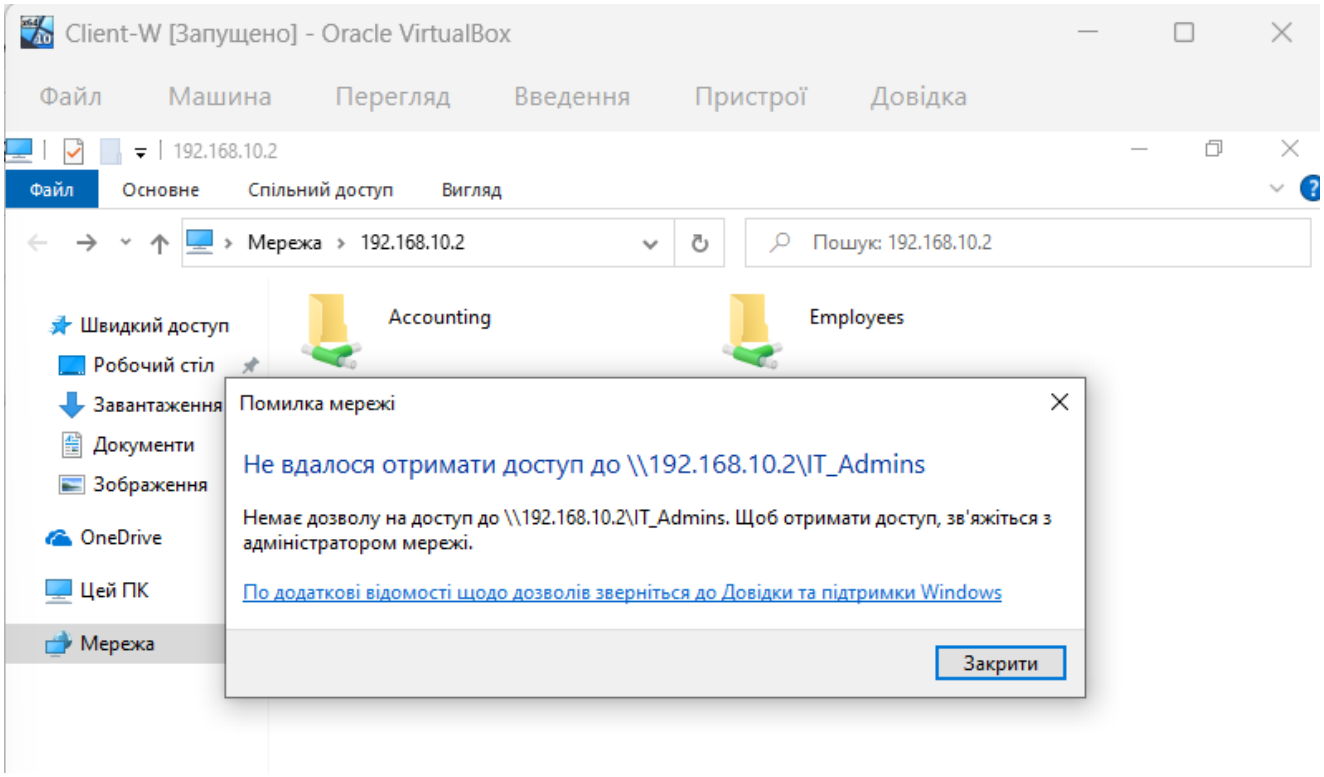


Рисунок 3.30 - Спроба доступу до ресурсів групи IT_Admins

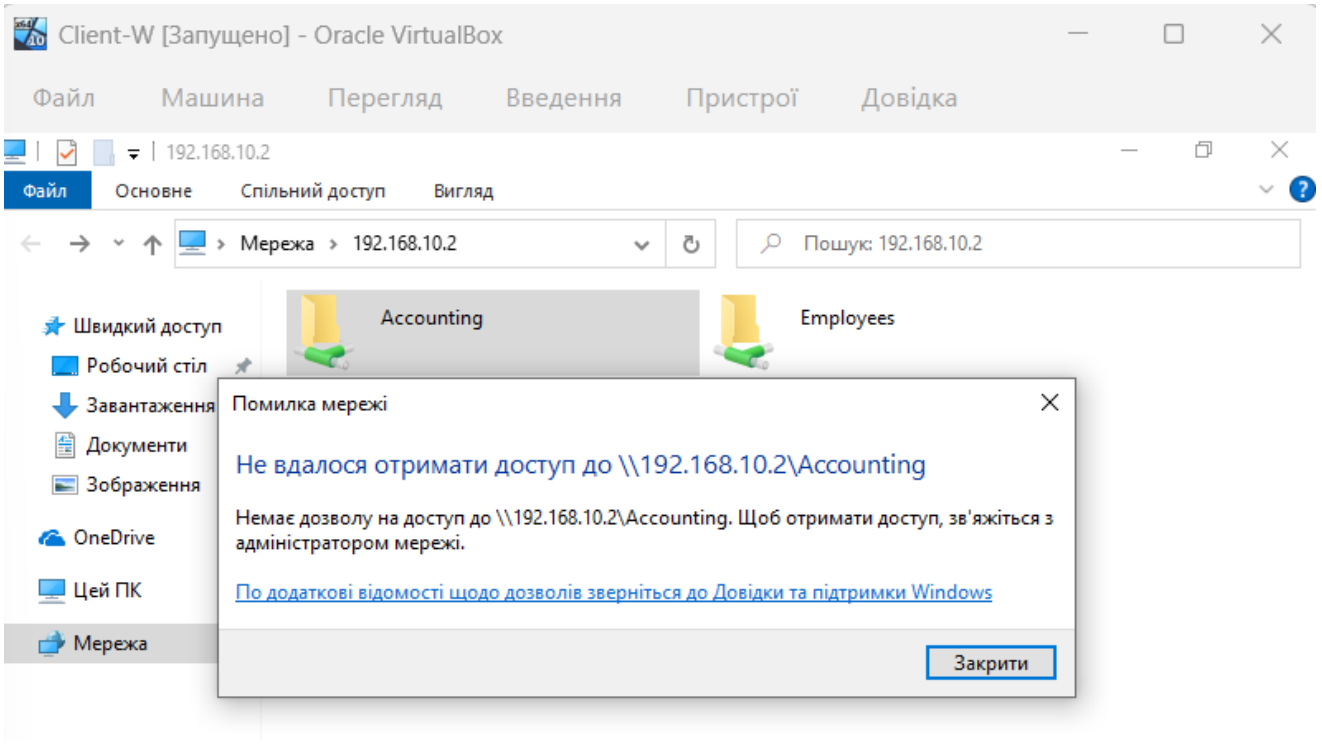


Рисунок 3.31 - Перевірка доступу до ресурсів групи Accounting

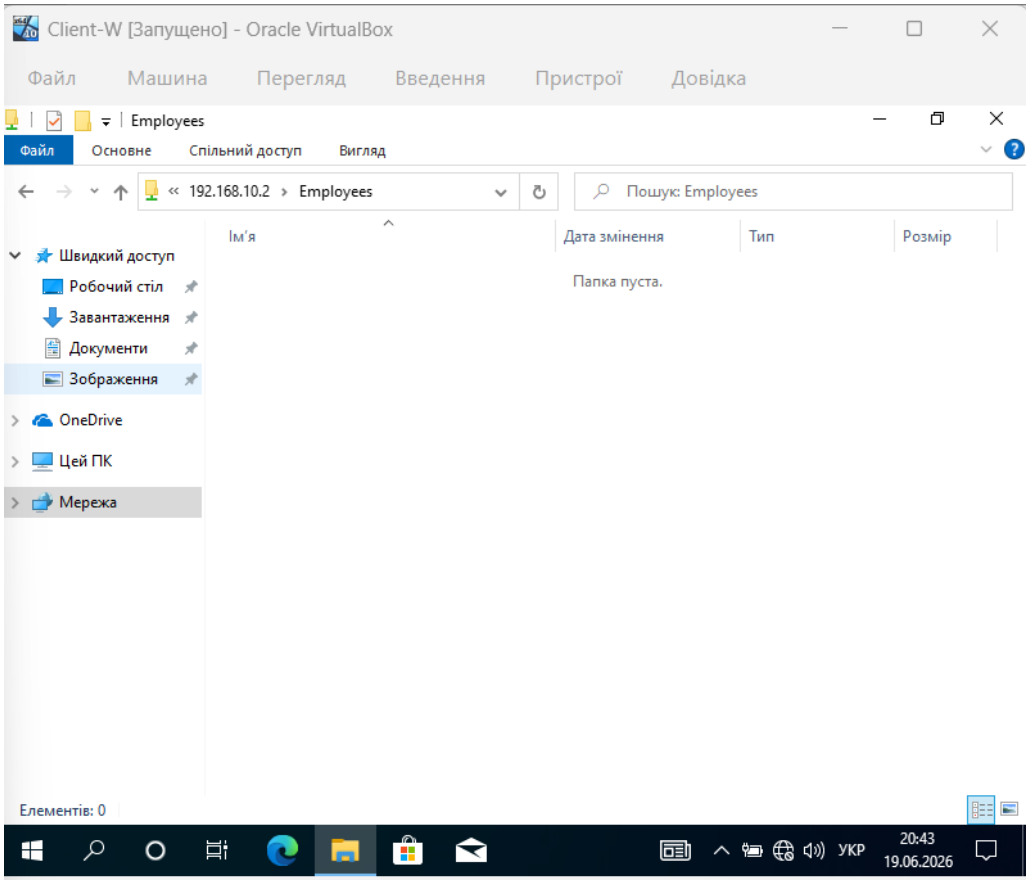


Рисунок 3.32 - Перевірка доступу до ресурсів групи Employees

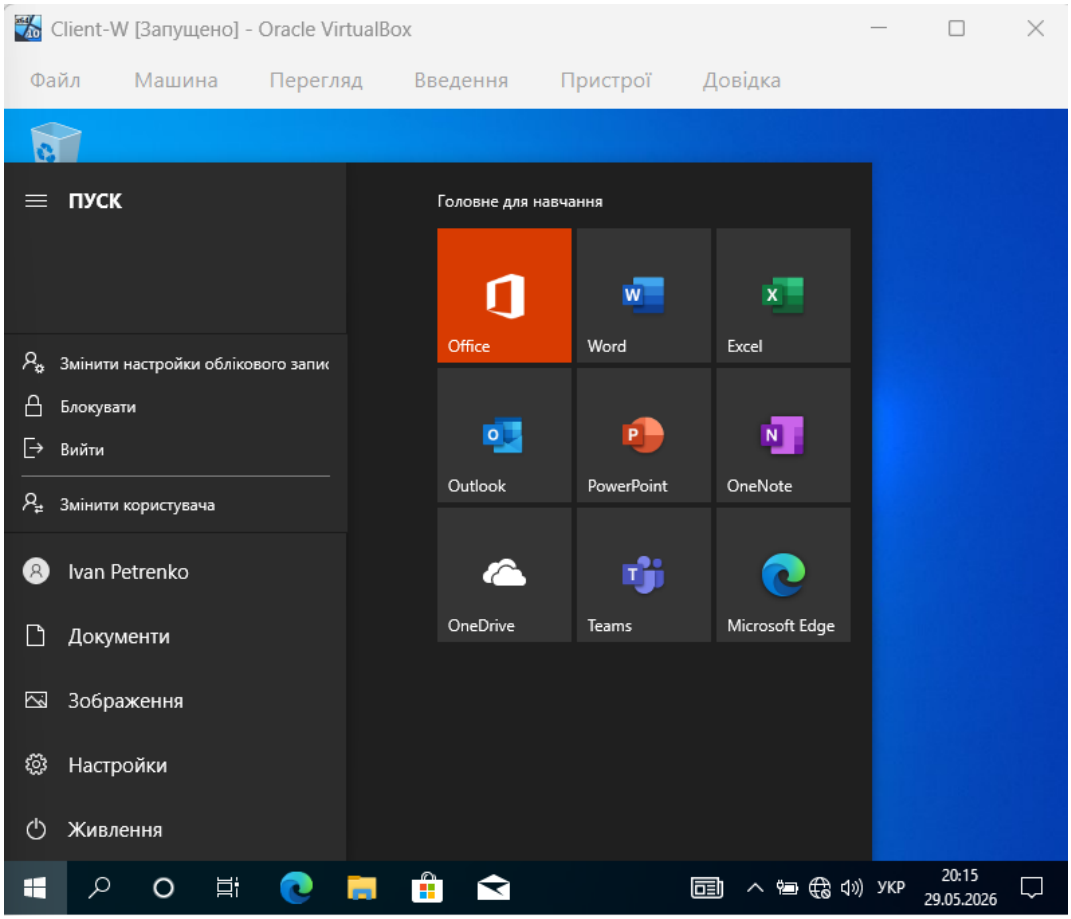


Рисунок 3.33 - Автентифікація користувача

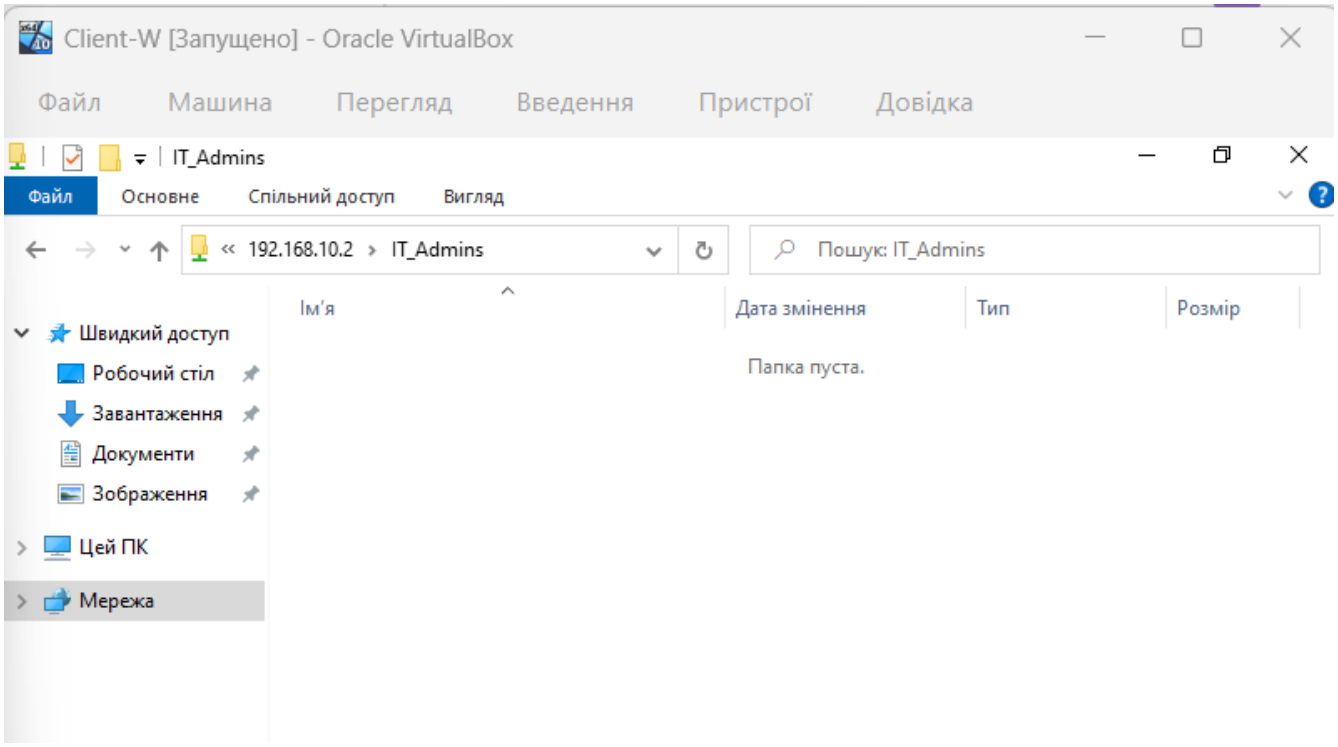


Рисунок 3.34 - Перевірка політик доступу для групи IT_Admins

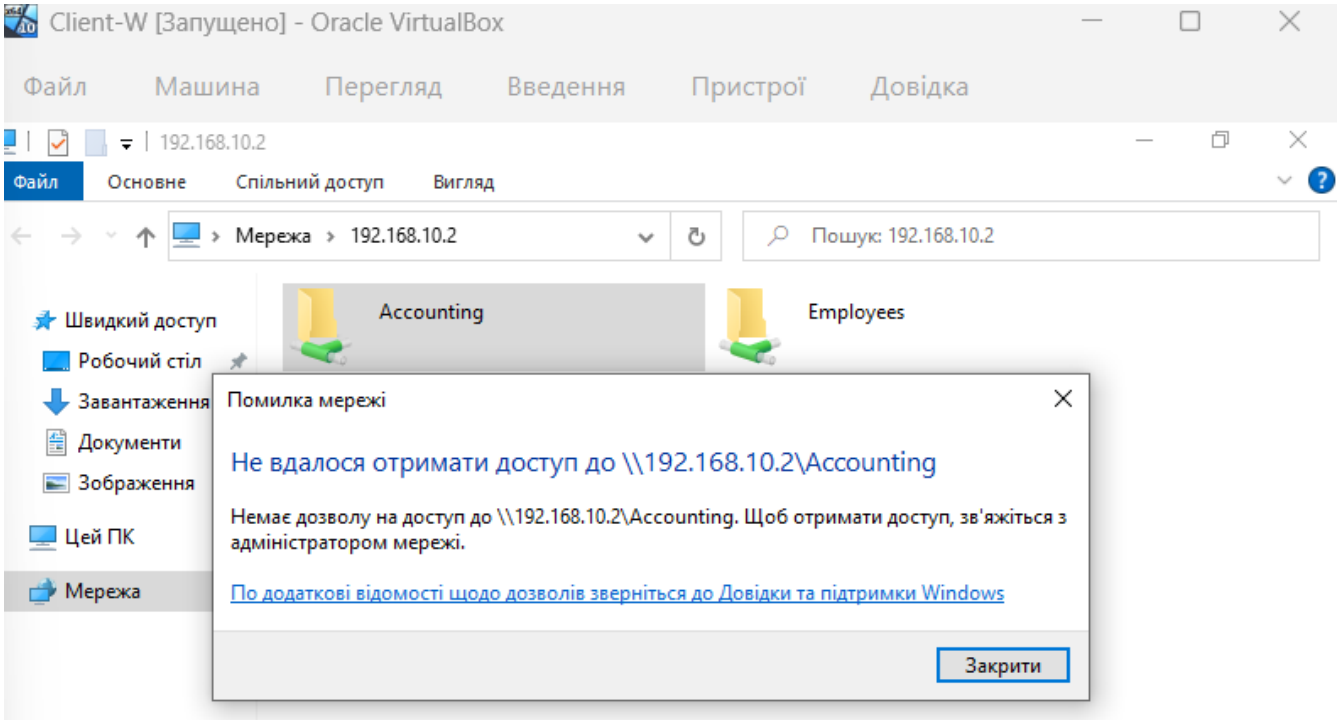


Рисунок 3.35 - Перевірка політик доступу для групи Accounting

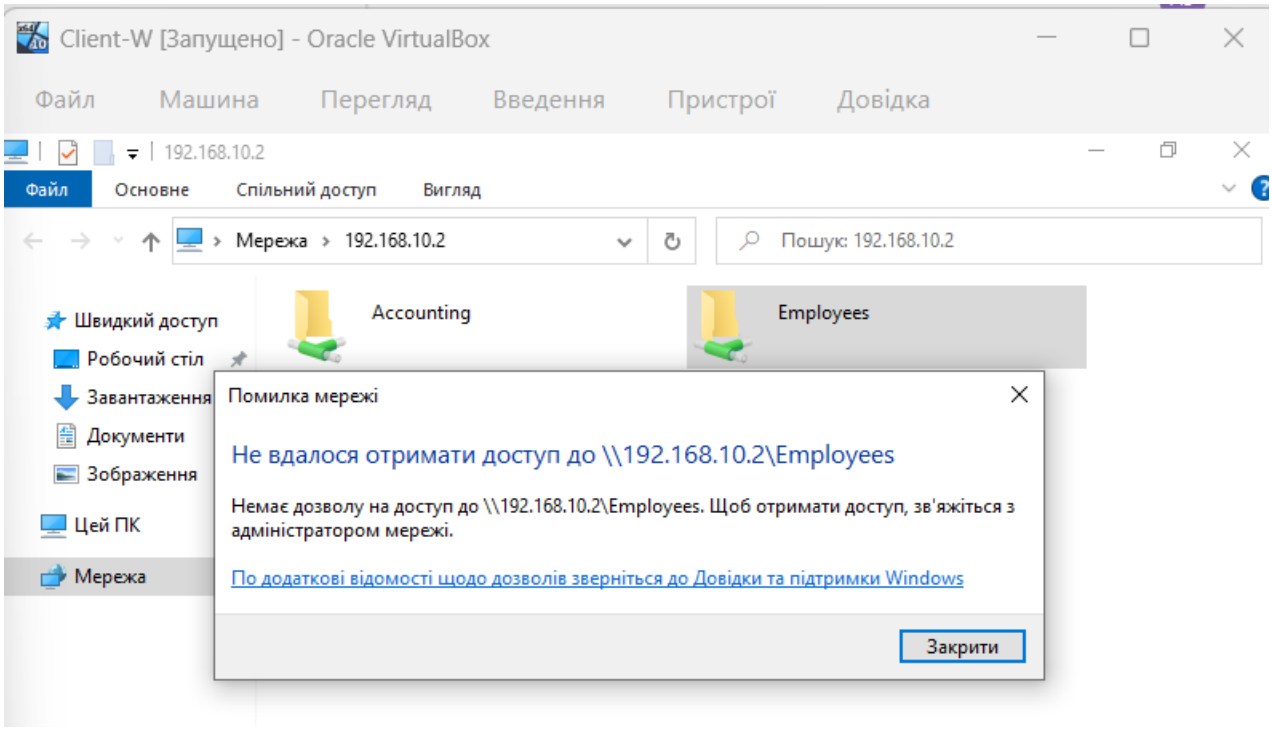


Рисунок 3.36 - Перевірка політик доступу для групи Employees

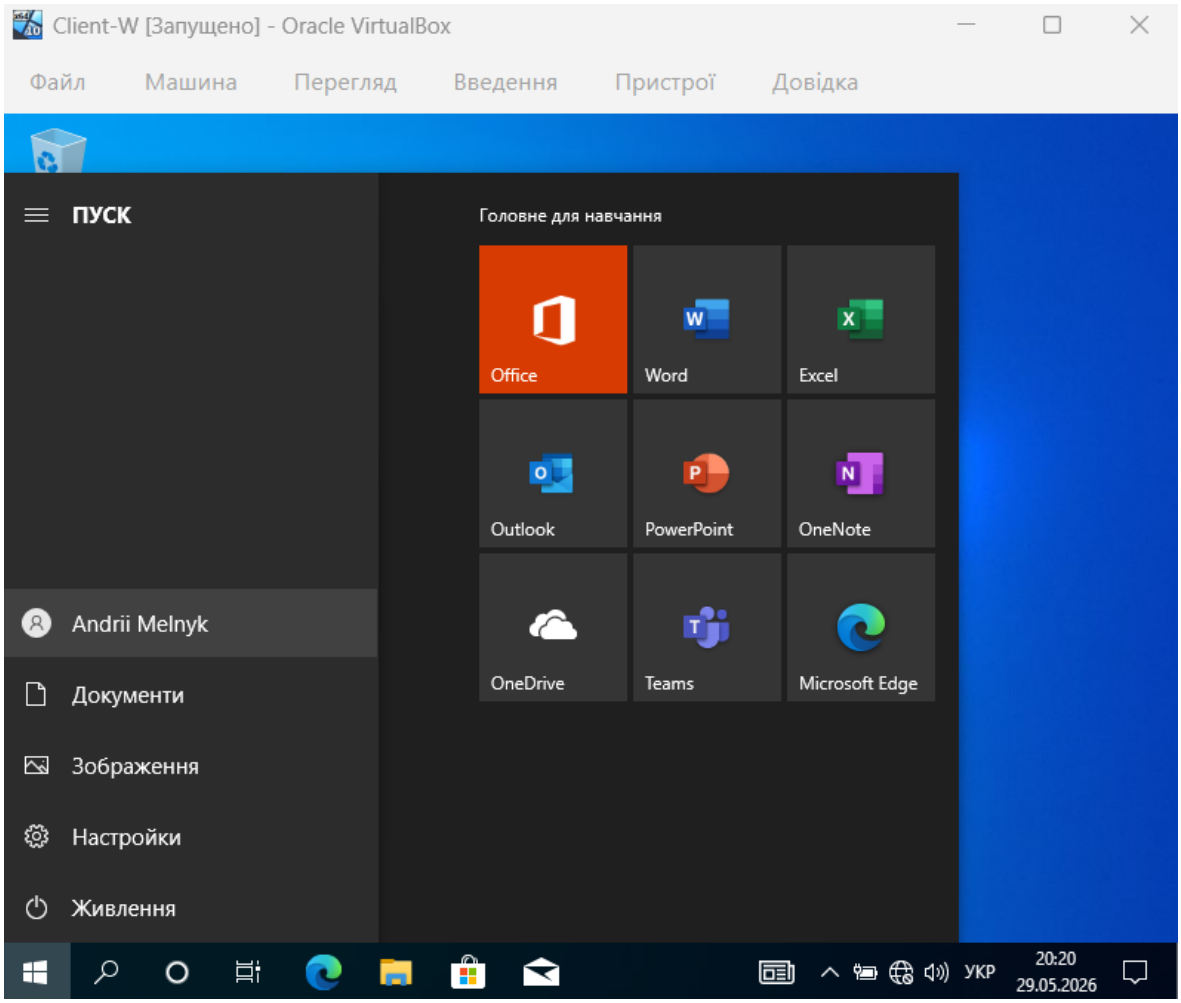


Рисунок 3.37 - Повторна автентифікація користувача в домені

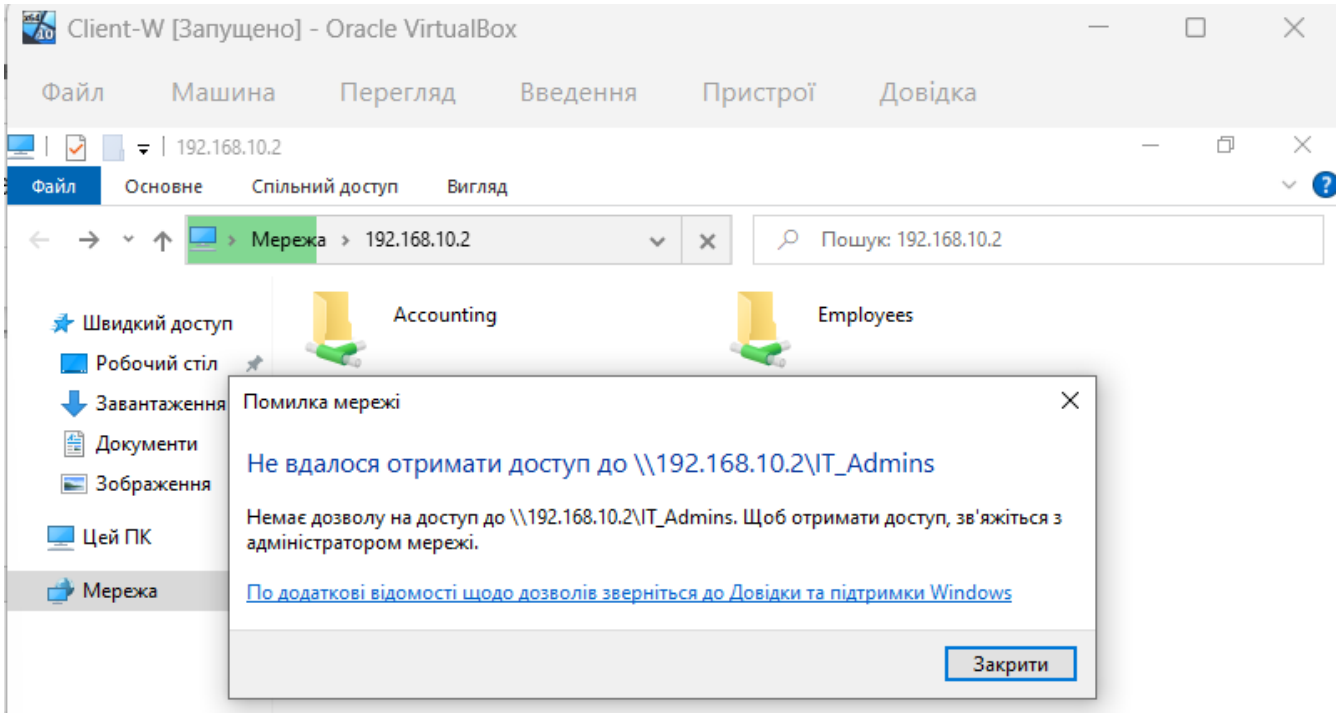


Рисунок 3.38 - Тест доступу до ресурсів IT_Admins

