

Хмельницький національний університет  
Факультет інформаційних технологій  
Кафедра кібербезпеки

### КВАЛІФІКАЦІЙНА РОБОТА

Барана Андрія Андрійовича

на здобуття ступеня вищої освіти Бакалавра

Система доступу до інформаційних ресурсів університету

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

Освітня програма Програмування та захист комп'ютерних систем і мереж

Шифр КРБКІ.001115.01.01 ПЗ

Виконав студент 4 курсу група КІ-20-1

Андрій БАРАН

Керівник старший викладач

Сергій МОСТОВИЙ

Нормоконтролер старший викладач

Сергій МОСТОВИЙ

До захисту допускаю:

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

19 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій  
Кафедра Кібербезпеки  
Рівень вищої освіти Бакалавр  
Галузь знань 12 – Інформаційні технології  
Спеціальність 123 – Комп'ютерна інженерія  
Освітня програма Програмування та захист комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ 

15 лютого 2024 р.

**ЗАВДАННЯ  
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Барану Андрію Андрійовичу

1 Тема роботи Система доступу до інформаційних ресурсів університету

Керівник роботи Сергій МОСТОВИЙ

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.06.2024 р.


3 Вихідні дані до роботи Технічна документація по інформаційній інфраструктурі університету, документація компанії Microsoft по серверних операційних системах

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ, Аналіз систем доступу до інформаційних ресурсів, Проекування системи доступу до ресурсів університету, Розробка та впровадження системи доступу до ресурсів університету

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Логічна топологія мережі університету, Інфраструктура домену khmnu.edu.ua

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедр кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Березень	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Квітень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент



Андрій БАРАН

Керівник кваліфікаційної роботи



Сергій МОСТОВИЙ



## АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система доступу до інформаційних ресурсів університету».

Автор роботи: *Баран Андрій Андрійович.*

Керівник роботи: *Мостовий Сергій Володимирович.*

Пояснювальна записка: 86 с., 111 рис., 2 дод., 42 джерела.

Графічна частина: 2 креслення.

ЛОГІЧНА ТОПОЛОГІЯ МЕРЕЖІ УНІВЕРСИТЕТУ, ІНФРАСТРУКТУРА  
ДОМЕНУ KHMNU.EDU.UA.

Мета кваліфікаційної роботи: проєктування та реалізація системи доступу до інформаційних ресурсів університету та забезпечення централізованого керування користувачами.

Під час виконання кваліфікаційної роботи, було спроектовано систему доступу до інформаційних ресурсів університету. Для реалізації системи доступу було створено домен khmnu.edu.ua, застосовані політики безпеки та налаштовано 2 сервери та 1 робочу станцію в програмному середовищі Oracle VM VirtualBox.

17.06.24

## ЗМІСТ

Вступ.....	4
1 Аналіз систем доступу до інформаційних ресурсів .....	6
1.1 Огляд технологій доступу до ресурсів установи.....	6
1.2 Огляд та аналіз серверних операційних систем.....	10
1.3 Постановка задачі.....	18
2 Проектування системи доступу до ресурсів університету.....	19
2.1 Ознайомлення з інформаційними технологіями та ресурсами університету .....	19
2.2 Вимоги до системи доступу до ресурсів університету та проектування її архітектури.....	27
2.3 Проектування структури домену та планування домену.....	30
2.4 Висновки .....	34
3 Розробка та впровадження системи доступу до ресурсів університету .....	36
3.1 Встановлення та налаштування серверної операційної системи Windows Server 2019.....	36
3.2 Розгортання служби Active Directory, DHCP та DNS .....	41
3.2.1 Розгортання служби Active Directory.....	41
3.2.2 Налаштування DHCP, DNS та другого сервера.....	47
3.2.3 Налаштування відмовостійкості на другому сервері.....	56
3.3 Створення та керування груповою політикою безпеки для реалізації системи доступу до ресурсів.....	58
3.3.1 Зіставлення дисків на сервері. Загальні папки.....	58

КРБКІ.001115.01.01 ПЗ				
Зм.	А	№ докум.	Підпис	Дата
Розробив		Баран А.А.		17.06.20
Перевірив		Мостовий С.В.		18.06.20
Н.контр.		Мостовий С.В.		18.06.20
Затвер.		Кляшч Ю.П.		19.06.20
Система доступу до інформаційних ресурсів університету				
Пояснювальна записка				
		Літера	Аркуш	Аркушів
		Н	2	86
ХНУ, КІІ-20-1				

3.3.2 Встановлення квот на папки.....	69
3.3.3 Встановлення та налаштування DFS. ....	72
3.4 Висновки.....	78
Висновки.....	78
Перелік літературних посилань.....	80
Додатки.....	86

## ВСТУП

В сучасному світі, де технології швидко розвиваються, інформація стала цінним активом, що визначає успіх і конкурентоспроможність будь-якої організації. Отримуючи доступ до інформації, організації можуть краще розуміти світові тренди, потреби клієнтів та конкурентну ситуацію на ринку. Університети, як осередки вищої освіти та дослідницької діяльності, є ключовими фігурантами у формуванні та поширенні знань, які грають визначальну роль у розвитку суспільства.