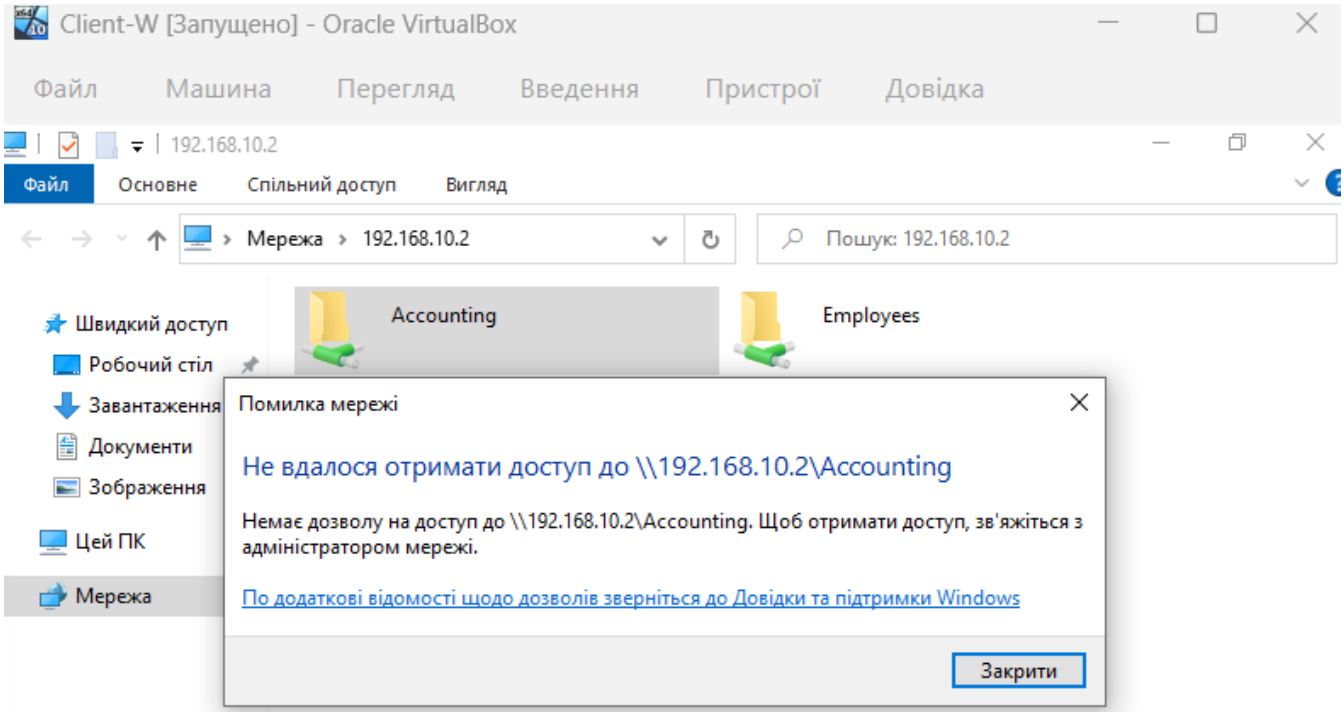


Рисунок 3.39 - Тест доступу до ресурсів Accounting

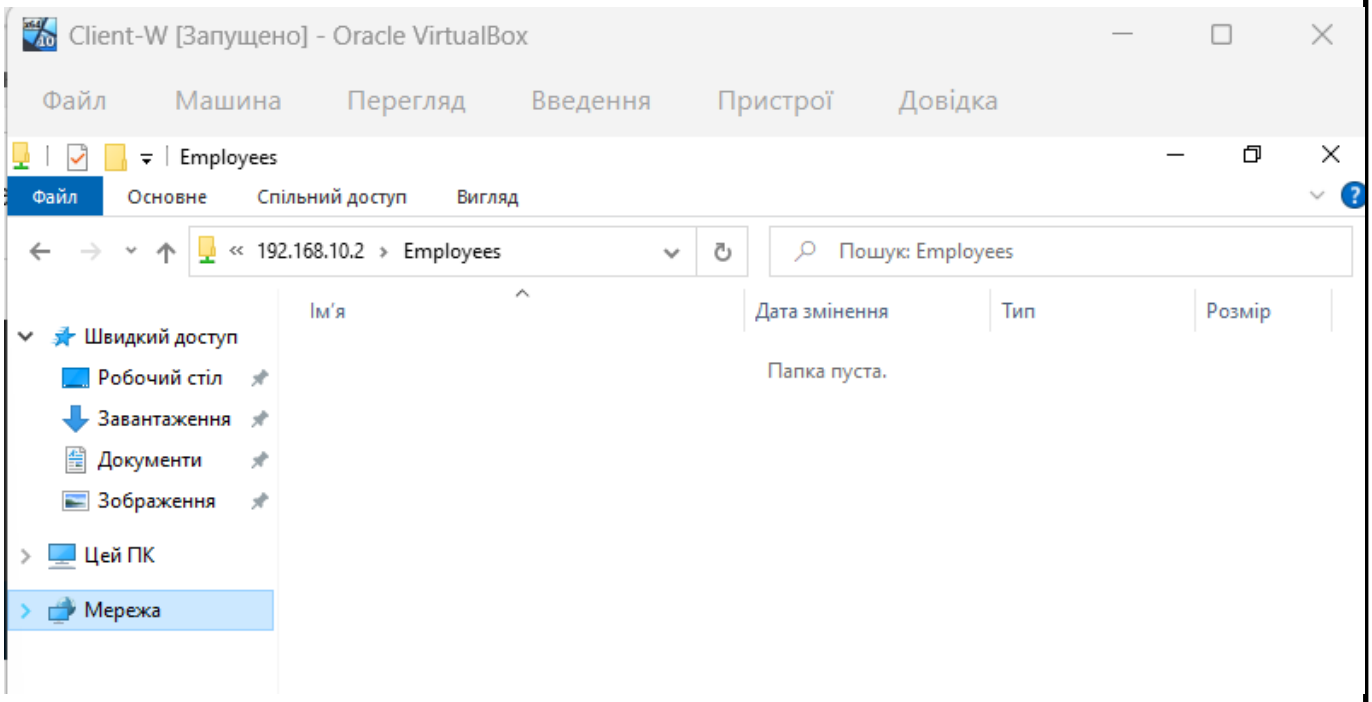


Рисунок 3.40 - Тест доступу до ресурсів Employees

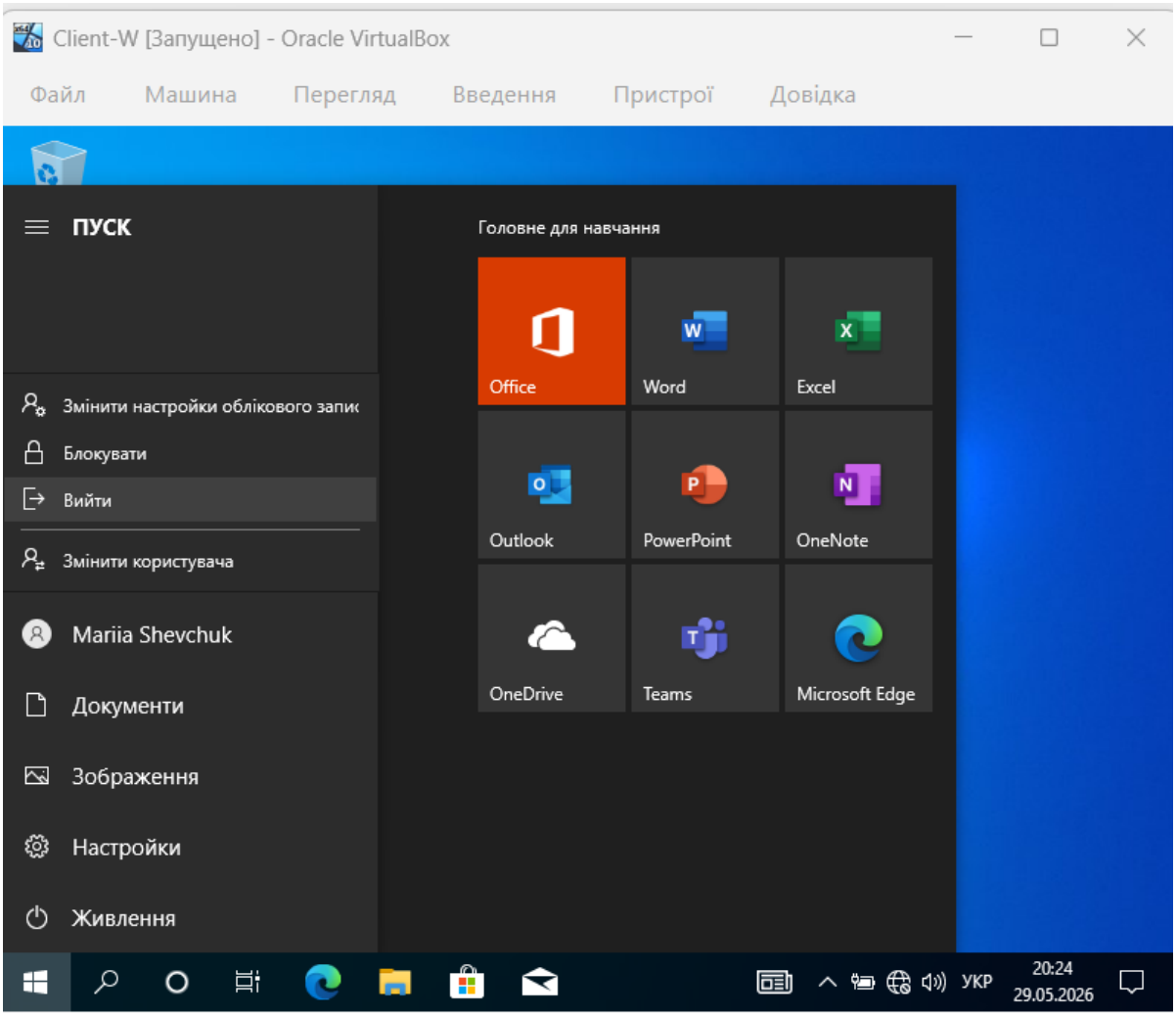


Рисунок 3.41 - Виконано вхід користувача до системи

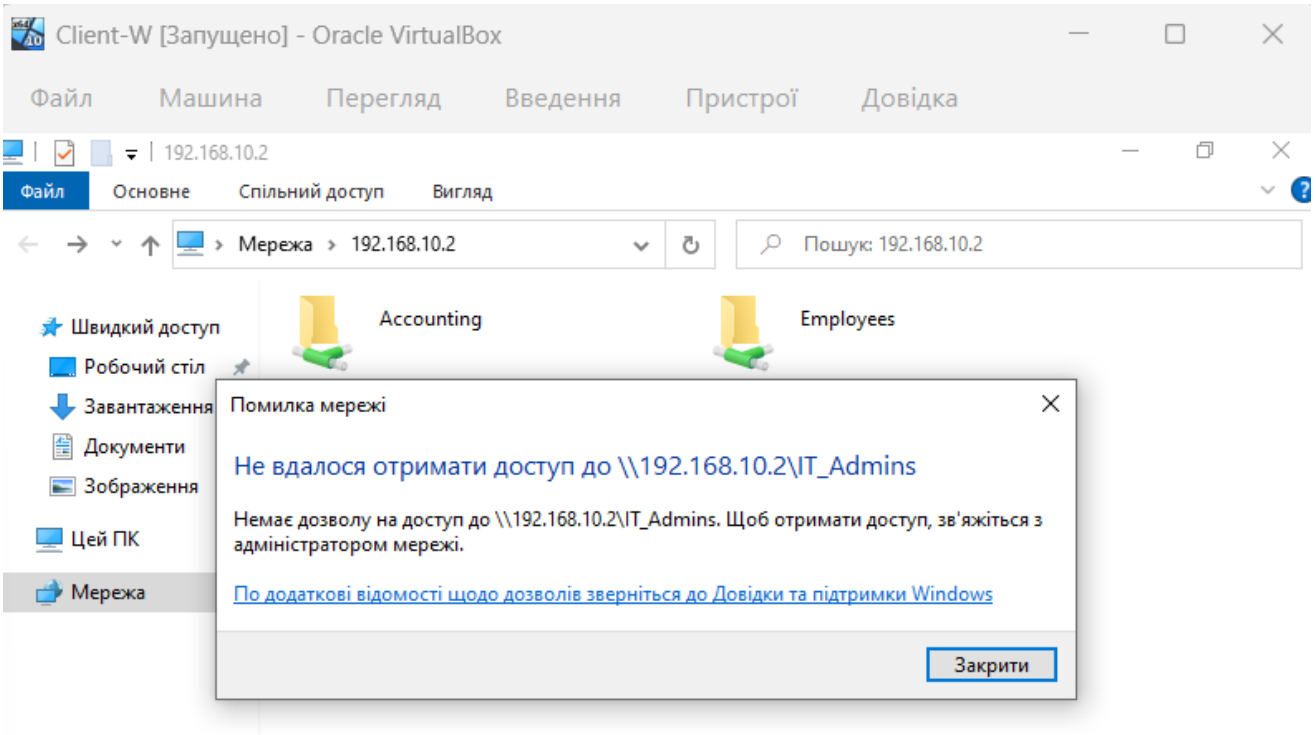


Рисунок 3.42 - Спроба доступу користувача до ресурсів групи IT_Admins

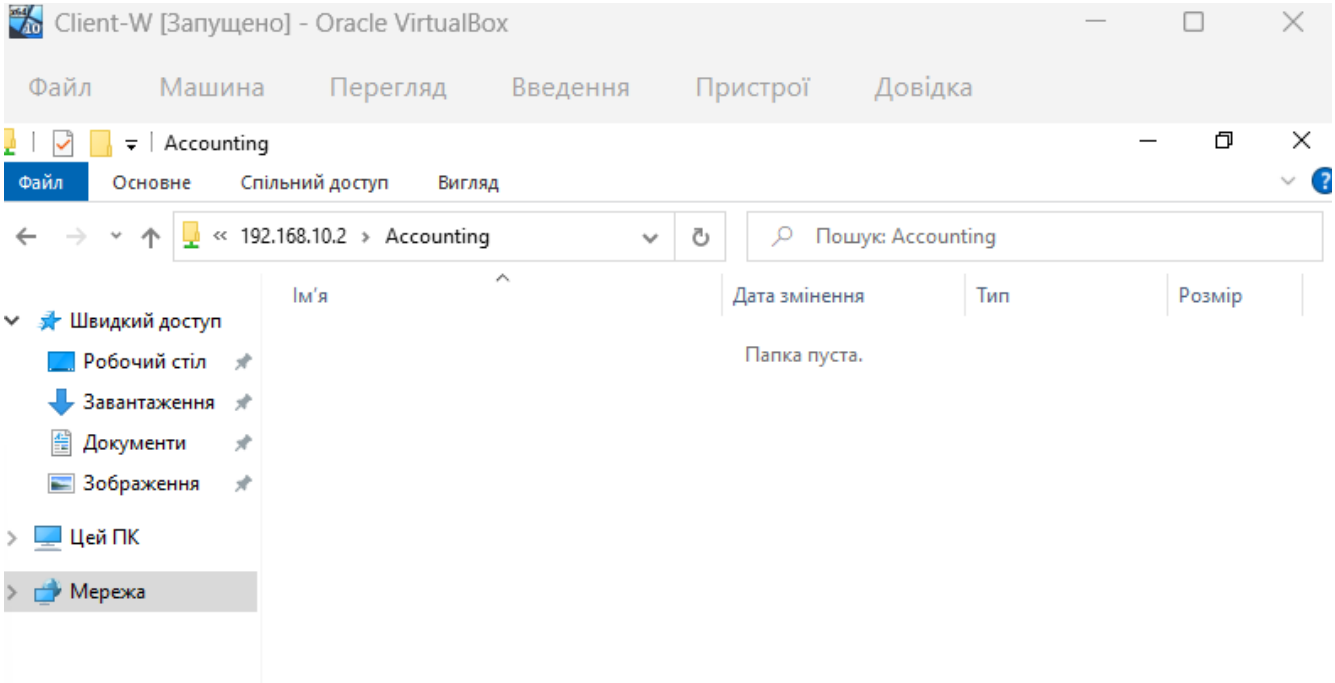


Рисунок 3.43 - Спроба доступу користувача до ресурсів групи Accounting

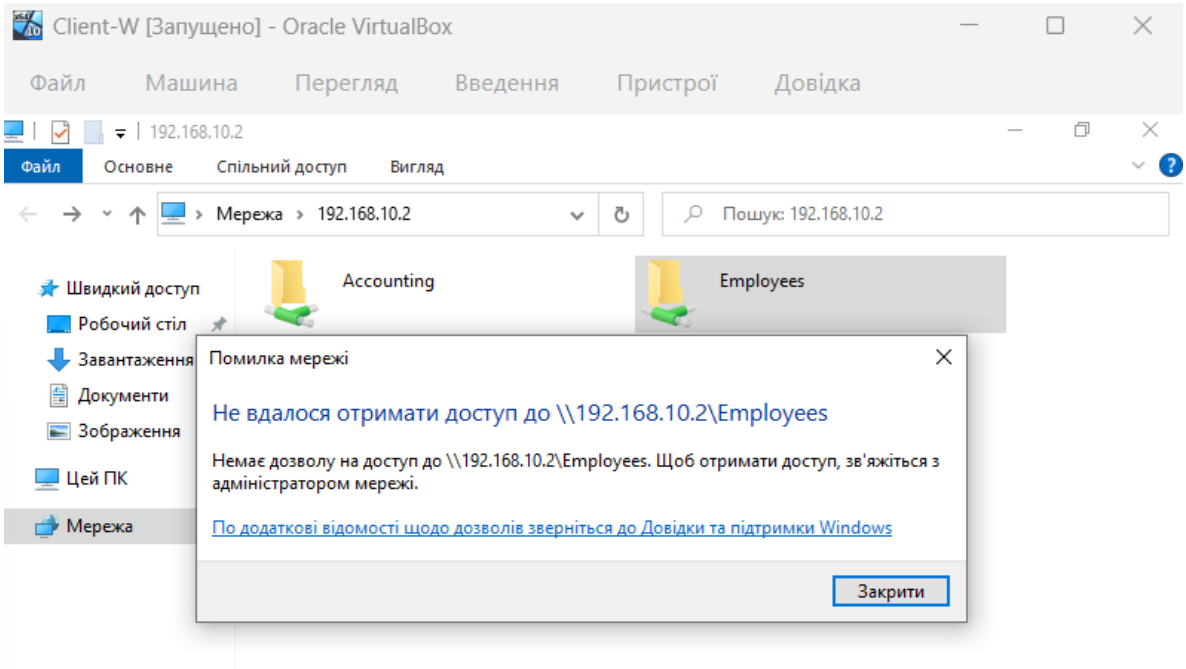


Рисунок 3.44 - Спроба доступу користувача до ресурсів групи Employees

3.4 Забезпечення відмовостійкості та резервного копіювання

Для підвищення надійності файлового сховища та захисту від втрати даних на файловому сервері FILE-SERVER було впроваджено технологію RAID 1 (дзеркало), яка забезпечує дублювання інформації на два фізичних диски. На початковому етапі до FILE-SERVER додали додатковий віртуальний жорсткий диск, як показано на рисунку 3.45.