Університети не лише забезпечують студентів необхідними знаннями та навичками для майбутньої кар'єри, але й проводять дослідження у різних галузях, сприяючи науковому прогресу та розвитку нових технологій. Крім того, вони виконують функцію зберігання та передачі знань через викладання, публікації та інші активності, що допомагають у формуванні і розповсюдженні нових ідей.

Забезпечення зручного доступу до інформаційних ресурсів університету для всіх його учасників є важливою передумовою для успішного функціонування навчального процесу та наукової діяльності. Це означає, що студенти, викладачі, науковці та адміністративний персонал повинні мати легкий доступ до різноманітних джерел інформації, необхідних для виконання їхніх обов'язків та досягнення навчальних та наукових цілей.

Студентам потрібний доступ до актуальних навчальних матеріалів, електронних бібліотек, навчальних платформ та інших ресурсів, які допоможуть їм здобути необхідні знання та навички. Викладачі повинні мати можливість швидко знаходити та використовувати актуальні наукові статті, матеріали для лекцій та досліджень, а також здійснювати спілкування з колегами та студентами. Науковці повинні мати доступ до наукових баз даних, журналів та інших ресурсів для проведення досліджень та публікацій результатів. Адміністративний

					КРБКІ.001115.01.01 ПЗ	Арк. 8
Зм.	Арк.	№ докум.	Підпис	Дата		

персонал потребує доступу до систем управління даними, фінансами та іншими ресурсами для ефективного керування університетом.

Забезпечення зручного доступу до інформаційних ресурсів включає в себе не лише технічні аспекти, такі як налагодження мережі та програмного забезпечення, але й організаційні заходи, спрямовані на забезпечення безпеки, конфіденційності та ефективного використання інформації. Це може включати впровадження політик доступу до інформації, навчання користувачів з питань кібербезпеки та захисту даних, а також постійний моніторинг та оновлення систем управління доступом.

Проте, існуючі методи та системи доступу можуть не завжди відповідати потребам сучасного університетського середовища. Тому актуальність розробки нової системи доступу до інформаційних ресурсів стає нагальною проблемою, що вимагає уваги та наукового дослідження.

Мета цієї кваліфікаційної роботи полягає в дослідженні та аналізі існуючих підходів до організації доступу до інформаційних ресурсів університетів, а також у розробці та впровадженні ефективної системи, яка забезпечить зручний та безпечний доступ до цих ресурсів. Основна мета полягає у поліпшенні якості освіти та наукових досліджень шляхом забезпечення ефективного доступу до інформаційних ресурсів університетського середовища.

					КРБКІ.001115.01.01 ПЗ	Арк.
						9
Зм.	Арк.	№ докум.	Підпис	Дата		

# 1 АНАЛІЗ СИСТЕМ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

## 1.1 Огляд технологій доступу до ресурсів установи

На сучасному етапі розвитку суспільства та технологій актуальність систем доступу до інформаційних ресурсів університетів набуває особливого значення.

Ось кілька ключових моментів, які підкреслюють цю актуальність:

- а) Зростаюча кількість інформації;
- б) Важливість дистанційного навчання;
- в) Безпека і конфіденційність;
- г) Необхідність ефективного управління.

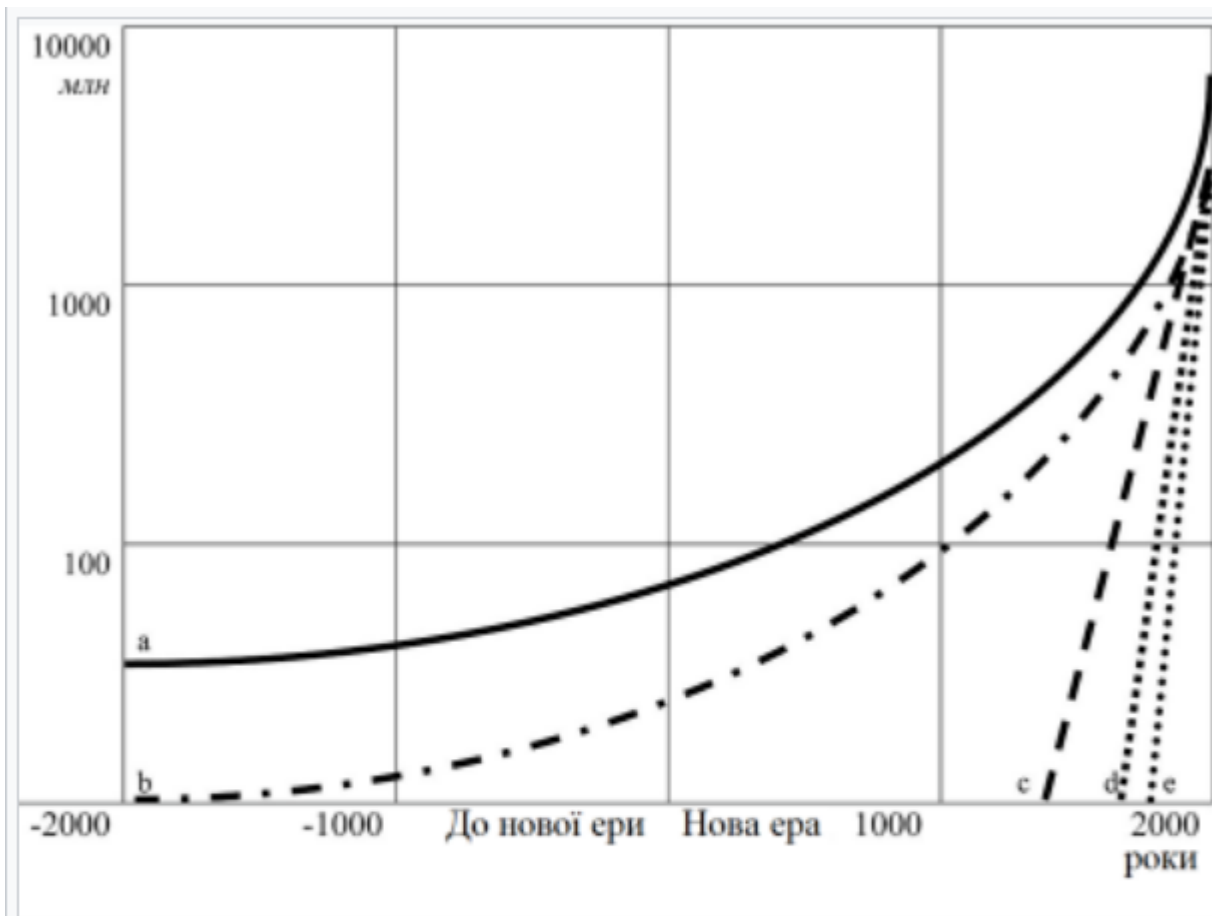
Цивілізаційні тенденції розвитку інформаційного суспільства характеризуються тим, що у 2002 році загальний обсяг виробленої людством інформації становив  $2,5 \cdot 10^8$  байт (18 Ексабайт). За п'ять попередніх років цей обсяг перевищив суму виробленої інформації за всю попередню історію. Кількість інформації в світі збільшується на 30% щорічно. У середньому, на одну людину у світі щорічно припадає  $2,5 \cdot 10^8$  байт. Сучасна інформаційна революція характеризується тим, що на кожних 7 мільярдів осіб припадає 6 мільярдів телефонів (відомості компанії «Ericsson», 2012), 6 мільярдів телевізійних пристроїв («Guinness Today», 2012), 2 мільярди комп'ютерів («Gartner», 2012), 2,3 мільярди користувачів інтернету («Internet World Stats», 2012).

У сфері електронних комунікацій на кінці ХХ століття спостерігалось різке зростання різноманітних приватних публікацій в Інтернеті. Кількість блогів збільшується вдвічі кожні 6 місяців. За статистикою, обсяг цифрової інформації подвоюється кожні вісімнадцять місяців. Більшість цього потоку (до 95%) складають неструктуровані дані, тоді як лише 5% представляють собою різноманітні бази даних, що відносяться до структурованої інформації.

Вікі-колаборативні портали також варто зазначити. Кількість статей у них експоненційно зростає. На наступному рисунку 1.1 показано як зростає кількість

					КРБКІ.001115.01.01 ПЗ	Арк. 10
Зм.	Арк.	№ докум.	Підпис	Дата		

населення Землі, грамотність, читання-друкування, отримання радіо-інформації та інформації через Інтернет з плином часу.



Поширення в популяції *Homo sapiens* нових функціонально-поведінкових відмінних ознак у вигляді корисних навичок інформаційної взаємодії. а — населення Землі; b — грамотність; с — читання-друкування — доступність всім грамотним; d — отримання радіо-, телевізійної інформації (кількість приймачів); e — інформаційний зв'язок через телефони, комп'ютери, інтернет (к-ть телефонів, комп'ютерів, користувачів Інтернет)<sup>[1]</sup>

Рисунок 1.1 – Поширення в популяції *Homo sapiens* нових функціонально-поведінкових відмінних ознак у вигляді корисних навичок інформаційної взаємодії

Зм.	Арк.	№ докум.	Підпис	Дата

Університети, як центри навчання та досліджень, повинні мати ефективні системи доступу, щоб студенти та викладачі могли з легкістю знаходити необхідну інформацію серед величезного потоку даних.

З поглибленням цифровізації освіти стає все більш поширеним дистанційне навчання. Перехід на дистанційне навчання, зумовлений пандемією (в минулому, а на разі війною), став неочікуваним та доволі серйозним випробуванням для всіх учасників освітнього процесу – освітян, вчителів, учнів та їхніх батьків.

Після тимчасової розгубленості всім довелось прийняти цей виклик та швидко адаптуватись до нових реалій, але питання розвитку дистанційної освіти набуло неабиякої актуальності.

І хоча дистанційне навчання не є заміною очного та ніколи не планувалось на довгострокову перспективу, воно може стати ефективним інструментом не тільки під час карантину та війни, а і в мирний час[2].

Забезпечення доступу до інформаційних ресурсів стає надзвичайно важливою необхідністю, щоб забезпечити рівні умови навчання для всіх студентів, незалежно від їхнього місцезнаходження та в умовах воєнного стану.

Інформаційна безпека – багатогранна, багатовимірна діяльність, в якій успіх може принести тільки системний, комплексний підхід. Безпека використання інформаційних систем полягає у забезпеченні доступності, цілісності, конфіденційності та підтримці інформаційних ресурсів її інфраструктури.