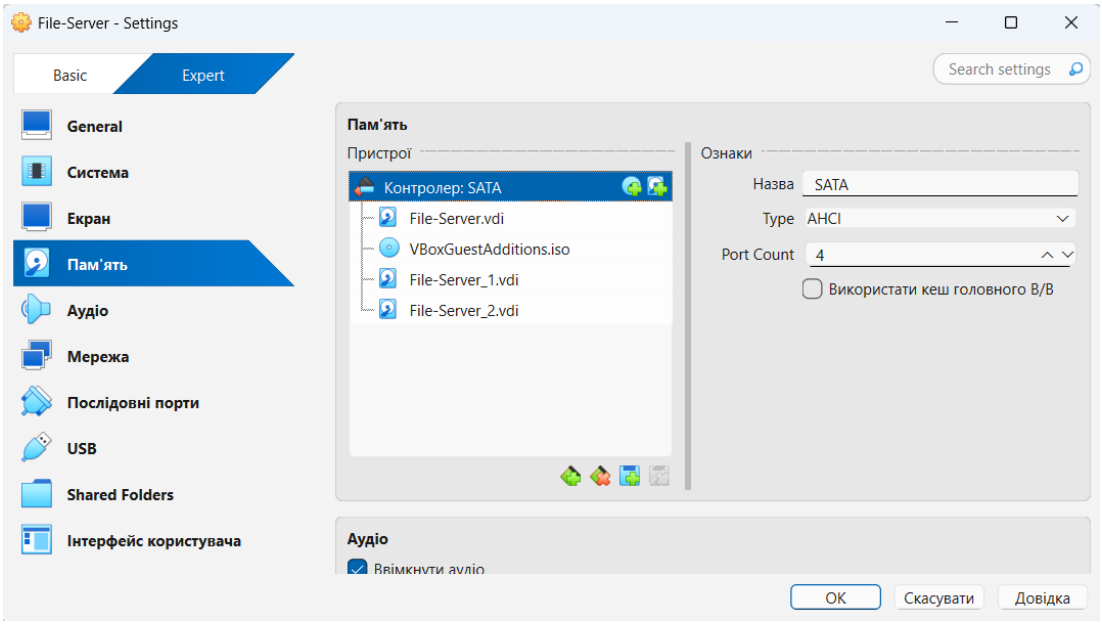


Рисунок 3.45 - Додавання додаткового віртуального диска до FILE-SERVER

Після цього диск було ініціалізовано та переведено в режим Dynamic Disk, що є необхідним для створення програмного RAID-масиву. Цей процес ілюструється на рисунках 3.46-3.47.

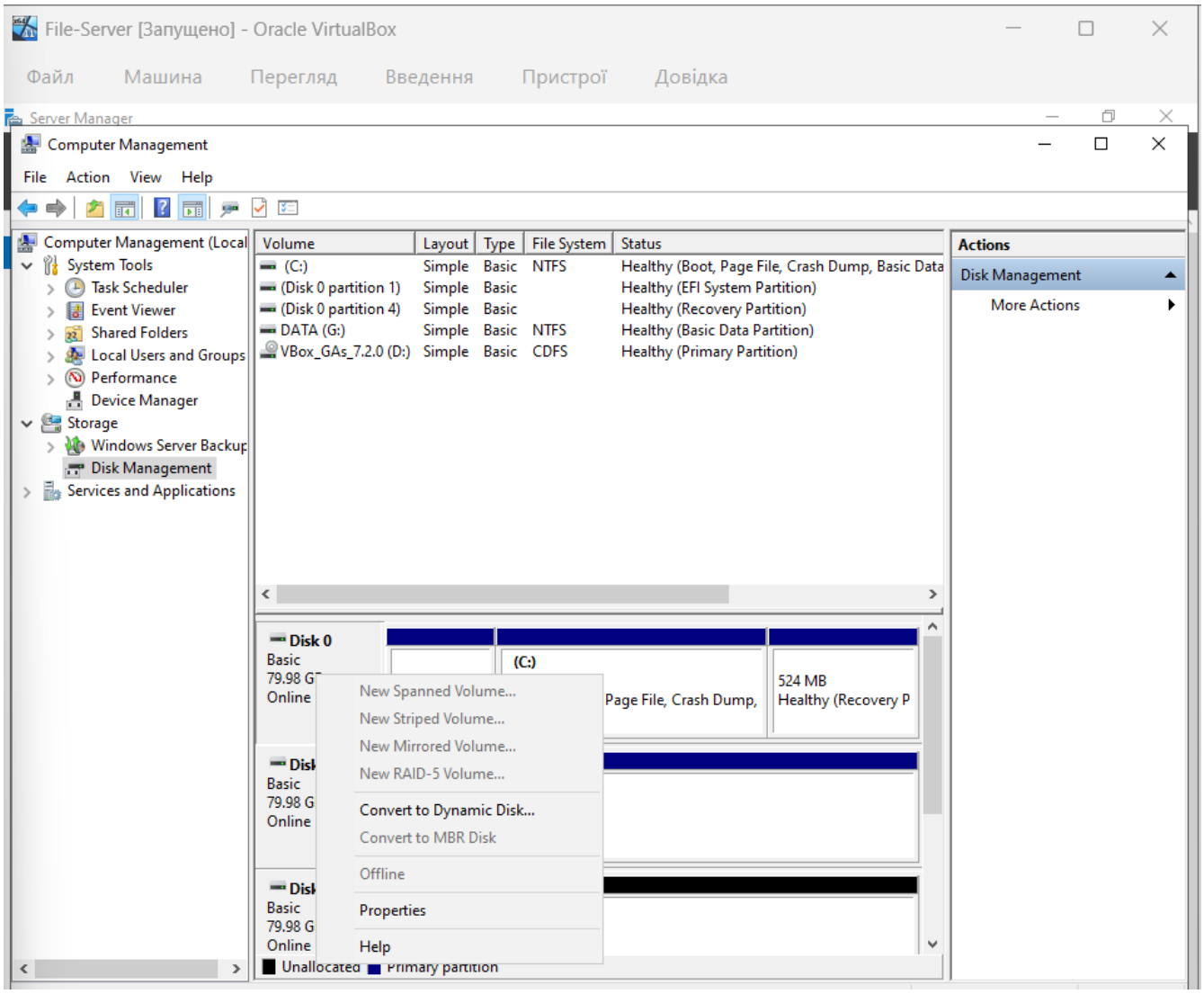


Рисунок 3.46 - Переведення диска у режим Dynamic Disk

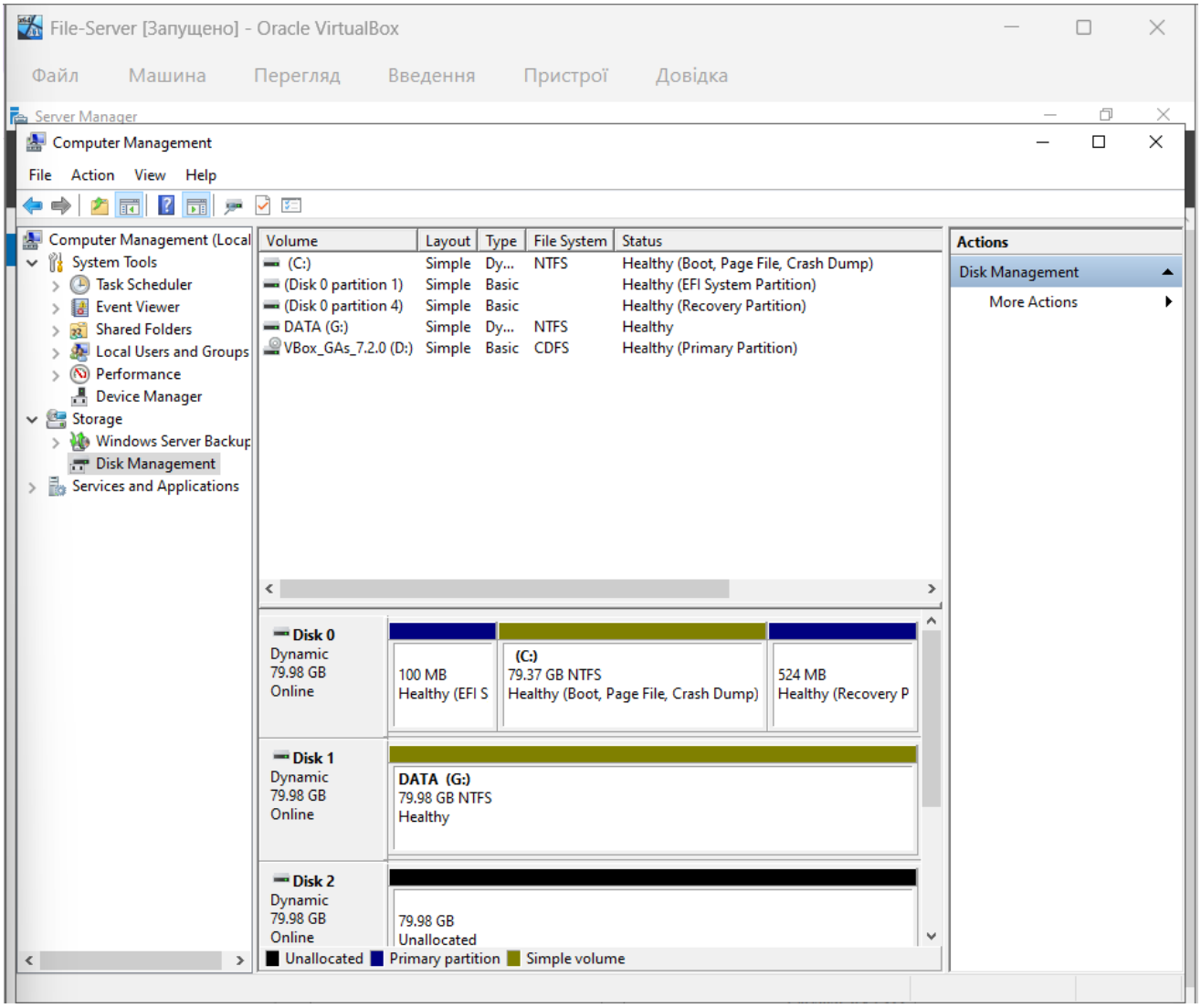


Рисунок 3.47 - Підтвердження зміни типу диска на Dynamic

Далі був створений дзеркальний том (RAID 1), після чого система розпочала синхронізацію даних між дисками. Формування та завершення створення дзеркального тому представлене на рисунках 3.48-3.49, а сам процес синхронізації - на рисунках 3.50-3.51. В результаті дані почали автоматично дублюватися на обидва носії, що забезпечує відмовостійкість файлового сервера.

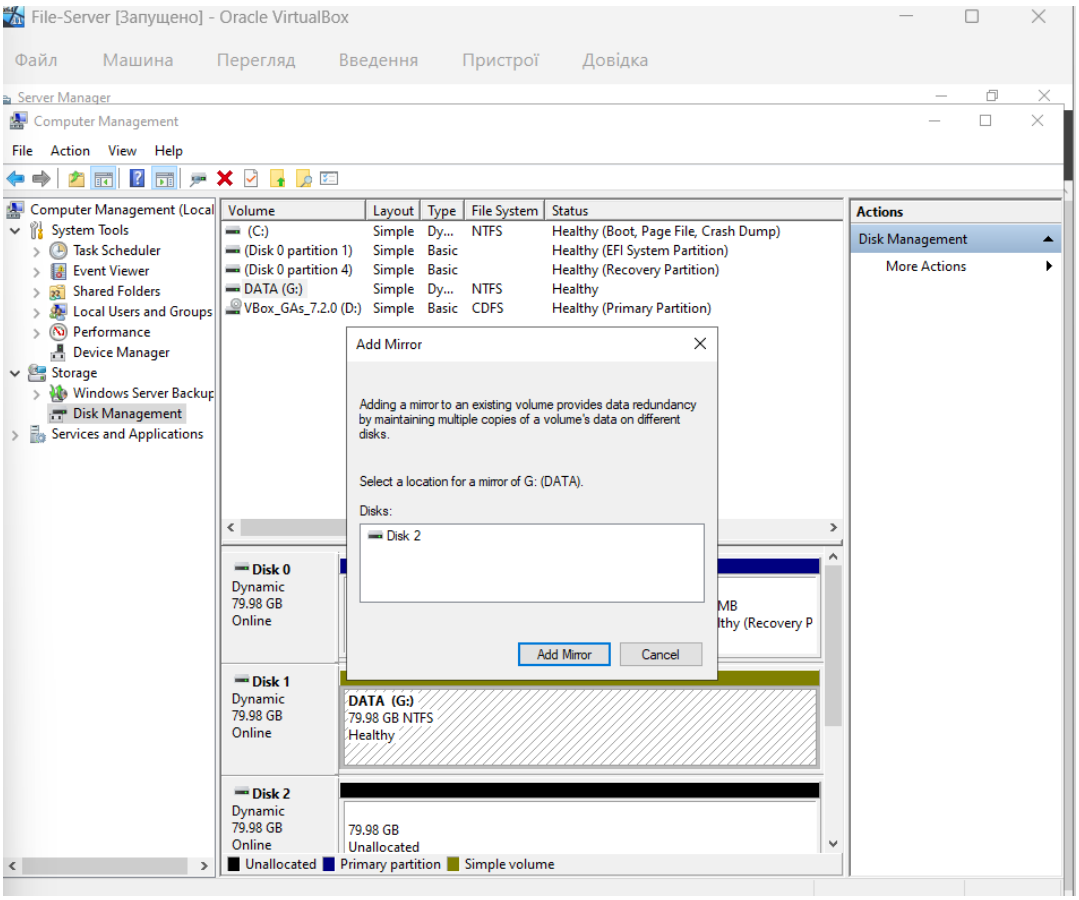


Рисунок 3.48 - Створення дзеркального тому RAID 1

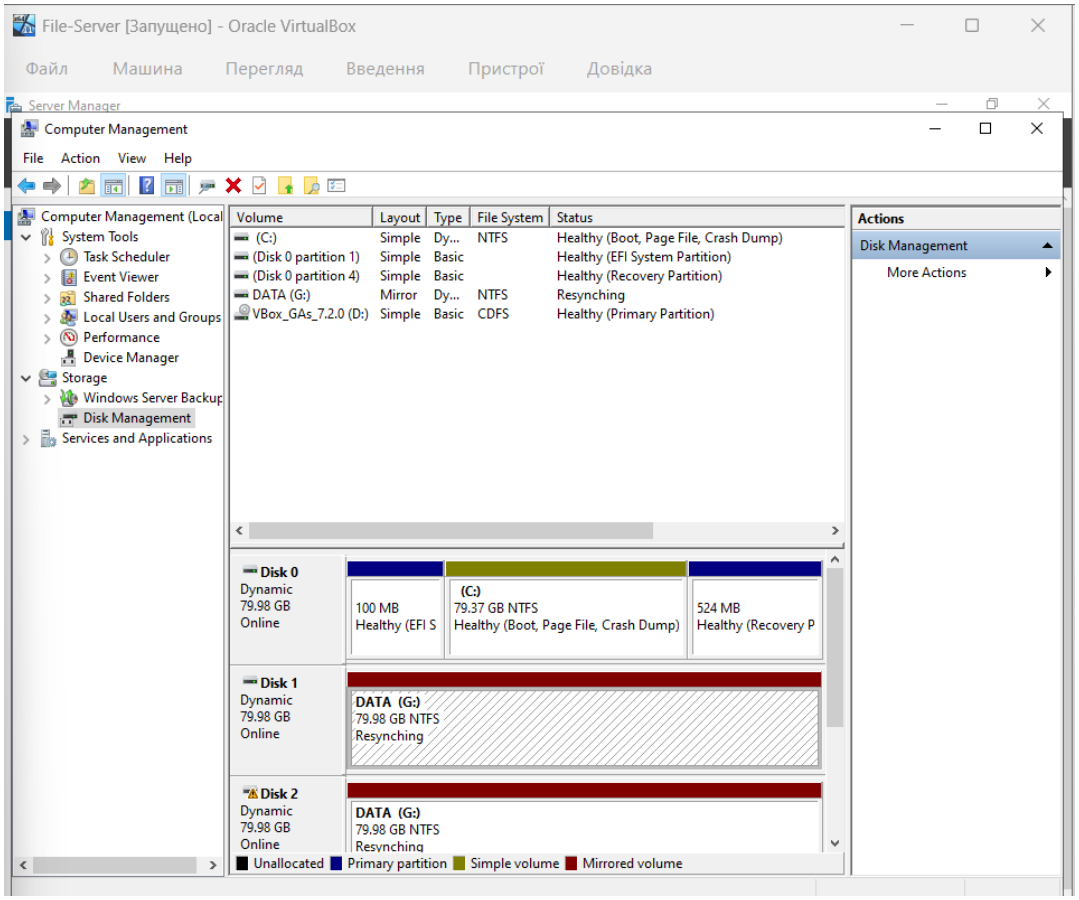


Рисунок 3.49 - Завершення створення RAID 1 (Mirror Volume)

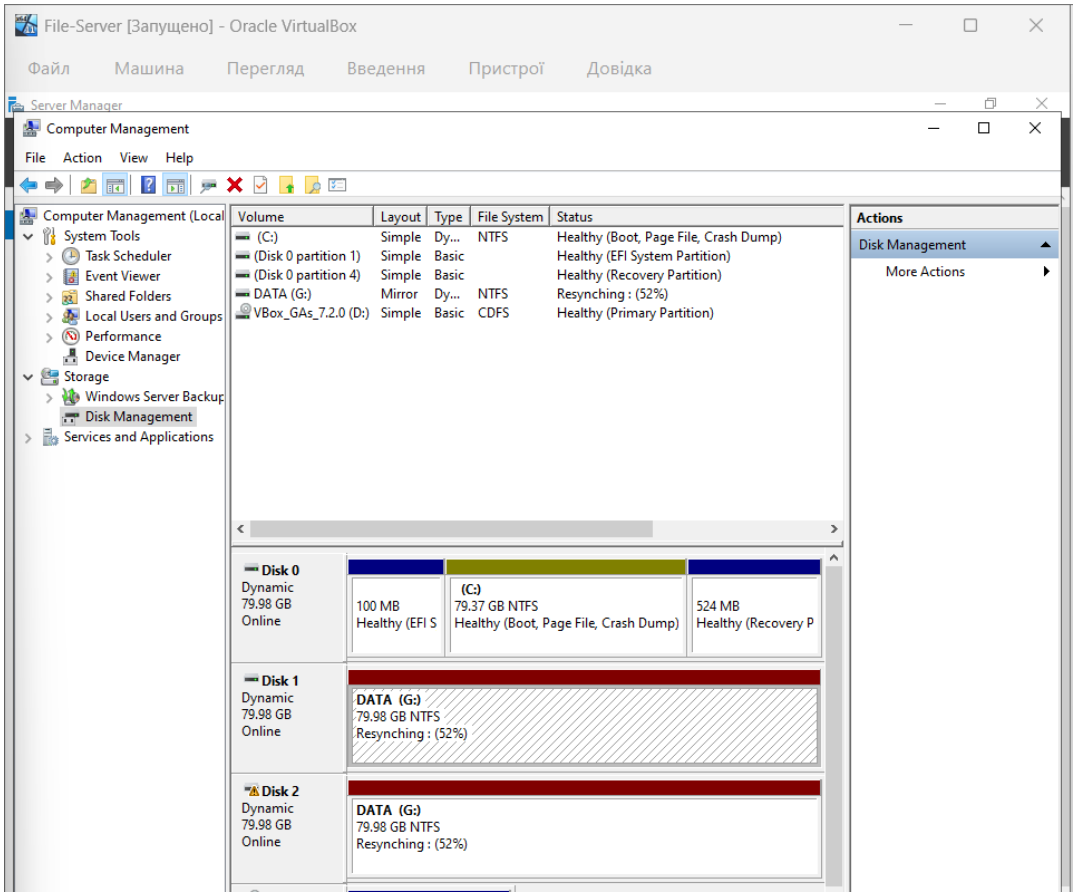


Рисунок 3.50 - Процес синхронізації даних RAID 1

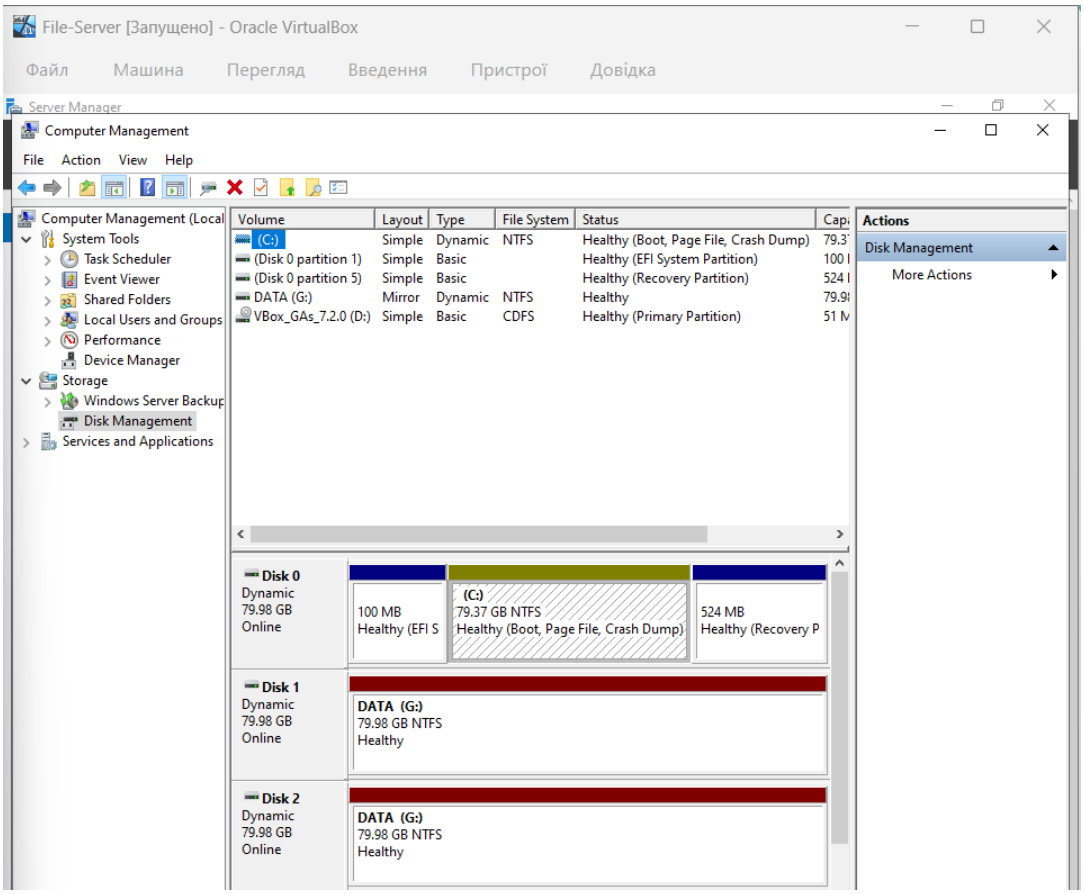


Рисунок 3.51 - Завершення синхронізації дзеркального масиву NAS-SERVER

Для організації резервного копіювання було налаштовано окремий сервер NAS-SERVER, який функціонує як віддалене мережне сховище. Його підключення до корпоративної мережі продемонстроване на рисунку 3.52, а перевірка доступності сервера - на рисунку 3.53.

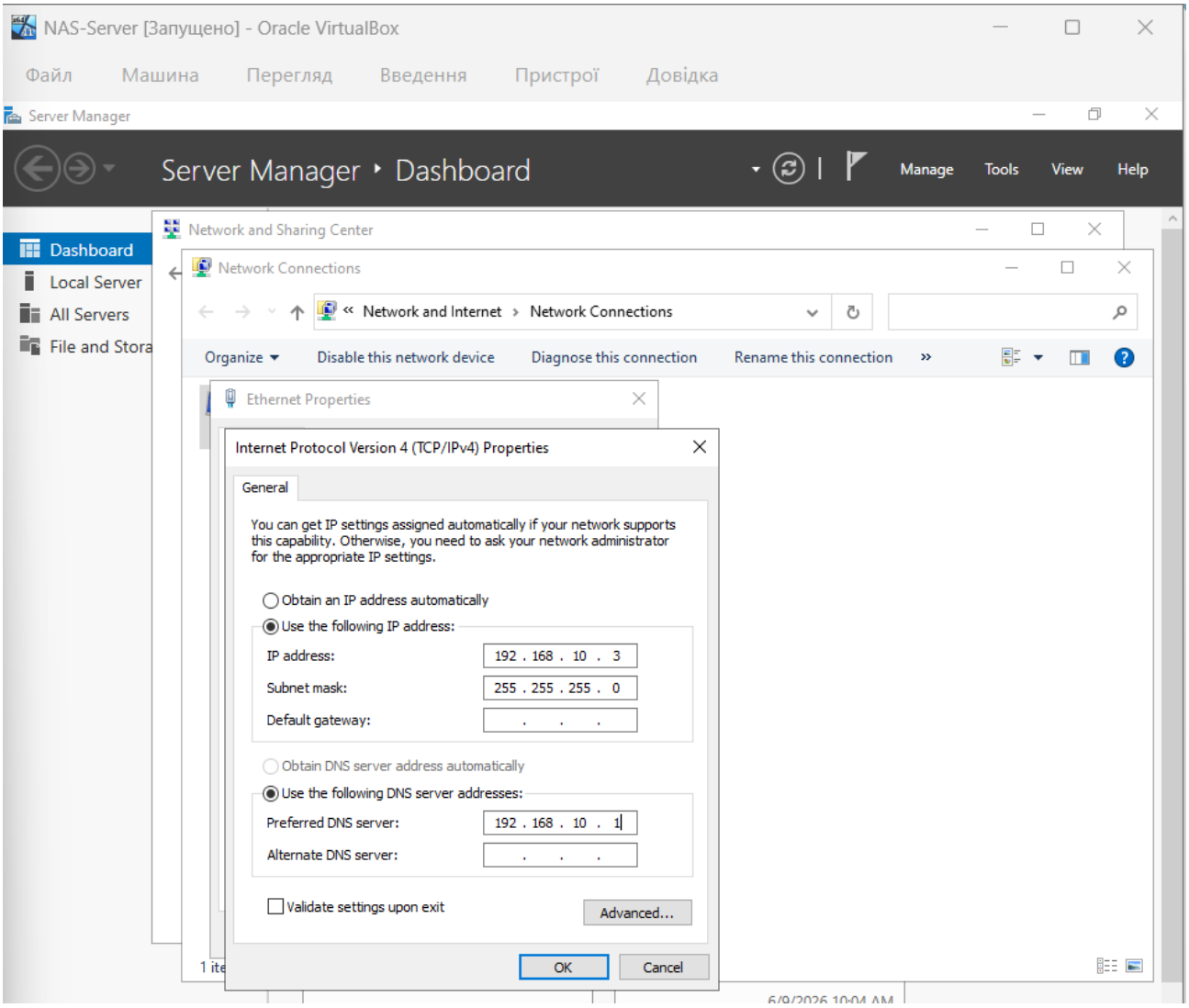


Рисунок 3.52 - Підключення NAS-SERVER до корпоративної мережі

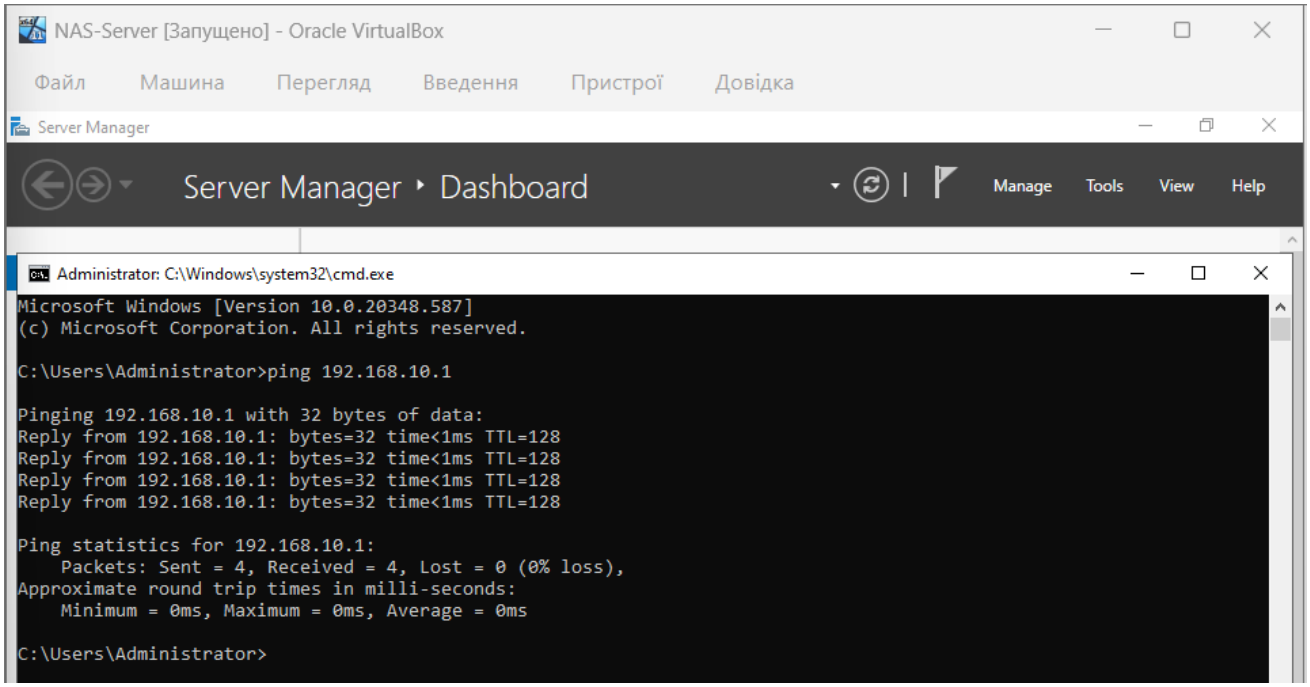


Рисунок 3.53 - Перевірка доступності NAS-SERVER (Ping)

На NAS-SERVER була створена структура каталогів для зберігання резервних копій, зокрема папка Backup з підкаталогами FILE-SERVER та Test, що показано на рисунку 3.54. Після цього було налаштовано спільний доступ до мережного ресурсу (SMB), як видно на рисунку 3.55.

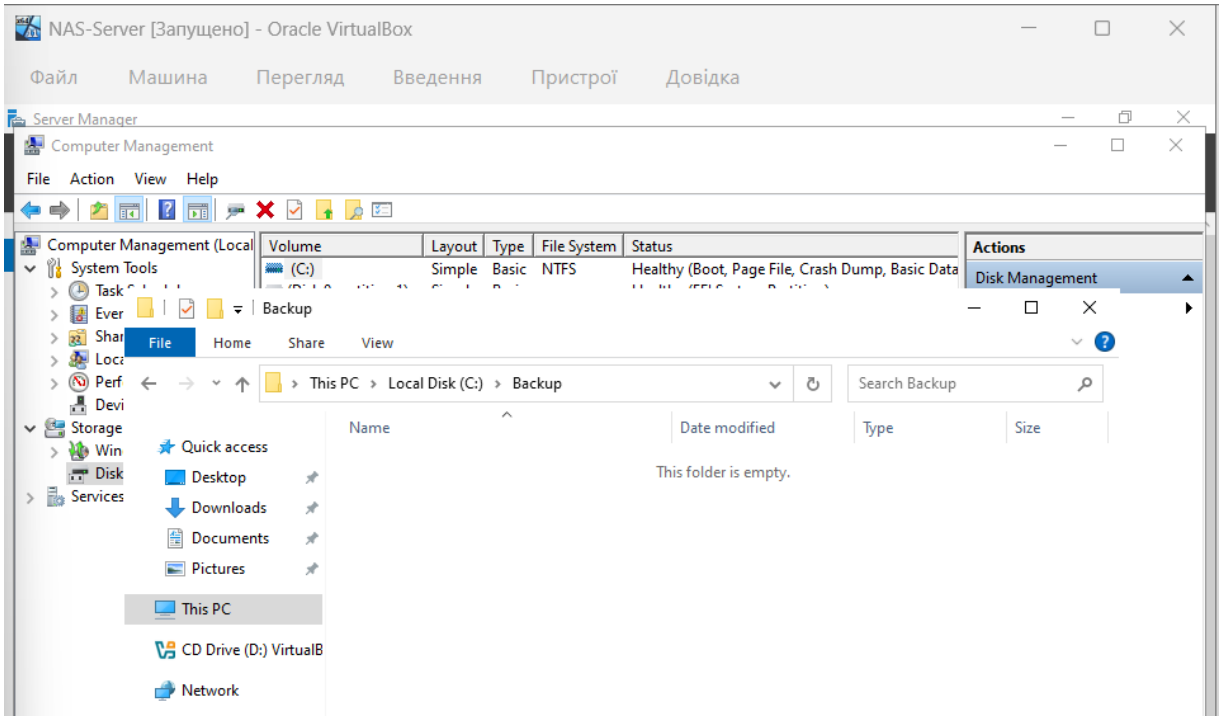


Рисунок 3.54 - Створення структури резервного сховища на NAS

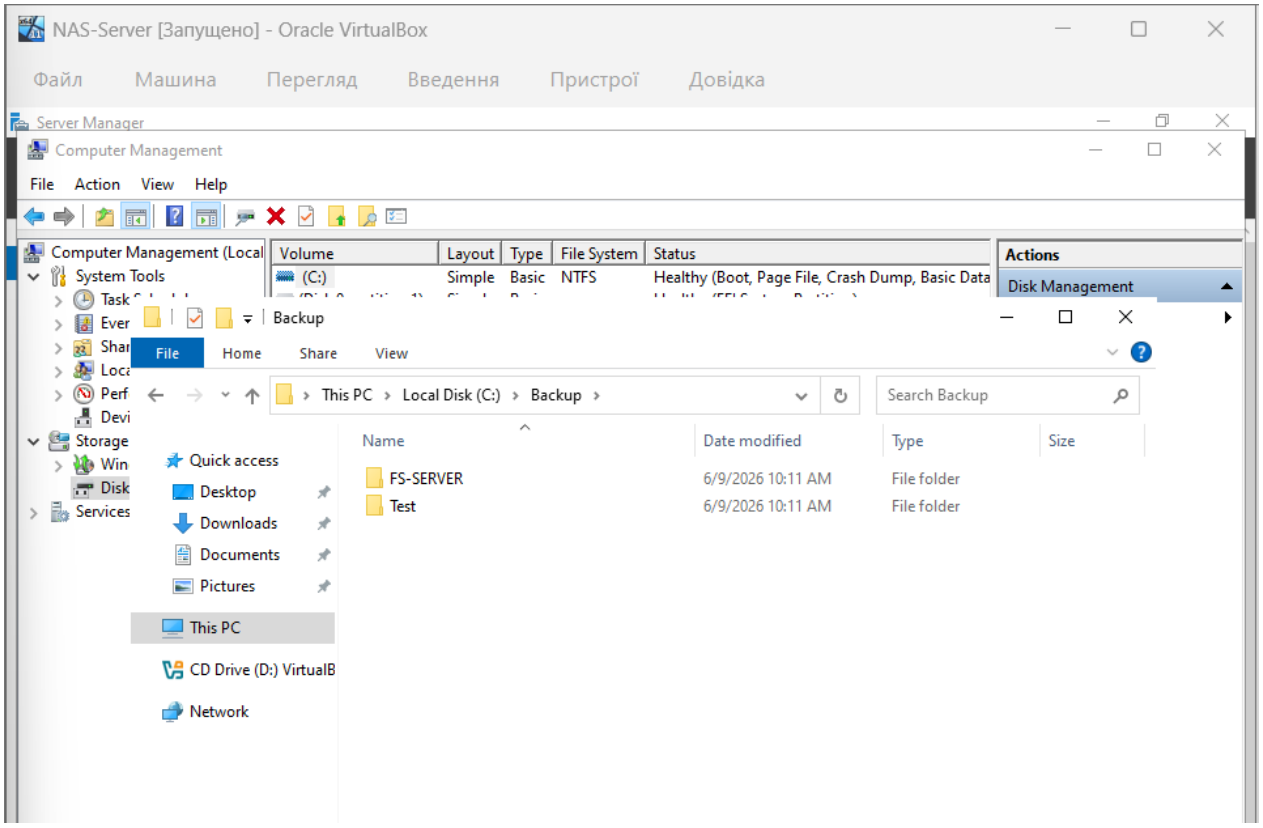


Рисунок 3.55 - Налаштування SMB-спільного доступу

З метою покращення безпеки були змінені стандартні права доступу: групу Everyone видалено, залишивши доступ лише для адміністраторів. Додаткові налаштування безпеки відображені на вкладці Security у рисунку 3.56.