В умовах постійно зростаючих загроз кібербезпеки та вимог щодо захисту персональних даних, системи доступу до інформаційних ресурсів університету повинні бути надійними та безпечними. Інформаційна безпека залежить від усього комплексу заходів та сучасних технологій, керування якими відбувається із застосуванням різноманітних інформаційних систем.

До основних складових інформаційної безпеки належить конфіденційність, тобто захист від несанкціонованого доступу до інформації.

					КРБКІ.001115.01.01 ПЗ	Арк. 12
Зм.	Арк.	№ докум.	Підпис	Дата		

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, яка полягає в тому, що інформаційна безпека є складова частина інформаційних технологій – області, що розвивається безпрецедентно високими темпами. Тут важливі не стільки окремі рішення (закони, навчальні курси, програмно-технічні вироби), що знаходяться на сучасному рівні, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу.

Складність механізмів прийняття сучасних управлінських рішень щодо захисту інформації в новому інформаційному середовищі пов'язана із застосуванням стрімко розвиваючих інформаційних систем, призначених для великого обсягу обробки, обміну та використання їх в сучасному житті кожної особистості, підприємства, держави, світі, а також швидкими темпами розвитку технічних засобів[3].

Забезпечення конфіденційності та захисту інформації є критично важливим завданням для університетських інформаційних систем.

Грамотне проектування інформаційних систем управління дає змогу будь-які дані вводити до системи лише один раз. При необхідності їх використання створюють відповідний запит до бази, дані опрацьовують і формують звіт з інформацією, що потрібна для прийняття рішення.

Сьогодні є можливість забезпечити вертикальну інтеграцію інформаційних систем різних рівнів управління освітою, а також горизонтальні зв'язки між системами одного рівня. У такому випадку не буде принципових проблем, якщо дані створюються в одній підсистемі, запит – в іншій, а звіт поступає до третьої[4].

Управління доступом до інформаційних ресурсів також вимагає ефективних та гнучких систем, щоб керувати правами доступу, моніторити активність та забезпечувати відповідність з правилами та регуляціями.

## 1.2 Огляд та аналіз серверних операційних систем

Є 2 варіанти керування користувачами в інформаційній мережі це або окремі облікові записи на кожному об'єкті, або централізовані сховища облікових записів.

Розглянемо плюси та мінуси цих двох підходів. Для систем, які мають окремі облікові записи на кожному пристрої, перевагами буде те, що вони легкі в реалізації(оскільки для кожного окремого об'єкта (комп'ютера або сервера) створюється окремий обліковий запис користувача) та мають локальне управління(керування обліковими записами відбувається локально на кожному пристрої, що може бути зручним для адміністраторів, які працюють безпосередньо з цими пристроями). Мінусом також буде локальне управління, бо в системі в якій великий потік кадрів, буде дуже проблематично додавати/видаляти нові облікові записи, а також і в разі потреби у регулярній синхронізації облікових даних між різними пристроями. Ще одним мінусом буде те, що будуть значні витрати на обслуговування, адже якщо університет має значну кількість пристроїв, витрати на обслуговування можуть зрости через необхідність керування багатьма окремими обліковими записами.

В свою чергу централізовані сховища облікових записів мають такі переваги:

- а) уніфіковане управління;
- б) оптимізація ресурсів;
- в) спрощене управління.

Підхід уніфікованого управління забезпечує централізоване управління обліковими записами з використанням директорії корпоративного рівня, такої як Active Directory для Windows або LDAP для Linux.

Централізована система зберігання облікових записів дозволяє ефективніше використовувати ресурси та забезпечує однорідність управління користувачами.

Адміністраторам легше керувати обліковими записами, оскільки вони можуть здійснювати це з одного централізованого місця.

Отже, можна зробити висновок, що централізована система керування буде набагато кращим вибором, бо керування великою кількістю облікових записів буде здійснюватись з одного пристрою/серверу, що зменшить навантаження на адміністраторів.

Вибравши варіант керування системою користувачів, залишається ще вибрати відповідну серверну операційну систему, за допомогою якої і буде здійснюватись контроль та адміністрування університету. Цей вибір є ключовим аспектом для забезпечення ефективного та безперебійного функціонування. Прийняття правильного рішення вимагає уважного розгляду різних характеристик і параметрів. Давайте розглянемо основні типи операційних систем та їх відмінності.

Незалежно від того, яка операційна система буде вибрана, вона буде відноситися до одного з двох основних сімейств – Linux або Windows.

Linux – загальна назва Unix-подібних операційних систем на основі однойменного ядра. Це один із найвидатніших прикладів розробки вільного (free) та відкритого (з відкритим кодом, open source) програмного забезпечення (software). На відміну від власницьких операційних систем (на кшталт Microsoft Windows та macOS), їхні вихідні коди доступні всім для використання, зміни та поширення абсолютно вільно (в тому числі безкоштовно)[41].

Microsoft Windows або Windows – група сімейств комерційних пропріетарних операційних систем корпорації Microsoft, орієнтованих управління за допомогою графічного інтерфейсу. MS-DOS є прабатьком Windows. Кожна родина обслуговує певний сектор комп'ютерної промисловості.