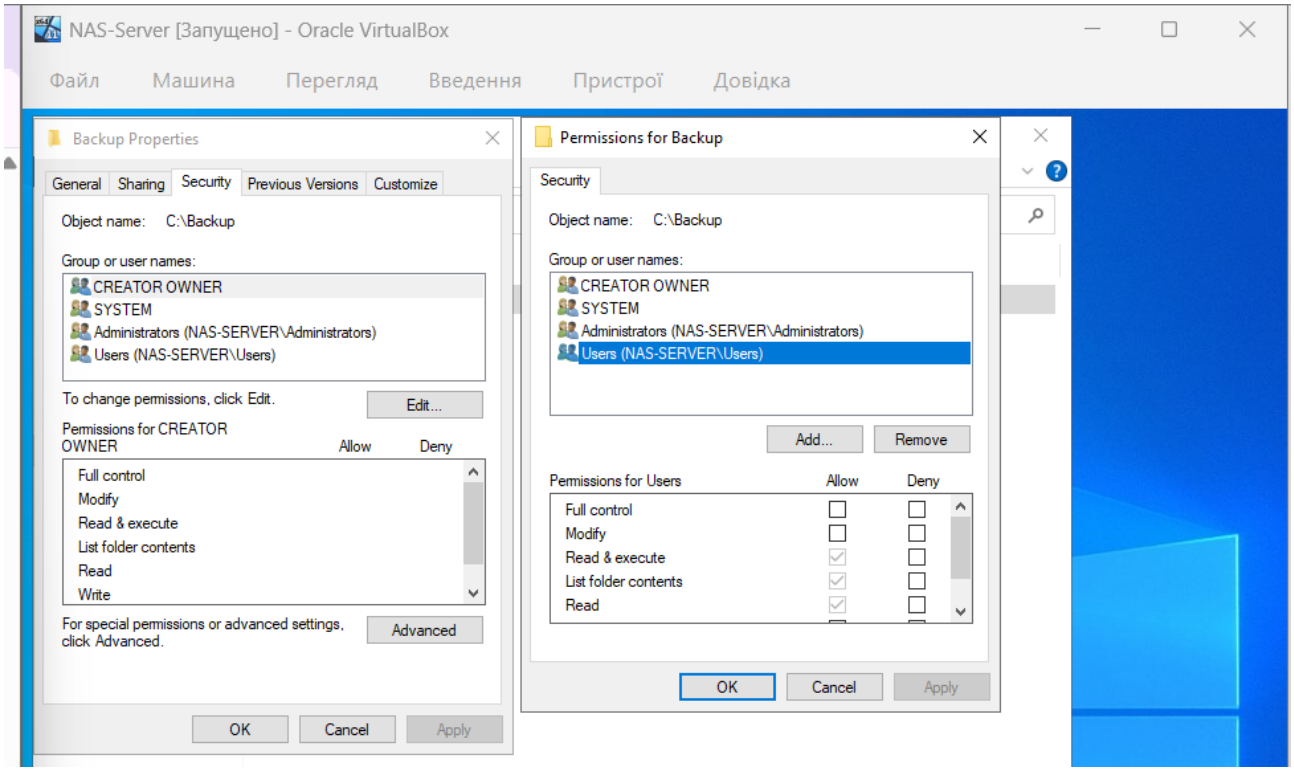


Рисунок 3.56 - Налаштування прав доступу (Security вкладка)

Для перевірки функціональності NAS-SERVER був створений тестовий файл на файловому сервері FILE-SERVER, після чого його копія успішно з'явилася у віддаленому сховищі, що підтверджено на рисунках 3.57-3.58.

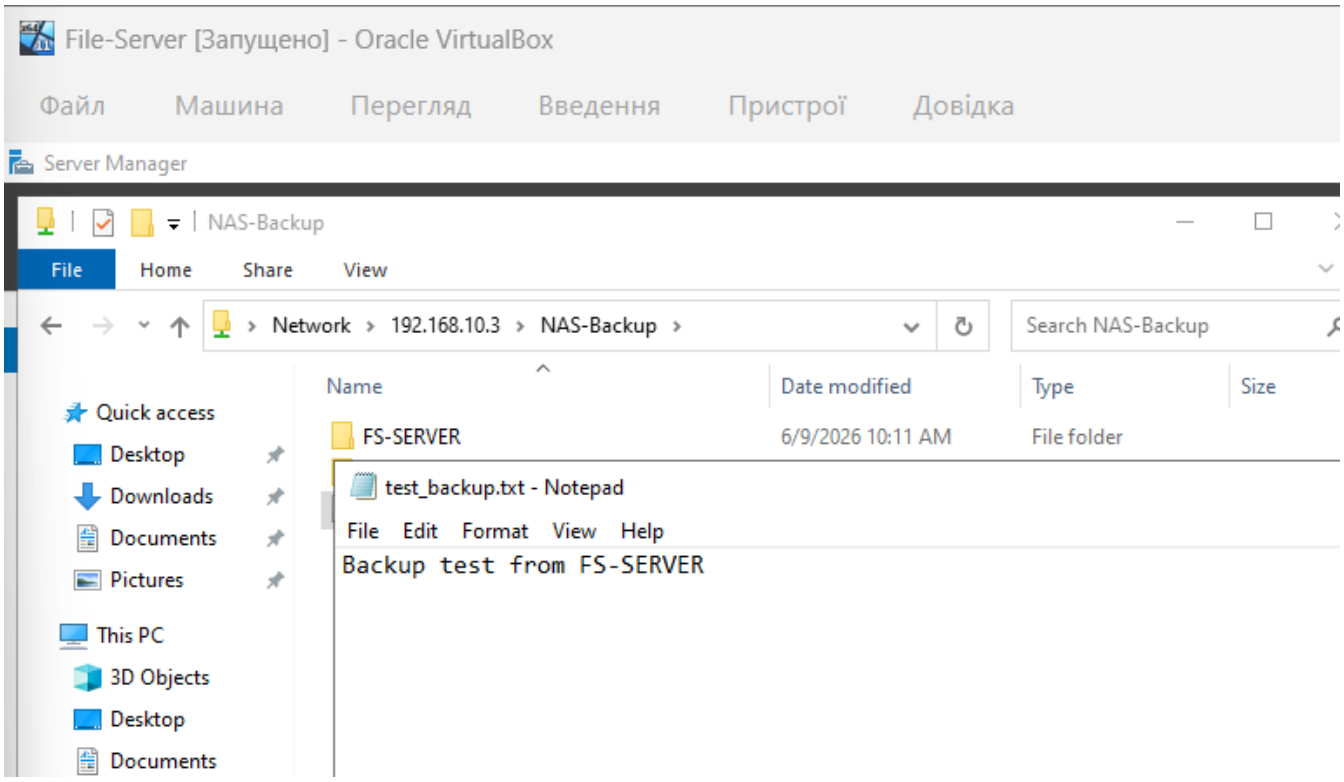


Рисунок 3.57 - Створення тестового файлу на FILE-SERVER

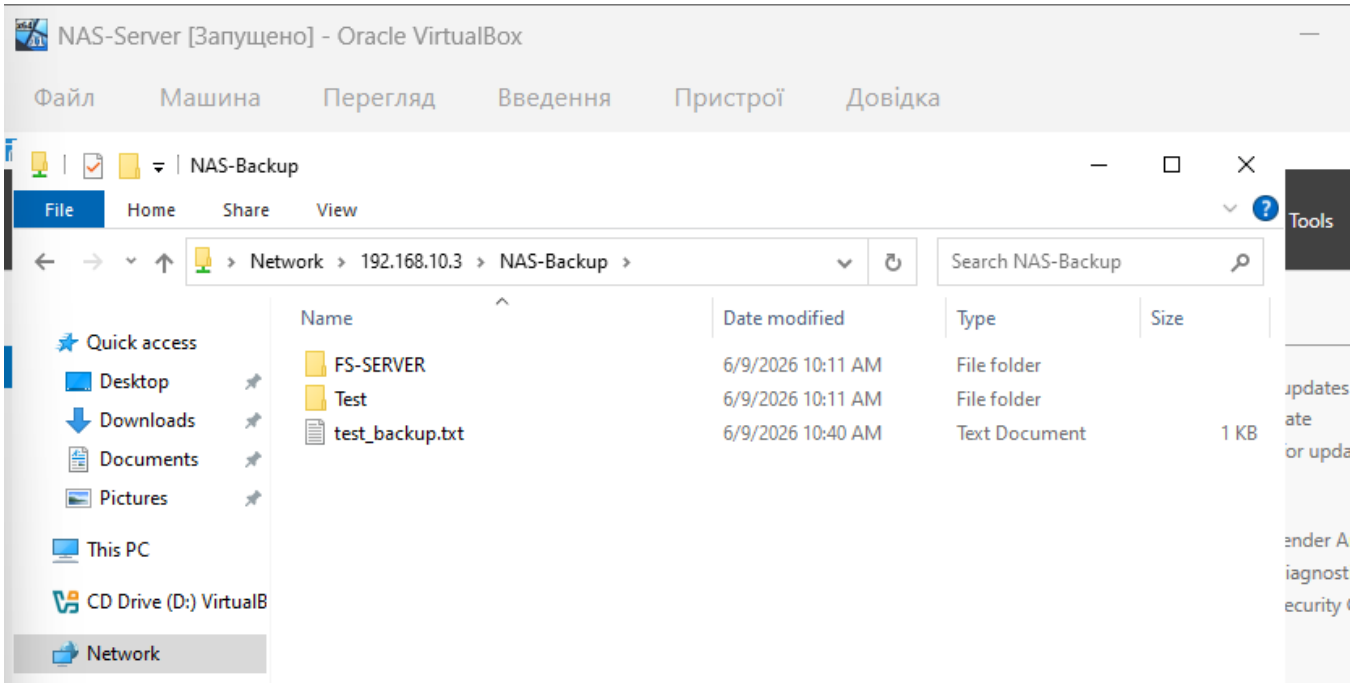


Рисунок 3.58 - Відображення файлу на NAS-SERVER

Резервне копіювання для FILE-SERVER здійснювалося за допомогою інструмента Windows Server Backup. Резервні копії зберігалися на NAS-SERVER через мережний ресурс NAS-Backup із використанням облікового запису backupuser. Запуск інструмента Windows Server Backup проілюстровано на рисунку 3.59.

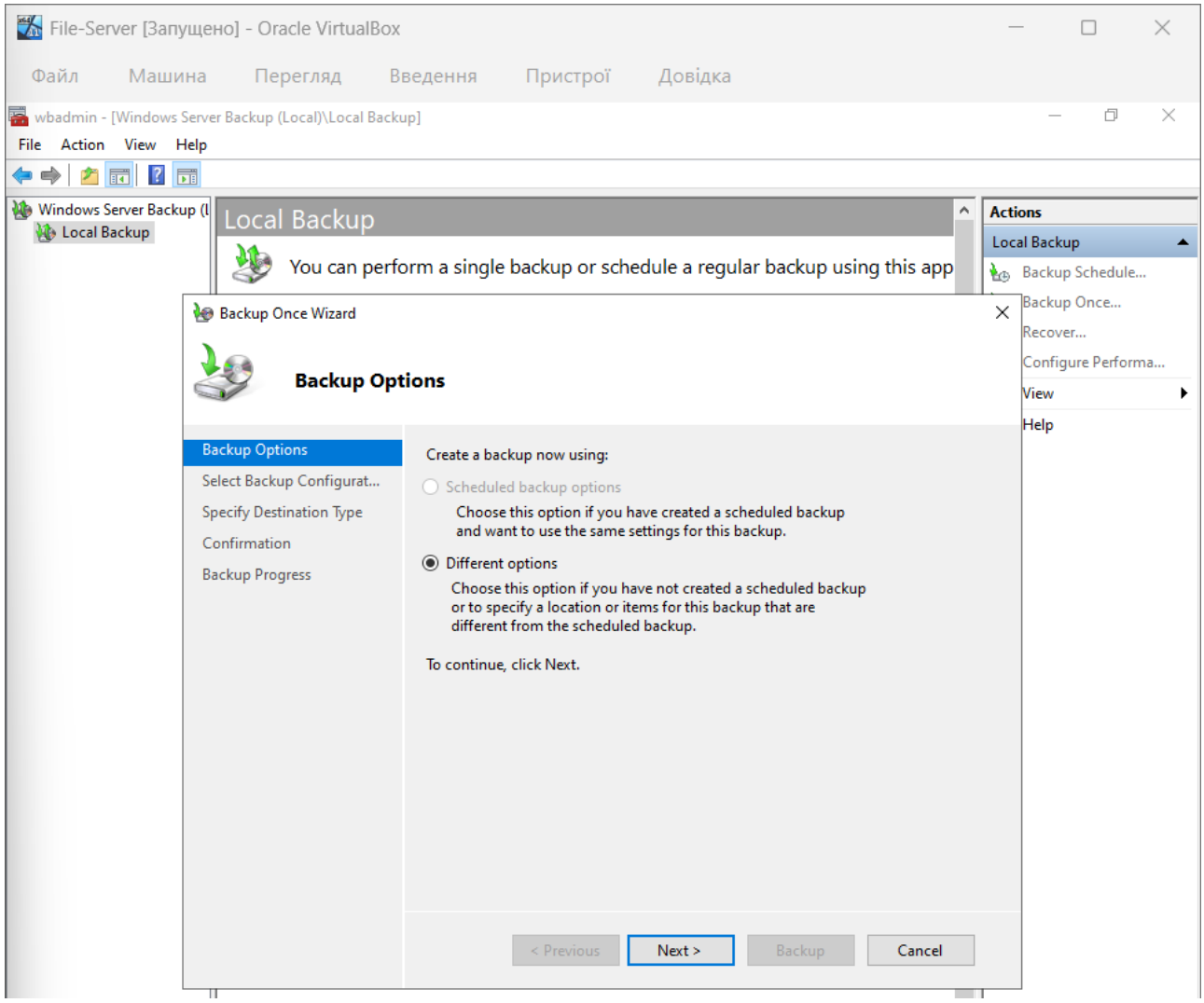


Рисунок 3.59 - Запуск Windows Server Backup

Під час налаштування був обраний режим Custom, визначено необхідні дані для резервування (папки IT_Admins, Employees, Accounting або D:\Shares) і вказано віддалене мережне сховище \\NAS-SERVER\NAS-Backup, що видно на рисунках 3.60-3.61.

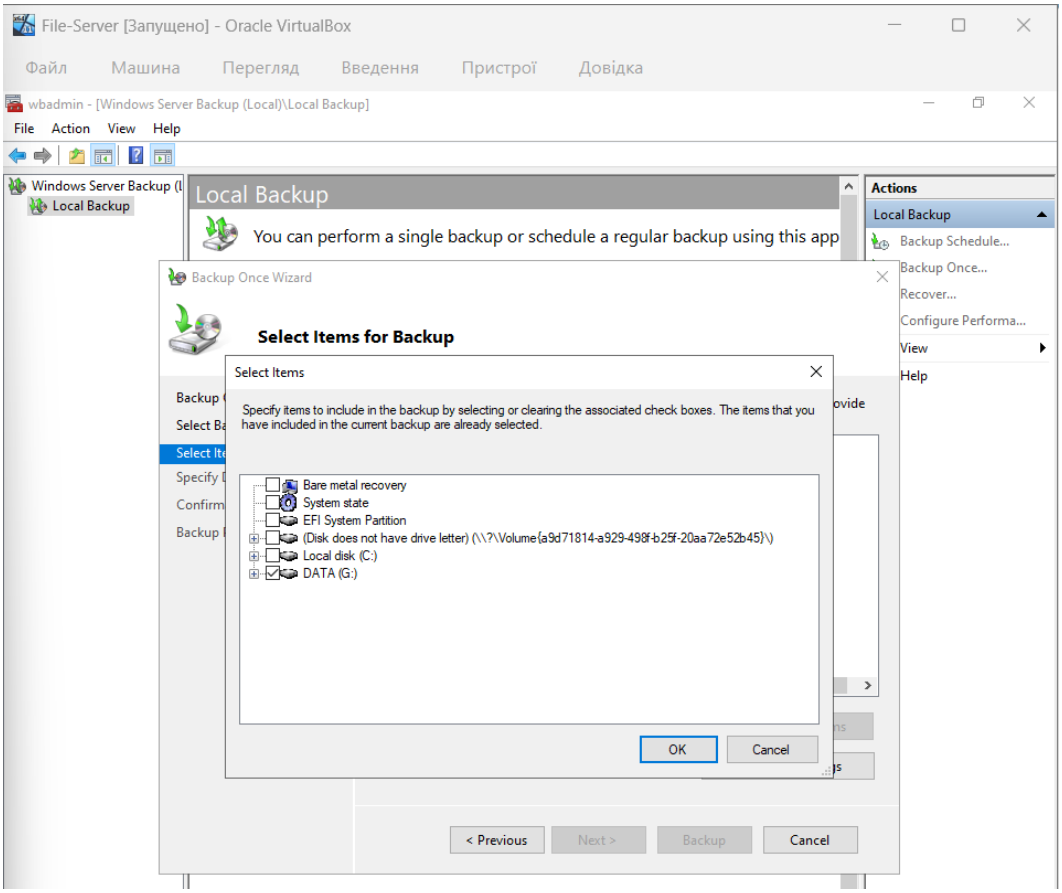


Рисунок 3.60 - Вибір даних для резервного копіювання

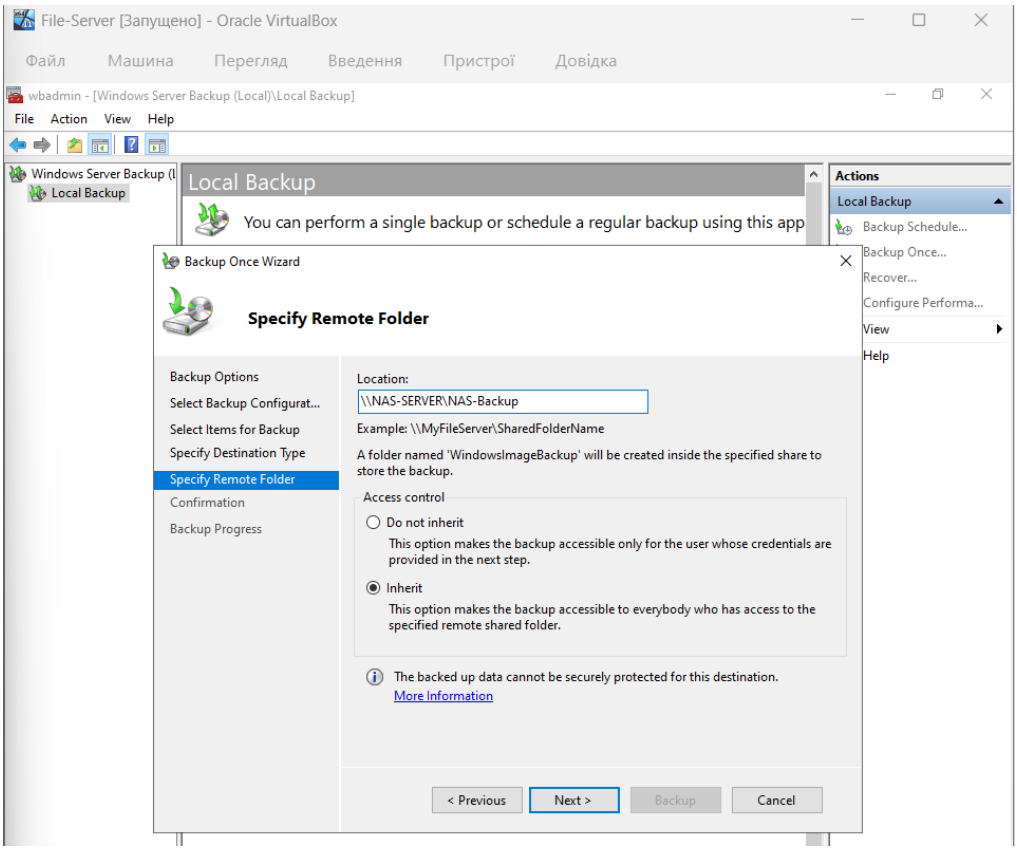


Рисунок 3.61 - Налаштування віддаленого сховища NAS

Після запуску процесу резервного копіювання система створила структуру WindowsImageBackup на NAS-сервері, що підтверджено малюнком 3.62; завершення процесу резервування показане у рисунку 3.63.