					КРБКІ.001115.01.01 ПЗ	Арк. 15
Зм.	Арк.	№ докум.	Підпис	Дата		

Активні сімейства Microsoft Windows включають Windows NT та Windows IoT; вони можуть містити підродини (наприклад, Windows Server або Windows Embedded Compact) (Windows CE)[42].

Перед тим, як приймати рішення, важливо зрозуміти, на яких критеріях треба зосередитися. Декілька ключових факторів:

- а) вартість;
- б) надійність;
- в) частота оновлень;
- г) комфорт застосування.

Необхідно заздалегідь з'ясувати, скільки коштує застосування того чи іншого варіанту (також є безкоштовні операційні системи). Репутація системи серед користувачів свідчить про її надійність. Потрібно дізнатися наскільки регулярно публікуються нові версії і всілякі доповнення. Є ОС з простим та інтуїтивно зрозумілим інтерфейсом, а також такі, що потребують досвіду для належного адміністрування. Ось перелік найбільш популярних та найбільш використовуваних серверних операційних систем:

- а) Windows Server;
- б) FreeBSD;
- в) Debian;
- г) Red Hat Enterprise Linux;
- д) CentOS;
- е) Ubuntu.

Windows Server це практичне рішення, особливо для зберігання файлів. Не варто порівнювати Віндовс Сервер зі звичною операційною системою Windows, що встановлена на більшості персональних комп'ютерів.

Серед беззаперечних переваг серверної версії – універсальність. Так, система використовується для:

- а) додатків;

б) поштових серверів;

в) файлових серверів.

Проте, зона ризику Windows Server пов'язана з безпекою. Більшість вірусів написана саме для атаки на програмне забезпечення Microsoft, через що потенційно знижується рівень захисту ОС. Однак останні версії операційної системи мають більш високий рівень безпеки, також існують якісні антивіруси.

FreeBSD – UNIX-подібна операційна система, коріння якої тягнеться від AT&T UNIX, через Berkeley Software Distribution (BSD) гілку операційних систем 386BSD та 4.4BSD. Працює на процесорах x86 (IA-32, x86-64), сумісних з ПК системах (включно з Microsoft Xbox, а також на комп'ютерах і процесорах DEC Alpha, Sun, Itanium (IA-64), AMD64, PowerPC та NEC PC-98. FreeBSD добре зарекомендувала себе як система для побудови інтранет- і інтернет-серверів. Вона надає достатньо надійні мережеві служби і ефективне управління пам'яттю[34].

FreeBSD найстаріша і досить надійна операційна система, безперечною перевагою якої є відсутність плати. У зв'язку з цим велика кількість серверів працюють саме на FreeBSD. Надійність, якість, гнучкість налаштувань – також в числі сильних сторін системи.

Однак актуальність даної ОС з часом втрачається, а відсутність достатньої кількості чітких інструкцій ускладнює адміністрування.

Debian – дистрибутив Linux, який складається тільки з вільного програмного забезпечення (main-секції архіву Debian). Популярний та впливовий дистрибутив Linux. Багатоцільова операційна система, що використовується: настільними комп'ютерами, ноутбуками, серверами, вбудованими системами[35].

Цей варіант здатний забезпечити безперебійну і стабільну роботу, тому вважається хорошим рішенням для сервера. Ключовим недоліком є те, що поновлення цієї операційки випускаються надзвичайно рідко.

					КРБКІ.001115.01.01 ПЗ	Арк.
						17
Зм.	Арк.	№ докум.	Підпис	Дата		

Red Hat Enterprise Linux (часто скорочується до RHEL) – дистрибутив Linux виробництва компанії Red Hat, орієнтований на комерційний ринок, включно з мейнфреймами. Red Hat здійснює підтримку кожної версії RHEL протягом 7 років з моменту її виходу. Уся офіційна підтримка Red Hat, і всі курси навчання та видача сертифікатів для розгортання апаратного та програмного забезпечення — Red Hat Certified Technician (RHCT), Red Hat Certified Engineer (RHCE), Red Hat Certified Security Specialist (RHCSS) та Red Hat Certified Architect (RHCA) складають основу платформи Red Hat Enterprise Linux[36].

Слід враховувати, що застосування можливе тільки на платній основі. Нові версії презентуються один раз в три роки.

CentOS (Community ENTerprise Operating System) – вільно доступний дистрибутив Linux, на основі якого формується комерційний дистрибутив Red Hat Enterprise Linux компанії Red Hat. У минулому (до версії 8 включно) метою проєкту було складання 100 % двійково сумісного з RHEL дистрибутиву. Підтримка CentOS 8 припинилася 31 грудня 2021 року; користувачам запропоновано перейти на безперервно оновлювану редакцію CentOS Stream або на альтернативні дистрибутиви, що використовують формат пакунків RPM[37].

Ubuntu – операційна система для робочих станцій, лептопів і серверів, найпопулярніший у світі дистрибутив Linux. Серед основних цілей Ubuntu – надання сучасного й водночас стабільного програмного забезпечення для пересічного користувача із сильним акцентом на простоту встановлення та користування[38].