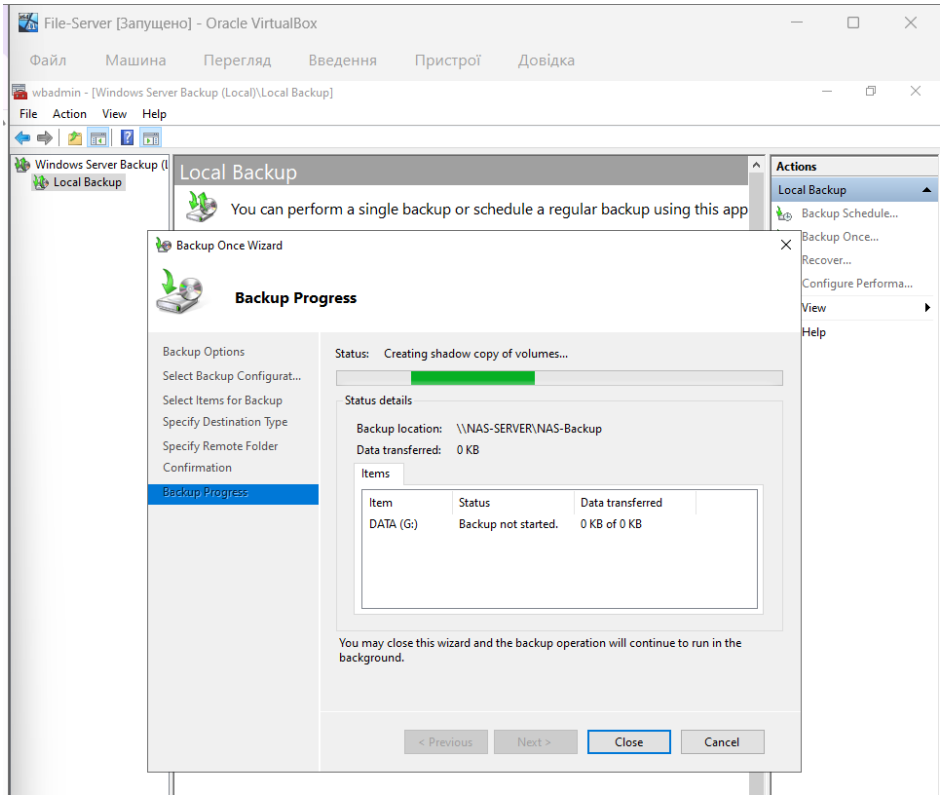


Рисунок 3.62 - Створення структури WindowsImageBackup

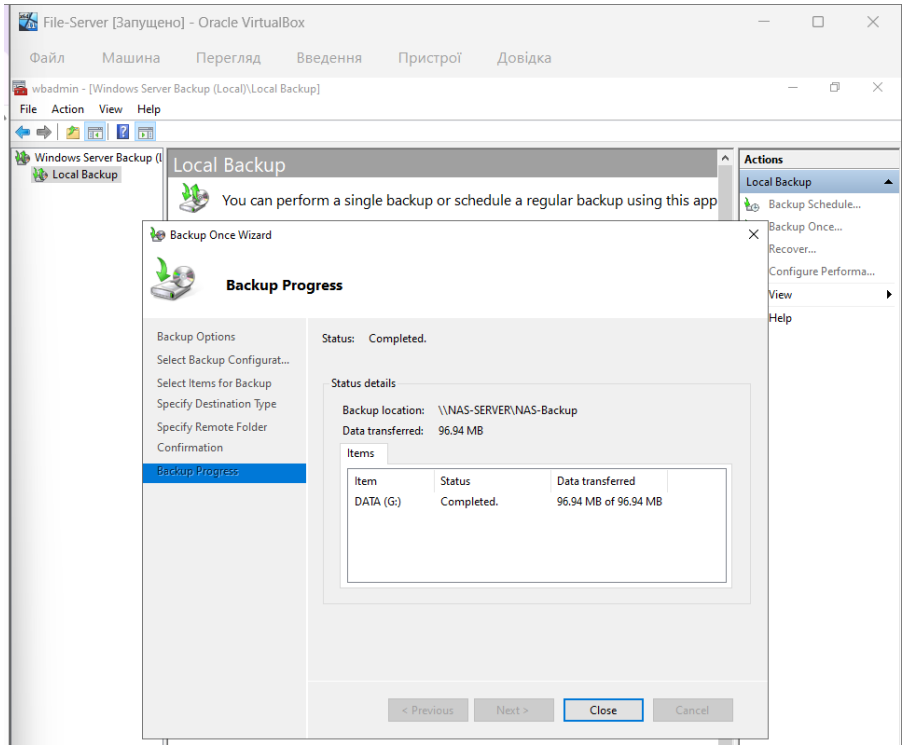


Рисунок 3.63 - Завершення процесу резервного копіювання

Для перевірки функціональності був створений тестовий файл test_backup.txt, який після виконання резервного копіювання успішно з'явився у резервній копії, про що свідчить малюнок 3.64.

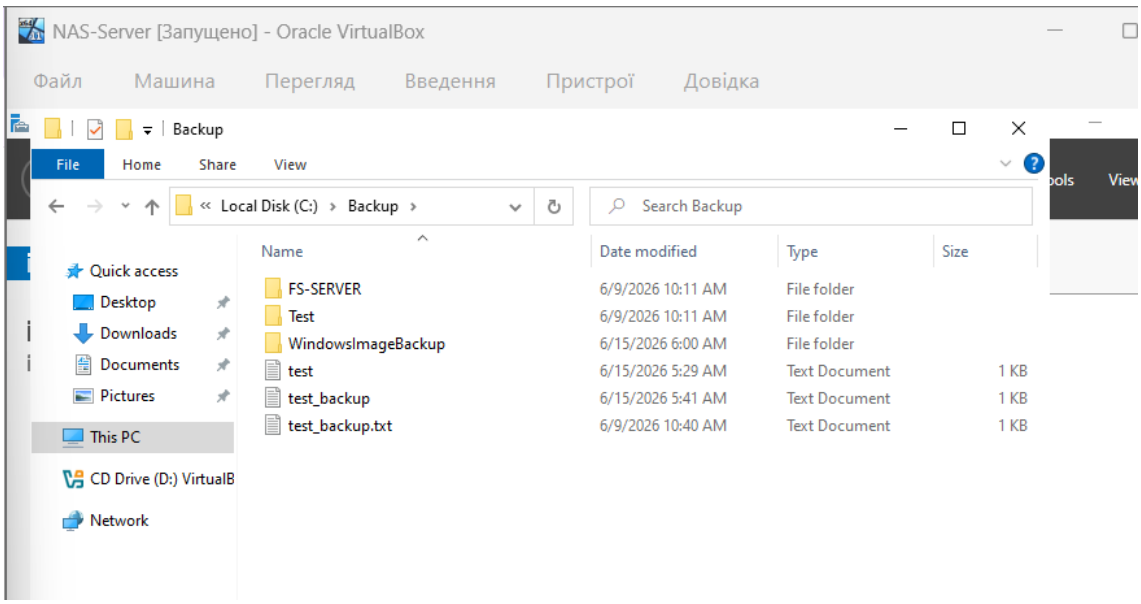


Рисунок 3.64 - Перевірка наявності резервної копії (test_backup.txt)

Отже, було підтверджено коректну роботу механізму резервного копіювання та взаємодії між FILE-SERVER і NAS-SERVER.

3.5 Підключення корпоративних робочих станцій (Windows та Linux) та тестування системи

Для перевірки функціональності розгорнутої корпоративної файлової інфраструктури було здійснено підключення корпоративних робочих станцій до мережі CORPNET.LOCAL. Основне завдання цього етапу полягало в тестуванні доступу користувачів до файлових ресурсів, перевірці коректності роботи SMB-протоколу та підтвердженні можливості використання файлового сховища з різних операційних систем.

Особлива увага була приділена кросплатформеному доступу, оскільки в корпоративному середовищі можуть використовуватися робочі станції з різними ОС. Для цього було підключено Client-L Ubuntu до файлового сервера FILE-SERVER, який функціонує на базі Windows Server і забезпечує доступ до спільних ресурсів через SMB-протокол.

На початковому етапі були перевірені мережні параметри корпоративної станції Ubuntu за допомогою команди ip a. В результаті було отримано IP-адресу та підтверджено його належність до корпоративного сегмента мережі 192.168.10.0/24. Результати перевірки мережної конфігурації наведені на рисунку 3.65.

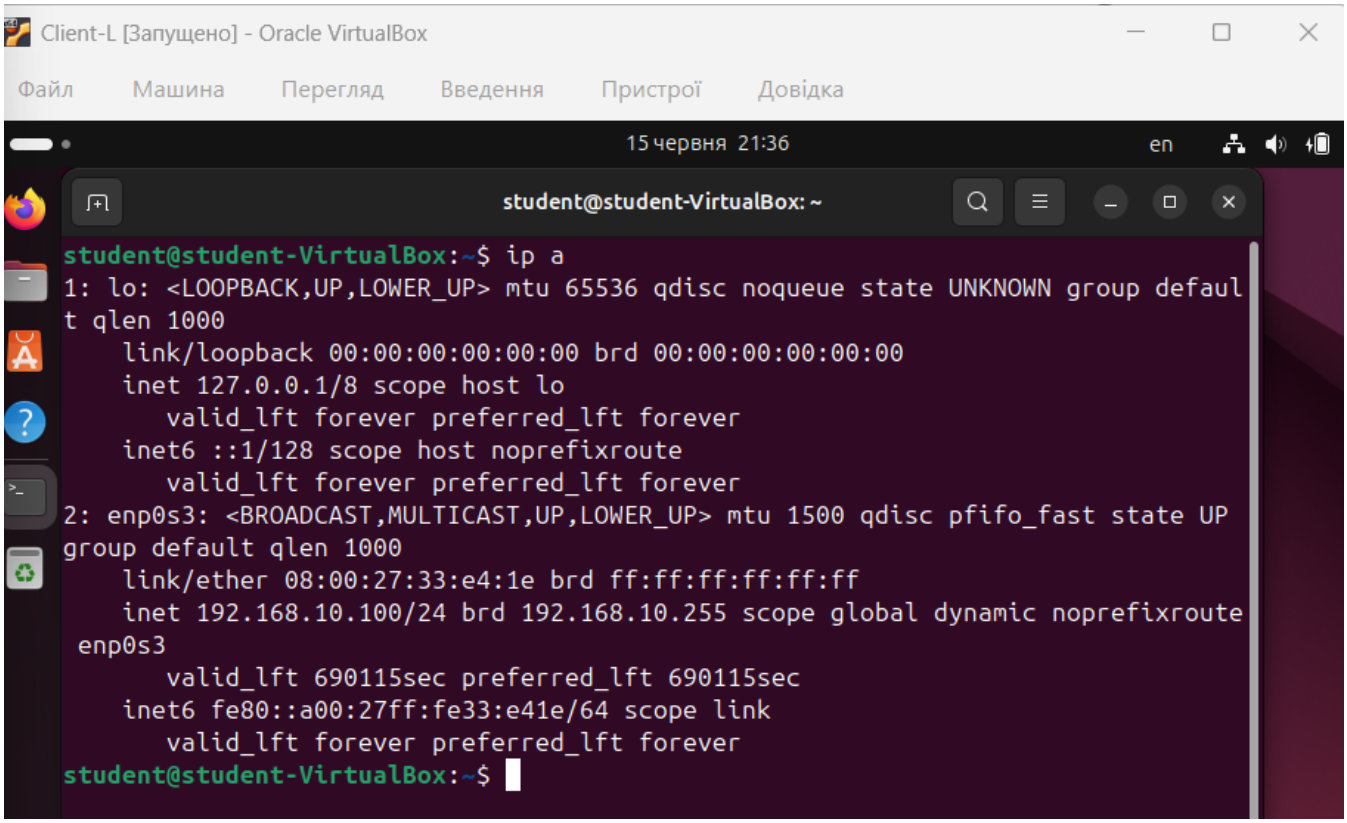


Рисунок 3.65 - Перевірка мережних параметрів Ubuntu Client

Після оцінки локальної конфігурації було проведено тестування мережної взаємодії між Ubuntu Client та контролером домену DC-SERVER. Для цього була використана команда ping 192.168.10.1, що дозволила перевірити доступність контролера домену в мережі. Успішно отримані відповіді підтвердили правильність підключення корпоративної станції до корпоративної інфраструктури, що показано на рисунку 3.66.

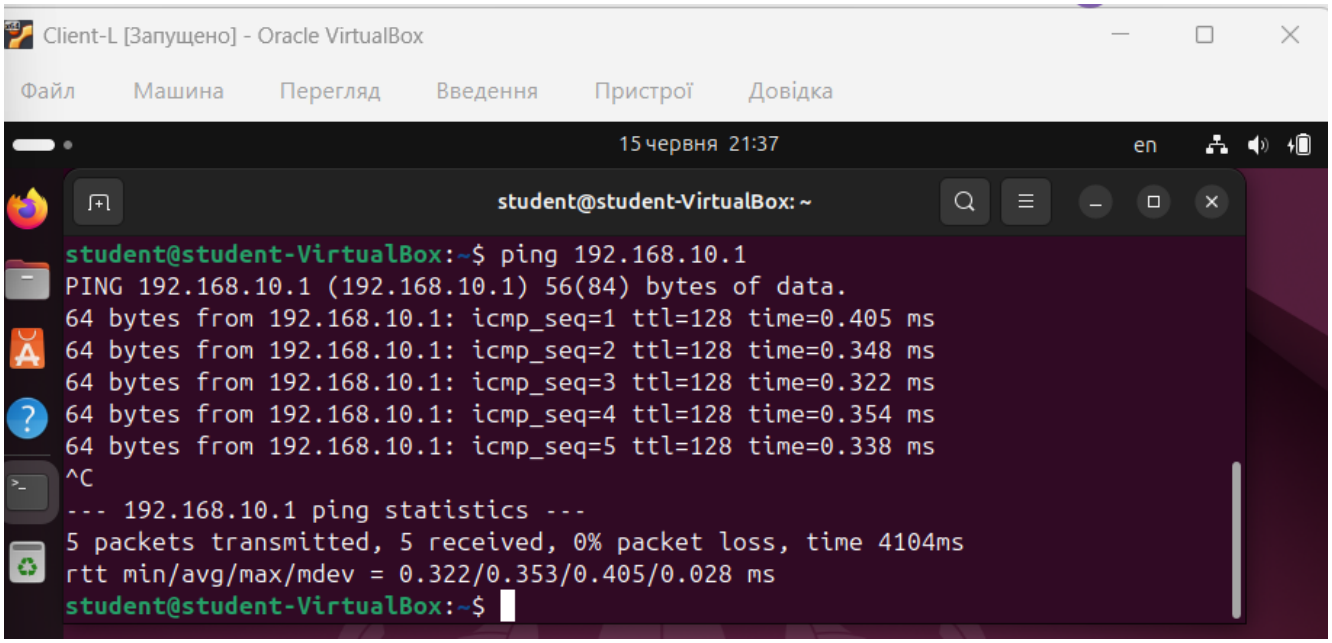


Рисунок 3.66 - Перевірка мережного з'єднання Ubuntu Client з DC-SERVER

Наступним кроком стало тестування доступності файлового сервера FILE-SERVER. За допомогою команди ping 192.168.10.2 було перевірено з'єднання між Client-L і сервером даних. Позитивний результат тестування засвідчив, що Ubuntu Client має мережний доступ до файлового сховища, як показано на рисунку 3.67.

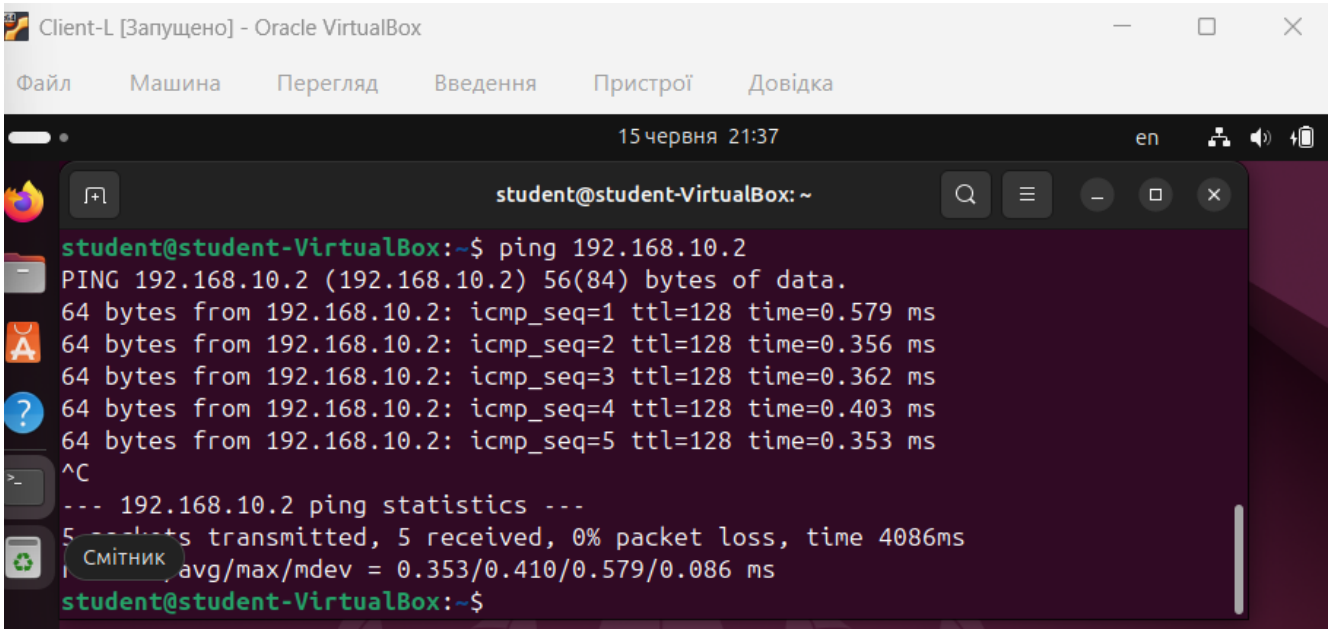


Рисунок 3.67 - Перевірка доступності файлового сервера FILE-SERVER

Для роботи з файловими ресурсами Windows у середовищі Linux були встановлені необхідні пакети smbclient та cifs-utils, які забезпечують підтримку

протоколу SMB/CIFS. Після цього була виконана перевірка доступних мережних ресурсів файлового сервера за допомогою команди smbclient -L //192.168.10.2 -U CORPNET\i.petrenko.

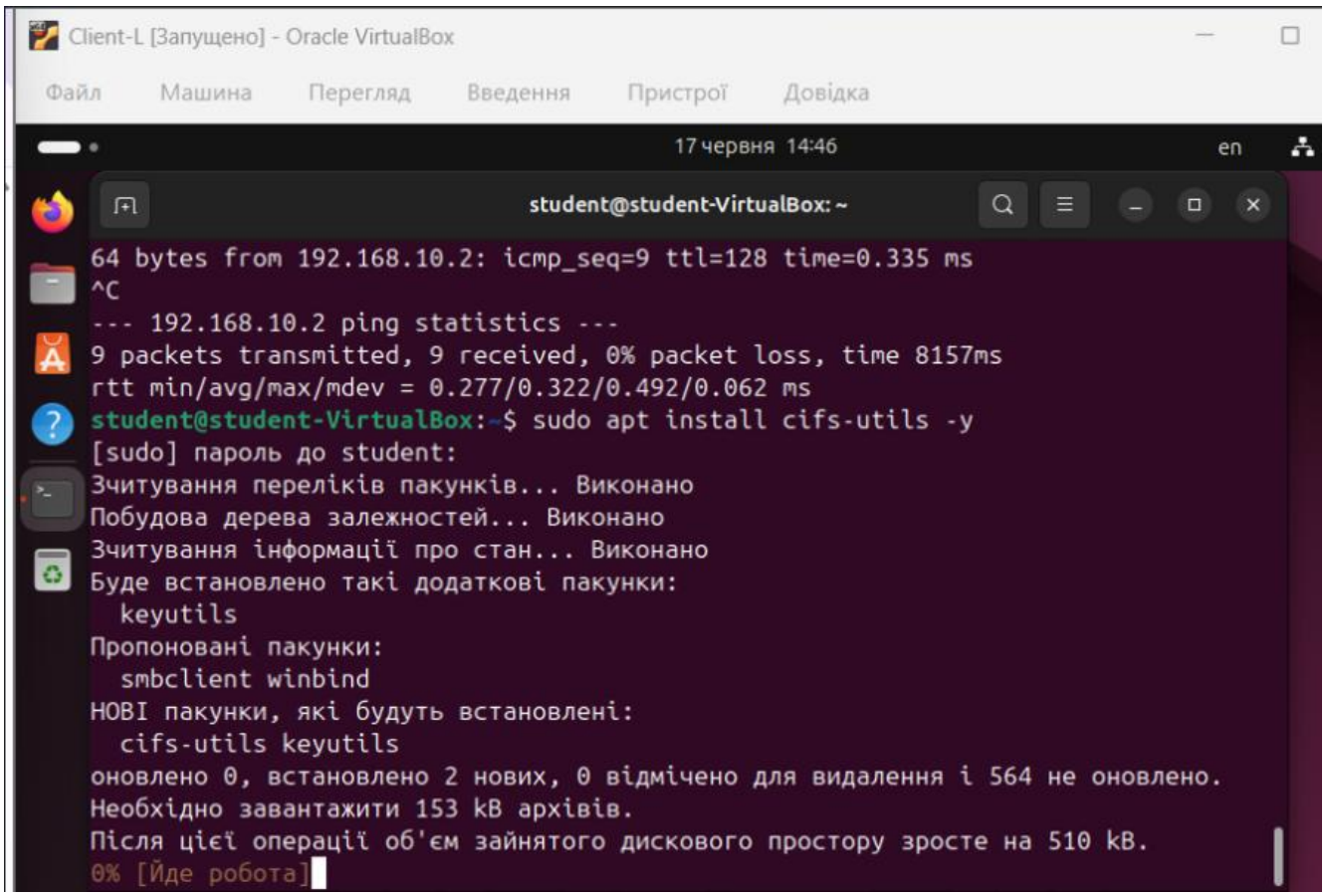


Рисунок 3.68 - Встановлення пакетів SMB/CIFS для роботи Ubuntu Client

За результатами авторизації користувача був отриманий список доступних спільних ресурсів на файловому сервері, включаючи папки Accounting, Employees та IT_Admins, що підтвердило правильність налаштування SMB-доступу і можливість роботи Client-L із корпоративним файловим сховищем.

Для додаткової перевірки було виконано підключення до конкретного ресурсу Employees через SMB. Після успішної авторизації користувач отримав доступ до файлового середовища SMB, що підтвердило коректну роботу механізму автентифікації та розмежування доступу.

Окремо була перевірена робота внутрішньої DNS-служби корпоративної мережі: за допомогою команди nslookup FILE-SERVER здійснено перевірку можливості визначення файлового сервера за доменним ім’ям, внаслідок чого було

підтверджено відповідність між ім’ям FILE-SERVER.corpnet.local та IP-адресою 192.168.10.2, що засвідчило коректну роботу DNS-сервера Active Directory.

Додатково була проведена перевірка доменного імені контролера DC-SERVER; команда nslookup dc-server.corpnet.local також продемонструвала правильне розпізнавання доменного ресурсу та відповідність назви серверу його мережній адресі; результати цієї перевірки представлені на рисунку 3.69.

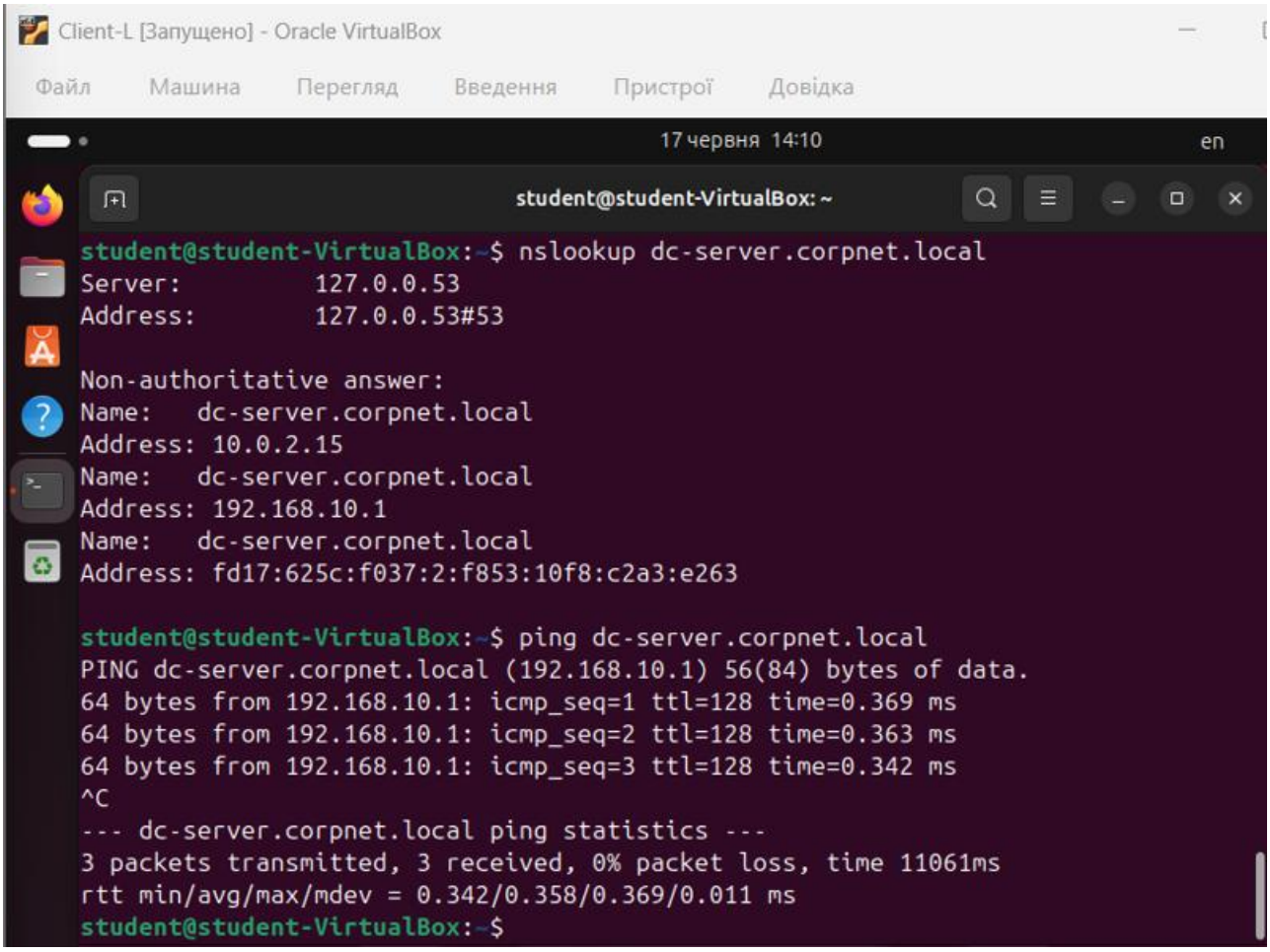


Рисунок 3.69 - Перевірка DNS-розпізнавання серверів корпоративної мережі

Таким чином, в ході проведених випробувань було підтверджено працездатність корпоративних робочих станцій, коректність мережної взаємодії між вузлами, можливість доступу Client-L до Windows-файлового сервера через SMB, а також ефективність роботи DNS-сервісів і доменної інфраструктури.

3.6 Моніторинг та аналіз роботи корпоративної інфраструктури

Для забезпечення постійного моніторингу корпоративної інфраструктури була впроваджена система PRTG Network Monitor. Це програмне забезпечення дозволяє централізовано контролювати доступність серверів і робочих станцій, відстежувати навантаження на апаратні ресурси, аналізувати використання дискового простору та своєчасно виявляти потенційні збої в роботі мережі.

Система моніторингу була розгорнута на сервері FILE-SERVER, який виконує функції центрального вузла збору та обробки інформації про стан всіх компонентів мережі. Після завершення установки програми було здійснено вхід у вебінтерфейс PRTG та проведено початкове налаштування. Результат успішного запуску системи ілюструється на рисунку 3.70.

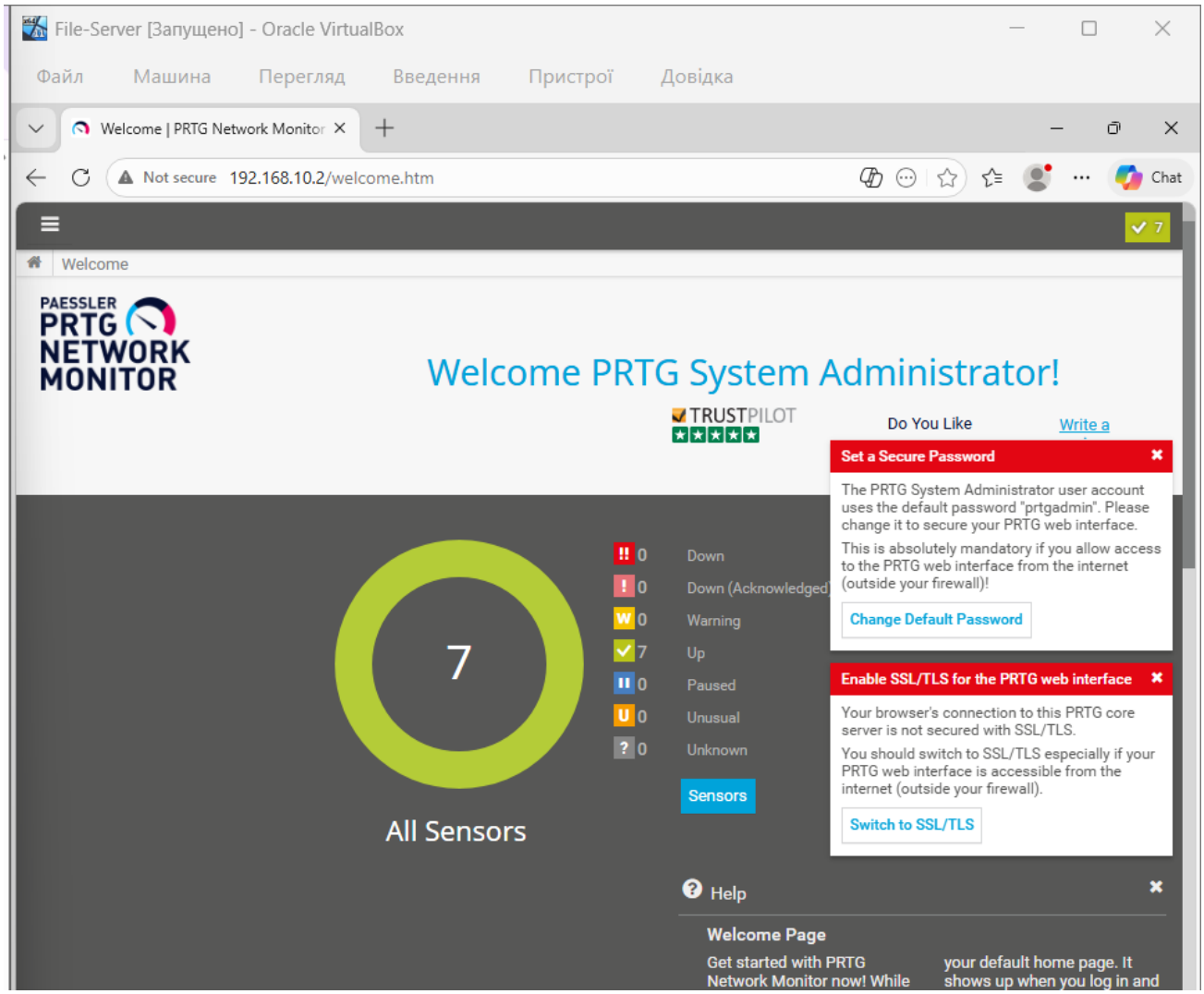


Рисунок 3.70 - Вебінтерфейс системи моніторингу PRTG Network Monitor

Першим пристроєм, доданим до системи моніторингу, став контролер домену DC-SERVER. Для цього пристрою був створений окремий об’єкт у структурі PRTG і налаштовано збір даних за допомогою протоколу WMI (Windows Management Instrumentation). Це надало можливість отримувати інформацію про навантаження на процесор, використання оперативної пам’яті, стан дискового простору та доступність сервера. Процес інтеграції контролера домену до системи показано на рисунку 3.71.

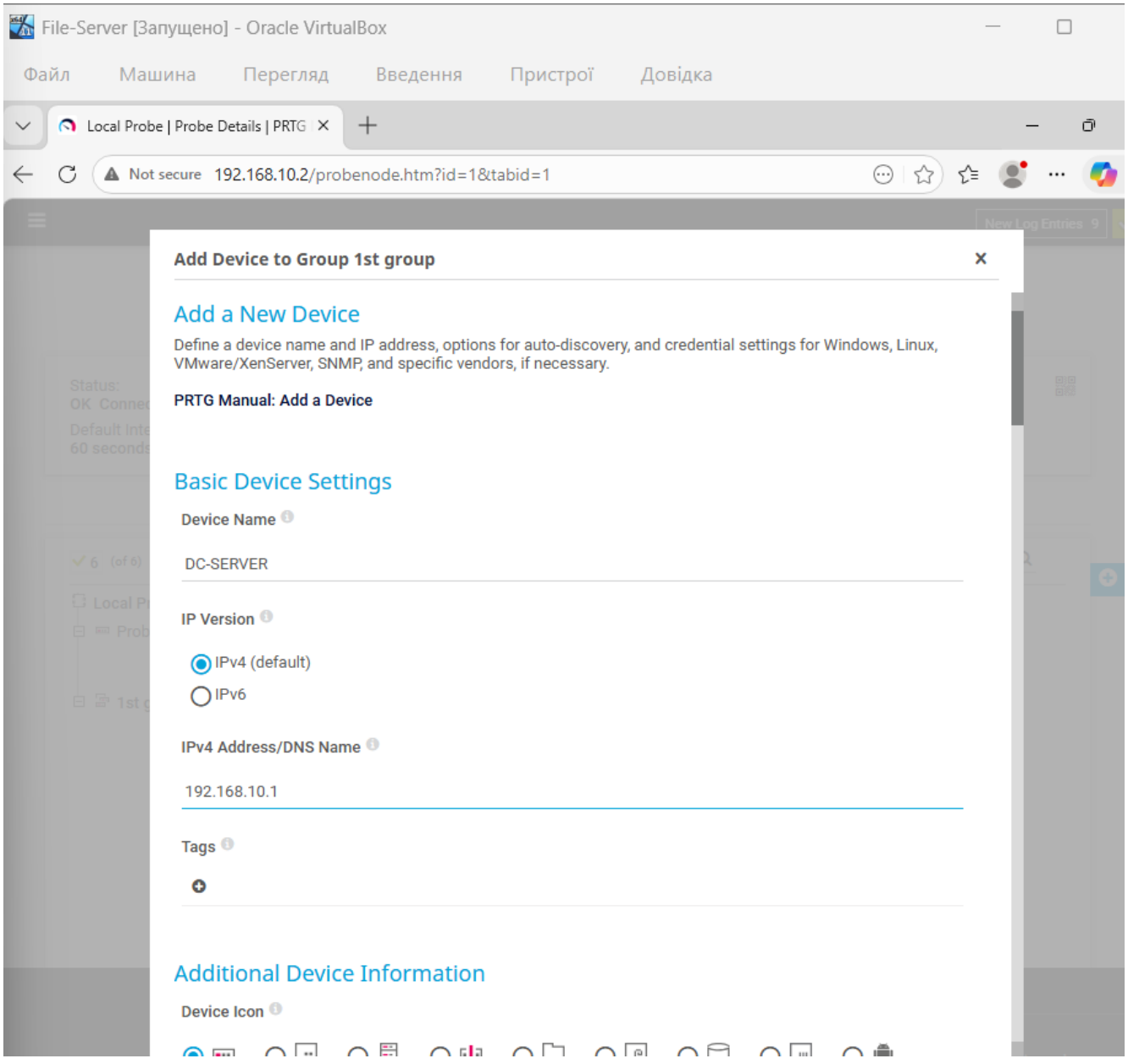


Рисунок 3.71 - Додавання контролера домену DC-SERVER до системи моніторингу

Після створення пристрою були налаштовані необхідні сенсори для моніторингу основних показників роботи сервера. До системи додали сенсори перевірки доступності вузла, контролю процесора, оперативної пам'яті та дискового простору. Приклад налаштування сенсорів представлений на рисунку 3.72.

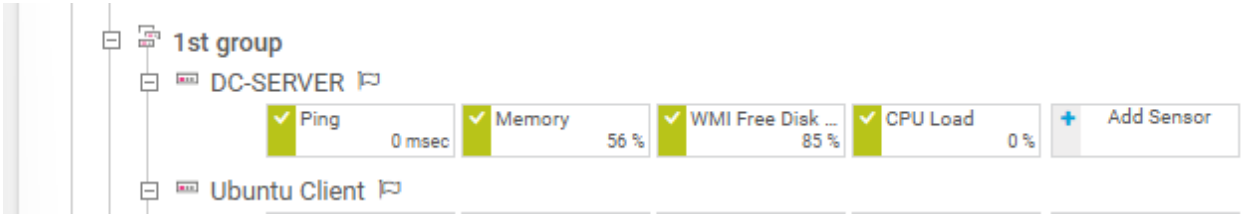


Рисунок 3.72 - Налаштування сенсорів моніторингу для DC-SERVER

Наступним етапом стало підключення файлового сервера FILE-SERVER, який є центральним елементом файлової інфраструктури. Для нього також було налаштовано набір сенсорів для контролю завантаження процесора, використання оперативної пам’яті, стану дискових ресурсів та доступності сервера в мережі. Загальний вигляд моніторингу файлового сервера наведено на рисунку 3.73.

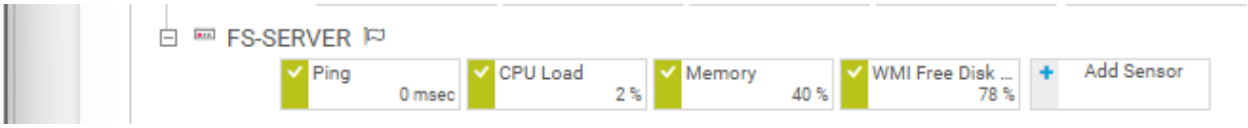


Рисунок 3.73 - Моніторинг файлового сервера FILE-SERVER у середовищі PRTG

Для контролю резервного сховища був доданий сервер NAS-SERVER, що використовується для зберігання резервних копій даних. Мониторинг цього вузла дає змогу стежити за доступністю мережного сховища, рівнем використання ресурсів і станом дискового простору - що критично важливо для надійності системи резервного копіювання. Результати моніторингу NAS-сервера представлені на рисунку 3.74.