Ubuntu – простий безкоштовний варіант, допустимий при відсутності серйозних навантажень. Зрозумілі керівництва, моментальна доступність до використання і відмінний рівень захищеності.

Зараз розглянемо головні відмінності операційних систем Windows і Linux.

Ядро – центральна частина операційної системи, що реалізовує інтерфейс між прикладними процесами та обладнанням комп'ютера. Завантажується в

					КРБКІ.001115.01.01 ПЗ	Арк. 18
Зм.	Арк.	№ докум.	Підпис	Дата		

оперативну пам'ять комп'ютера і безпосередньо взаємодіє з апаратурою, забезпечуючи керування апаратними засобами (при цьому використовуються драйвери (модулі ядра) підключеного в систему обладнання), підтримку одночасної роботи багатьох користувачів (багатокористувацький режим), підтримку паралельного виконання багатьох процесів в системі (багатозадачність). Зазвичай ядро робить ці об'єкти доступними для прикладних процесів через механізми міжпроцесної взаємодії і системних викликів[39].

У кожного типу операційної системи ядро побудовано по-різному. У Linux систем ядро має такі властивості:

а) ядро – це моноліт, реалізований у вигляді одного файлу, – якщо виникне потреба в удосконаленні функцій ядра, застосовуються модулі;

б) взаємодіє з програмами за допомогою системних викликів – завдяки стандартизації цього процесу програмне забезпечення без змін може працювати на різних Linux-системах;

в) має вбудовані драйвери – так як програми розташовуються в просторі користувача з урахуванням графічної оболонки, підвищується рівень безпеки.

З Windows ситуація кардинально відрізняється. Ядро має такі характеристики:

а) включає велику кількість фрагментів бібліотек dll, при цьому кожна частина несе свій функціонал;

б) цілком відсутнє використання системних викликів;

в) програми користувачів застосовують спеціальні бібліотеки, що викликають в свою чергу функції з ntdll.dll;

г) управління драйверами здійснюється за допомогою бібліотеки hal.dll, кожен драйвер окремо підключається до ядра;

д) система піддається адаптації до різного програмного забезпечення.

Незважаючи на високий рівень адаптивності ядра Windows, потрібно враховувати, що продуктивність даної системи набагато нижче, ніж у Linux.

					КРБКІ.001115.01.01 ПЗ	Арк. 19
Зм.	Арк.	№ докум.	Підпис	Дата		

Файлова система — спосіб організації даних, який використовується операційною системою для збереження інформації як файлів на носіях інформації. Також цим поняттям позначають сукупність файлів та директорій, які розміщуються на логічному або фізичному пристрої[40].

Різниця в особливостях функціонування файлових систем Windows і Linux також є суттєвою.

Linux пропонує такі можливості:

- а) початок роботи з основного каталогу розділу системи з подальшим підключенням дисків, розташованих в необхідних підкаталогах;
- б) сортування файлів по каталогам з урахуванням типу;
- в) розташування пристроїв зберігання за алфавітом, а розділів — в нумерованих списках.

Файли в Windows розміщуються з такими особливостями:

- а) аналогічна Linux класифікація розділів і дисків, проте з приховуванням даної інформації (ми бачимо, наприклад, диски C і D);
- б) розташування кожної програми в окремій директорії з наявністю налаштувань, ресурсів і файлів.

Зазвичай, файлова система Windows більш комфортна для початківців.

Говорячи про особливості зберігання налаштувань, важливо враховувати не тільки комфорт для користувачів, але і питання безпеки. У випадку з Лінукс настройки мають наступні характеристики:

- а) зберігаються в стандартних файлах;
- б) застосовуються для всіх користувачів;
- в) у випадку з програмними настройками — розміщені в прихованих підкаталогах.

Windows пропонує дещо інше рішення:

- а) налаштування збережені у реєстрі;

б) є поділ по ключам і гілках, завдяки чому можна забезпечити оперативний доступ;

в) можливо змінювати налаштування ПО в віддаленому режимі.

Незважаючи на те, що обидва варіанти рішень є безпечними, у випадку з Віндовс є очевидний недолік, а саме – відсутність можливості перенесення налаштувань. З точки зору зберігання налаштувань плюси і мінуси є як в Windows-, так і в Linux-системах.

Якщо в питанні особливостей зберігання налаштувань системи знаходяться на рівних, то з керуванням оновленнями і програмами – дещо інша ситуація. Вибираючи сервер з ОС Лінукс, зверніть увагу, що:

а) є в наявності репозиторії пакетів програмного забезпечення;

б) потреби завантажувати з інтернету ПО немає, що забезпечує високий рівень безпеки і безперебійності оновлень.

Windows має такі характеристики:

а) потреба в самостійному завантаженні інсталяції програмного забезпечення;

б) самостійне оновлення програм.

Таким чином, в цьому питанні операційні системи Linux наділені більш вагомими перевагами[5].

Отже, порівнявши всі особливості операційних систем на базі Лінукс і Windows, я дійшов до висновку, що Windows Server по всім критеріям набагато краще підходить до вирішення мого завдання(у випадку університету з великою кількістю машин, централізована система керування користувачами, зокрема Active Directory, може бути оптимальним вибором, оскільки вона забезпечує уніфіковане управління обліковими записами та забезпечує зворотну сумісність з існуючим середовищем), а ще також тому, що в Хмельницькому Національному Університеті є налагоджені відносини з компанією Microsoft(все

університетське обладнання використовує ОС Windows та має офіційні ключі до них).

### 1.3 Постановка задачі

Постановка задачі передбачає визначення конкретних цілей та завдань, які система має вирішити, а саме:

а) зменшення роботи системних адміністраторів, використовуючи централізовану систему керування користувачами;

б) розробка імовірності відбору доступу до різних категорій інформації відповідно до ролей користувачів (студенти, викладачі, адміністративний персонал);

в) забезпечення безпеки системи за допомогою аутентифікації та авторизації користувачів;

г) реалізація механізмів контролю доступу до конфіденційної інформації, наприклад, академічних даних та особистої інформації;

д) розробка системи моніторингу та аналізу активності користувачів з метою виявлення можливих загроз безпеці;

е) розробка системи резервного копіювання, за для зменшення втрат важливих даних.

					КРБКІ.001115.01.01 ПЗ	Арк.
						22
Зм.	Арк.	№ докум.	Підпис	Дата		

## 2 ПРОЄКТУВАННЯ СИСТЕМИ ДОСТУПУ ДО РЕСУРСІВ УНІВЕРСИТЕТУ

### 2.1 Ознайомлення з інформаційними технологіями та ресурсами університету

Логічна топологія є термін, який використовується для опису архітектури механізму зв'язку для всіх вузлів мережі. Це важливе поняття в комп'ютерних мережах, оскільки воно визначає спосіб зв'язку пристроїв один з одним. Логічна топологія відрізняється від фізичної топології, яка стосується фізичного розташування пристроїв у мережі.

Логічну топологію можна підтримувати та динамічно змінювати за допомогою мережевого обладнання, такого як маршрутизатори та комутатори. Це дозволяє адміністраторам мережі налаштовувати топологію мережі відповідно до мінливих потреб організації.

Існує кілька типів логічної топології, зокрема:

а) топологія шини: усі пристрої підключаються до одного кабелю, який діє як шина;

б) кільцева топологія: кожен пристрій підключено до своїх безпосередніх сусідів, утворюючи кільце;

в) зіркоподібна топологія: усі пристрої підключені до однієї центральної точки, наприклад комутатора або концентратора;

г) меш-топологія: кожен пристрій підключений до будь-якого іншого пристрою в мережі.

Кожен тип логічної топології має свої плюси і мінуси. Наприклад, топологія шини проста і легко налаштовується, але вона може бути менш надійною, ніж інші топології, оскільки збій кабелю може вивести з ладу всю мережу. З іншого боку, сітчаста топологія є високонадійною, оскільки якщо один

пристрій виходить з ладу, інші пристрої все ще можуть спілкуватися один з одним.

Комп'ютерні мережі складаються з пристроїв, які взаємодіють між собою. Логічна топологія – це спосіб обміну даними цих пристроїв. Існують різні типи логічної топології, які можна використовувати в мережі. У цьому розділі будуть представлені три типи логічної топології: топологія шини, топологія кільця та топологія зірки.

Топологія шини – це тип логічної топології, у якій усі пристрої з'єднані одним кабелем, що називається «шиною». У цій топології дані надсилаються на всі пристрої, підключені до шини. Кожен пристрій перевіряє, чи підходять дані для нього, і, якщо ні, відкидає їх. Топологія шини найкраще підходить для невеликих простих мереж, оскільки в міру зростання мережі продуктивність може погіршуватися.

Кільцева топологія – це тип логічної топології, в якій пристрої з'єднані в замкнуте коло. Кожен пристрій підключається до попереднього та наступного пристроїв. Дані надсилаються в одному напрямку по кільцю. Кожен пристрій перевіряє, чи дані для нього, і якщо ні, передає їх на наступний пристрій. Кільцева топологія найкраще підходить для мереж, де комунікація є критичною.

Топологія «зірка» – це тип логічної топології, у якій усі пристрої підключені до одного центрального пристрою, який називається «комутатор» або «маршрутизатор». Дані надсилаються з пристрою-джерела на центральний пристрій, а потім на пристрій призначення. Кожен пристрій перевіряє, чи підходять дані для нього, і, якщо ні, відкидає їх. Топологія «зірка» найкраще підходить для великих і складніших мереж, оскільки дозволяє легко додавати або видаляти пристрої, не впливаючи на продуктивність мережі.

Логічна топологія мережі визначає, як потоки даних переміщуються між підключеними пристроями. Важливо розуміти, як ці потоки даних керуються, щоб забезпечити ефективну та надійну передачу інформації.

					КРБКІ.001115.01.01 ПЗ	Арк. 24
Зм.	Арк.	№ докум.	Підпис	Дата		



В ХНУ також є такі сервери:

- а) сервер Модульного середовища;
- б) сервер LDAP;
- в) сервери електронного середовища;
- г) сервер ISU1, ISU2;
- д) сервер резервних копій;
- е) сервер віртуальних машин;
- ж) сервер DHCP;
- з) сервер DNS;
- и) сервер відеоспостереження.