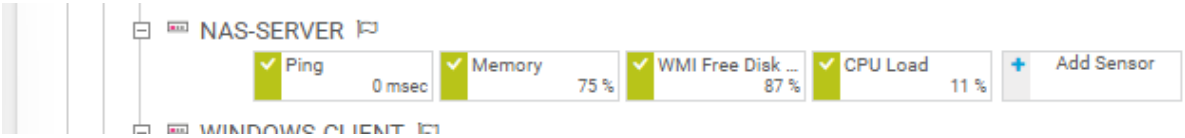


Рисунок 3.74 - Моніторинг NAS-SERVER засобами PRTG Network Monitor

Окремо було звернуто увагу на моніторинг Client-LClient-L. Оскільки операційна система Ubuntu не підтримує технології WMI, для збору системних показників використовувався протокол SNMP. Після налаштування відповідних параметрів до PRTG було інтегровано Client-L і створено сенсори для контролю навантаження на процесор, використання оперативної пам’яті, дискового простору та доступності вузла. Результати моніторингу Client-Lвідображаються на рисунку 3.75.



Рисунок 3.75 - Моніторинг Client-LClient-L за допомогою SNMP

Для аналізу працездатності мережної інфраструктури використовувалися вбудовані засоби візуалізації PRTG. За допомогою графічних відображень та статистичних даних здійснювався контроль завантаження процесора, використання оперативної пам'яті, стану дискових підсистем і доступності серверів у режимі реального часу. Приклад відображення системних показників і графічних діаграм наведено на рисунку 3.76.

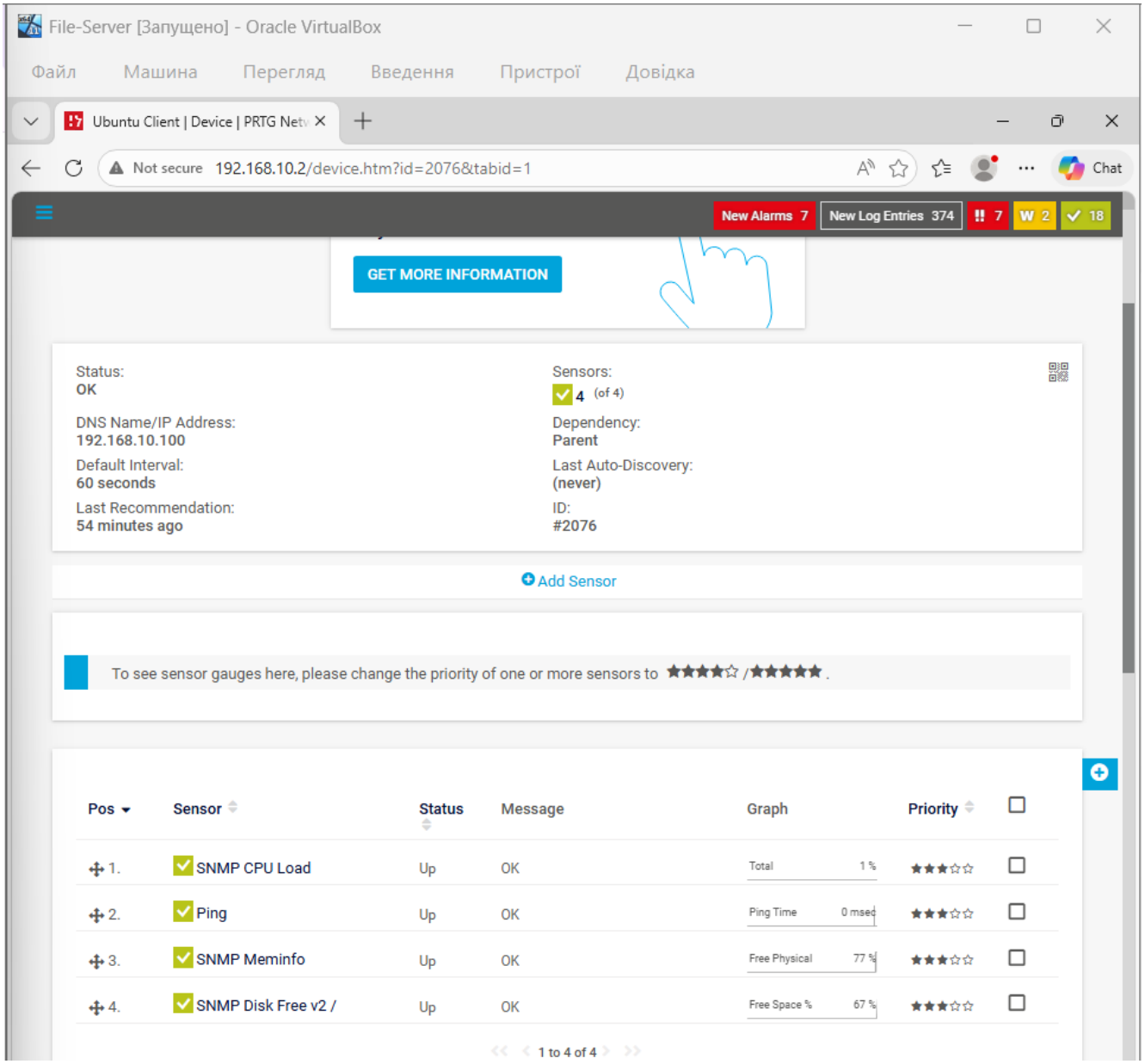


Рисунок 3.76 - Графіки завантаження процесора та використання системних ресурсів у PRTG

У ході тестування було встановлено стабільну реакцію всіх серверів і корпоративних станцій на мережні запити при допустимому рівні використання системних ресурсів. Аналіз отриманих даних підтвердив коректну роботу доменної інфраструктури, файлового сервера, резервного сховища й корпоративних станцій. Впровадження PRTG Network Monitor забезпечило централізований контроль ключових компонентів корпоративної мережі й створило ефективний механізм швидкого виявлення можливих несправностей і загроз.

Висновок до третього розділу

У третьому розділі було здійснено практичну реалізацію та тестування захищеного корпоративного файлового сховища в тестовому середовищі Oracle VM VirtualBox. В результаті цього розгорнуто корпоративну мережну інфраструктуру, яка охоплювала контролер домену (DC-SERVER), файловий сервер (FILE-SERVER), сервер резервного копіювання (NAS-SERVER), а також корпоративні робочі станції під управлінням операційних систем Windows та Linux.

У межах реалізації проєкту було конфігуровано доменну інфраструктуру Active Directory, налаштовано служби DNS і DHCP, створено облікові записи користувачів та групи безпеки, а також впроваджено централізоване управління доступом до корпоративних ресурсів. Застосування Active Directory сприяло спрощенню мережного адміністрування, централізованій аутентифікації користувачів та посиленню контролю за доступом до даних.

В процесі налаштування файлового сервера було розроблено структуру мережних ресурсів та реалізовано механізм розмежування доступу із застосуванням списків контролю доступу (ACL). Практичне використання моделі Zero Trust та принципу мінімальних привілеїв дозволило обмежити доступ користувачів лише до тих ресурсів, які є необхідними для виконання їхніх службових обов'язків, що мінімізує ризики несанкціонованого проникнення та витоку даних.

З метою забезпечення відмовостійкості застосовано технологію RAID 1. Порівняльний аналіз RAID 1 та RAID 5 продемонстрував, що хоча RAID 1 характеризується меншим коефіцієнтом ефективності використання дискового простору, оскільки половина ємності витрачається на дублювання даних, він забезпечує спрощене адміністрування, прискорене відновлення після відмови носія та знижений ризик втрати даних під час відбудови масиву. Зважаючи на відносно невеликий обсяг корпоративного файлового сховища та пріоритет надійності над економією дискового простору, саме RAID 1 було визнано найоптимальнішим рішенням для цього проєкту.

Для убезпечення від втрати даних було впроваджено систему резервного копіювання за допомогою Windows Server Backup із збереженням копій на окремому NAS-SERVER. Комбінація RAID 1 та резервного копіювання гарантувала захист як від апаратних збоїв, так і від випадкового видалення файлів, помилок операторів або наслідків впливу шкідливого програмного забезпечення. Отже, вдалося реалізувати багаторівневий підхід до гарантування надійності зберігання інформації.

Проведене тестування підтвердило коректне функціонування файлового сховища як для Client-W, так і для Client-L. Застосування протоколу SMB уможливило кросплатформний доступ до спільних ресурсів із збереженням функціональності та механізмів контролю доступу.

Значну увагу приділено моніторингу інфраструктури за допомогою PRTG Network Monitor. Результати тестування показали, що система дозволяє своєчасно виявляти проблеми доступності серверів, перевантаження процесора, нестачу дискового простору та інші критичні події. Це забезпечує оперативне реагування на інциденти та посилює загальну керованість корпоративної мережі.

Таким чином, практична реалізація підтвердила ефективність обраних технологій та рішень. Інтеграція Active Directory, ACL, концепції Zero Trust, RAID 1, Windows Server Backup, NAS-сховища та PRTG Network Monitor дозволила створити захищене корпоративне файлове сховище, що надає централізоване управління доступом, високу відмовостійкість, функціонал відновлення даних та постійний моніторинг стану інфраструктури. Отримані результати свідчать про досягнення поставленої мети кваліфікаційної роботи та підтверджують можливість практичного застосування розробленого проєкту в корпоративному секторі.

ВИСНОВКИ

У цій роботі було розроблено та впроваджено проєкт захищеного корпоративного файлового сховища. Це сховище забезпечує централізоване зберігання даних, ефективний контроль доступу для користувачів, регулярне резервне копіювання інформації, постійний моніторинг стану інфраструктури та підвищення загальної стабільності корпоративної мережі.

Під час виконання роботи було проаналізовано сучасні підходи до побудови корпоративних файлових сховищ та методів їхнього захисту. Визначено ключові загрози інформаційній безпеці, такі як несанкціонований доступ до даних, порушення їхньої цілісності, збої обладнання, помилки користувачів та вплив шкідливого програмного забезпечення. За результатами цього аналізу встановлено, що найбільш ефективним є комплексний підхід, який поєднує централізовану перевірку та надання прав доступу користувачам, розподіл їхніх прав, резервне копіювання, забезпечення безвідмовності та безперервний моніторинг усієї інфраструктури.

Також у роботі було досліджено та зіставлено різні технології для забезпечення надійного зберігання даних. Порівняльний аналіз RAID 1 та RAID 5 показав, що RAID 1 простіший в адмініструванні, дозволяє швидше відновити систему після відмови накопичувача та має менший ризик втрати інформації під час реконструкції масиву. З огляду на вимоги проєкту, саме RAID 1 було обрано як найкраще рішення для забезпечення безвідмовності корпоративного файлового сховища.

На основі отриманих результатів було створено архітектуру корпоративної мережі та модель захищеного файлового сховища. Запропонована система включає контролер домену (DC-SERVER), файловий сервер (FILE-SERVER), сервер резервного копіювання (NAS-SERVER) та корпоративні робочі станції під керуванням Windows і Linux. Розроблена модель гарантує централізоване керування користувачами, мережними ресурсами та політиками безпеки.

У процесі проєктування було обґрунтовано вибір необхідного програмного забезпечення та технологій. Для побудови інфраструктури використано Windows Server, Active Directory, DNS, DHCP, файлову систему NTFS, протокол SMB, технологію RAID 1, засоби резервного копіювання Windows Server Backup та систему

моніторингу PRTG Network Monitor. Обрані рішення забезпечують необхідний рівень функціональності, безпеки та сумісності компонентів корпоративної мережі.

Практична реалізація проєкту відбулася у віртуальному середовищі Oracle VM VirtualBox. У ході цього етапу було створено домен CORPNET.LOCAL, налаштовано служби Active Directory, DNS та DHCP, створено користувачів і групи безпеки, впроваджено структуру файлових ресурсів та налаштовано розмежування доступу відповідно до принципу мінімальних привілеїв та концепції Zero Trust.

Для забезпечення безперервної роботи системи було впроваджено RAID 1 та організовано резервне копіювання даних на окремий NAS-SERVER за допомогою Windows Server Backup. Таке рішення захистило інформацію як від апаратних збоїв, так і від випадкового видалення чи пошкодження даних. Проведене тестування підтвердило функціональність механізмів резервування та можливість успішного відновлення інформації.

Особливу увагу приділено перевірці сумісності створеного рішення з різними платформами. Результати тестування засвідчили коректну роботу файлового сховища як для Client-W, так і для Client-W, що дозволяє використовувати систему в різнорідних корпоративних середовищах.

Для спостереження за станом інфраструктури було розгорнуто систему моніторингу PRTG Network Monitor. Налаштовані датчики дозволяють відстежувати доступність мережних вузлів, навантаження на процесор, використання оперативної пам’яті та дискового простору, що забезпечує своєчасне виявлення проблем і підвищує зручність керування мережею.

Отже, всі поставлені на початку роботи завдання було успішно виконано. Створене захищене корпоративне файлове сховище гарантує централізоване керування ресурсами, надійний контроль доступу, безвідмовне зберігання даних, резервне копіювання та моніторинг інфраструктури. Отримані результати підтверджують ефективність запропонованого рішення та можливість його застосування як основи для побудови корпоративних файлових систем з високим рівнем інформаційної безпеки та надійності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Active Directory Domain Services overview. Вебпортал - Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
2. CISA. Cybersecurity and Infrastructure Security Agency (CISA) Official Website - Overview of the Agency and Its Role in National Cybersecurity. Вебпортал U.S. Department of Homeland Security. URL: https://www.cisa.gov/?
3. Microsoft Learn. Access Control Lists (ACLs). Вебпортал Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows/win32/secauthz/access-control-lists
4. NIST. Zero Trust Architecture (NIST SP 800-207). Вебпортал National Institute of Standards and Technology. URL: https://csrc.nist.gov/pubs/sp/800/207/final
5. Paessler. PRTG Network Monitor Manual. Вебпортал Paessler AG. URL: https://www.paessler.com/manuals/prtg?
6. NIST. Cybersecurity Framework (CSF). Вебпортал National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework
7. NIST. Access Control Project Overview. Вебпортал National Institute of Standards and Technology. URL: https://csrc.nist.gov/projects/access-control
8. TechTarget. Discretionary Access Control (DAC) Definition. Вебпортал TechTarget SearchSecurity. URL: https://www.techtarget.com/searchsecurity/definition/discretionary-access-control-DAC
9. NIST. Role-Based Access Control Project Overview. Вебпортал National Institute of Standards and Technology. URL: https://csrc.nist.gov/projects/role-based-access-control
10. NIST. Zero Trust Architecture (SP 800-207). Вебпортал National Institute of Standards and Technology. URL: https://csrc.nist.gov/pubs/sp/800/207/final
11. TechTarget. RAID Definition and Overview. Вебпортал TechTarget SearchStorage. URL: https://www.techtarget.com/searchstorage/definition/RAID

12. IBM. IBM Storage Protect Documentation. Вебпортал IBM Documentation. URL: https://www.ibm.com/docs/en/storage-protect
13. DiskInternals. RAID 1 vs RAID 5 Comparison. Вебпортал DiskInternals. URL: https://www.diskinternals.com/raid-recovery/raid-1-vs-raid-5/
14. Synology. Data Backup Solutions Overview. Вебпортал Synology. URL: https://www.synology.com/en-global/dsm/solution/data_backup
15. Paessler. Network Monitoring Tool Overview (PRTG). Вебпортал Paessler AG. URL: https://www.paessler.com/monitoring/network/network-monitoring-tool
16. Microsoft Learn. SMB Protocol Configuration and Version Management. Вебпортал Microsoft Learn. URL: https://learn.microsoft.com/uk-ua/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server
17. Microsoft Learn. Active Directory Domain Services Overview. Вебпортал Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
18. NIST. Cybersecurity Framework. Вебпортал National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework
19. IBM. Storage Protect Documentation (Version 8.1.0). Вебпортал IBM Documentation. URL: https://www.ibm.com/docs/en/storage-protect/8.1.0
20. Paessler. PRTG Network Monitor (Official Documentation). Вебпортал Paessler AG. URL: https://www.paessler.com/prtg
21. Microsoft Learn. File Server SMB Overview. Вебпортал Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview
22. Microsoft Learn. DHCP Technology Overview. Вебпортал Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top
23. B&H Photo Video. Understanding RAID (Educational Article). Вебпортал B&H Explora. URL: https://www.bhphotovideo.com/find/newsLetter/Understanding-

RAID.jsp?c3api=2572%2C138045322040&gad_campaignid=658944934&gad_source=1&gbraid=0AAAAAD7yMh3Bpedh52IXk3TLU_xv7_3ts&gclid=EAIaIQobChMIhcPJ4MeflQMVzwqiAx3TEwhcEAAYASAAEgKdgvD_BwE

24. TransIP. Configuring Windows SMB File Server Guide. Вебпортал TransIP Knowledge Base. URL: https://www.transip.eu/knowledgebase/4711-configuring-windows-smb-file-server
25. Netwave. Захист корпоративних мереж: засоби та методи. Вебпортал Netwave Blog. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/
26. Entro Security. Active Directory Authentication Glossary. Вебпортал Entro Security. URL: https://entro.security/glossary/active-directory-authentication/
27. Microsoft Learn. Configure Group Policies and Security Settings. Вебпортал Microsoft Learn. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/configure-group-policies-set-security
28. RocketMe Up Cybersecurity. Role-Based Access Control (RBAC) in Enterprise Applications - A How-To Guide. Вебпортал Medium. URL: https://medium.com/@RocketMeUpCybersecurity/role-based-access-control-rbac-in-enterprise-applications-a-how-to-guide-933321670df9
29. FileCloud. NTFS Security Permissions Overview. Вебпортал FileCloud. URL: https://www.filecloud.com/ntfs-security-permissions/
30. Xinnor. RAID Advantages and Disadvantages Guide. Вебпортал Xinnor Blog. URL: https://xinnor.io/blog/a-guide-to-raid-pt-1-advantages-and-disadvantages-of-raid/
31. Contabo. How to Do Backups on Windows Server. Вебпортал Contabo Blog. URL: https://contabo.com/blog/how-to-do-back-ups-on-windows-server/?utm_source=google&utm_medium=cpc&utm_campaign=&utm_term=&utm_content=&gad_source=1&gad_campaignid=23616421152&gbraid=0AAAAAD_Qy-fJ8vbwldllegjQ32XOx07cG&gclid=CjwKCAjwuuPRBhAnEiwA2Ji8el98ELH0i-rTp29zTDoUPDsoSg5epsJA2nX7X9jt7-Gp0G9OP2Sa4hoCGqIQAvD_BwE

32. Yugabyte. Types of Data Recovery Explained. Вебпортал Yugabyte. URL: https://www.yugabyte.com/key-concepts/what-are-the-four-types-of-data-recovery/
33. Medium. Securing NAS Systems: Best Practices for Data Safety. Вебпортал Medium. URL: https://medium.com/@frankd228801/securing-nas-systems-best-practices-for-data-safety-31d7fe938d4d
34. ReadTheManual. Windows Networking DNS/DHCP Guide. Вебпортал ReadTheManual. URL: https://readthemanual.co.uk/windows-networking-dns-dhcp/
35. IT-Homyak. Встановлення та налаштування DHCP-сервера. Вебпортал IT-Homyak. URL: https://it-homyak.com.ua/server/%D0%B2%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F-%D1%82%D0%B0-%D0%BD%D0%B0%D0%BB%D0%B0%D1%88%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-dhcp-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80/
36. Duo Security. Zero Trust vs Least Privilege. Вебпортал Duo. URL: https://duo.com/learn/zero-trust-vs-least-privilege
37. CiberSafety. SNMP Protocol for Network Management and Security. Вебпортал CiberSafety. URL https://cibersafety.com/en/SNMP-protocol-for-network-management-and-security/
38. E-Server. RAID Comparison Guide (RAID 1 vs RAID 5 vs RAID 6 vs RAID 10). Вебпортал E-Server. URL: https://e-server.com.ua/uk/poradi/iakii-tip-raid-krashhii-porivniujemo-raid-1-vs-raid-5-i-raid-6-vs-raid-10?srsltid=AfmBOoraqQn1Uwdb02mwlZJYDa7JCTmpGaZYIPCp5vETWHGlSjspCM5_