Сервер Модульного середовища являє собою місце де викладачі та студенти можуть обмінюватись інформацією стосовно навчання. Це може бути різна текстова інформація, файли, посилання, методички та тести. Як викладач так і студент може завантажувати свої файли з виконаним завданням, на перевірку, і потім відстежувати свої оцінки. Для захисту викладачів і студентів, працюючих у модульному середовищі, зроблено наступні заходи:

а) використовується шифрований канал зв'язку між сервером та клієнтським комп'ютером;

б) на сервері встановлено антивірусну програму, яка сканує всі файли, що завантажуються користувачами на сервер (наприклад, викладачі завантажують файли з методичними вказівками, студенти – файли з відповідями на деякі завдання).

Для шифрування каналу зв'язку використовується спеціальний серверний сертифікат, який виконує роль своєрідного ключа і гарантує для користувача, що сервер не є якоюсь пасткою. Звичайно ми генеруємо такий сертифікат за параметрами нашого сервера, який потім необхідно надіслати і підписати в одній з довірених міжнародних організацій. Така організація здійснює ретельну перевірку нашого сервера і потім підписує сертифікат терміном на 1 або 2 роки.

					КРБКІ.001115.01.01 ПЗ	Арк. 26
Зм.	Арк.	№ докум.	Підпис	Дата		

Ця процедура коштує від \$200 до \$500. В наших умовах, на жаль, зробити це дуже складно. Тому ми самі і підписуємо свій же сертифікат. Коли браузер користувача з'єднується з сервером і отримує такий сертифікат, то враховує наш підпис сертифікату (а не довіреної організації) як порушення, про що і повідомлює користувача. При чому деякі антивірусні програми приймають таку ситуацію за небезпеку і можливість вірусної атаки. Тому користувачам, працюючим з сервером модульного середовища слід прийняти сертифікат (або зробити виключення для цього сервера – для браузерів Mozilla Firefox 3, Internet Explorer 7), не зважаючи на попередження браузера або антивірусної програми. Після цього весь потік інформації між користувачем і сервером починає шифруватися, чим і забезпечується конфіденційність у роботі.

Антивірусна програма ClamAV, що встановлена на сервері, щоденно оновлює антивірусну базу даних і забезпечує надійний захист файлів, що завантажуються користувачами. При виявленні віруса у файлі, користувача буде повідомлено про це, а файл буде переміщено із модульного середовища у спеціальну захищену папку на сервері (так званий карантин). Після цього користувачеві слід навести порядок у своїх файлах, вилучити всі віруси на своєму локальному комп'ютері, а потім повторити завантаження необхідного файлу на сервер. Слід пом'ятати, що 100%-ої надійності не дає жодна антивірусна програма, але в нашому випадку ймовірність зараження вірусом дуже мала. Як додаткові заходи безпеки в налаштуваннях параметрів модульного середовища встановлено приймати від користувачів матеріали тільки у вигляді "чистого" тексту, тобто з матеріалу вилучаються всі програмні сценарії, мульті-медіа вставки і т.ін. Тобто якщо матеріал надходить не у вигляді файлу, а вводиться безпосередньо через вікно браузера, то система очищує його від будь-яких небезпечних елементів[7].

LDAP – це аббревіатура від Lightweight Directory Access Protocol, протокол, який можна використовувати для зв'язку з DSA. LDAP є відкритим стандартом,

					КРБКІ.001115.01.01 ПЗ	Арк. 27
Зм.	Арк.	№ докум.	Підпис	Дата		

який використовує базові правила кодування (Basic Encoding Rules) підмножини ASN.1 для кодування зв'язку для кожного LDAP-повідомлення. LDAP – це протокол типу "запит-відповідь", де кожен запит супроводжується відповіддю. Існує декілька обмінів протоколом LDAP, які можуть мати один або більше запитів і нуль або більше відповідей[8].

LDAPv3 – це стандарт, визначений IETF в RFC 2251.

Обов'язково він також визначає і описує, як дані представлені в службі каталогів (модель даних або DIT). Нарешті, він визначає, як дані завантажуються (імпортуються) і зберігаються (експортуються) в службі каталогів (за допомогою LDIF). LDAP не визначає, як зберігати дані або маніпулювати ними. Зберігання даних є "автоматичним" процесом, наскільки це передбачено стандартом.

Кожне повідомлення LDAP передається як одне ціле число, що є однією з причин, чому LDAP є "легким".

Іншими словами, обміни протоколу LDAP визначають все, що ви можете зробити з LDAP, і вони повинні виконуватися окремо. (Тобто ви НЕ можете виконувати модифікацію і пошук в одній операції)[9].

Сервер LDAP в ХНУ використовується для авторизації акаунтів всіх користувачів електронного університету.

Сервери електронного середовища – це інформаційна система, яка дозволяє проводити внутрішній документообіг, викладачі можуть виставляти оцінки, реєструвати кваліфікаційні роботи, бачити свій розклад пар, заповнювати відомості. Студенти в свою чергу мають можливість відслідковувати свої оцінки, нездані дисципліни, пропуски та інше. Працівники деканату можуть складати формувати відомості та формувати групи.

Сервери ISU1, ISU2 – це сервери, які зберігають всі файли студентів, котрі робили курсові роботи, дипломні та магістерські роботи.

На цих серверах перевіряють роботи студентів на антиплагіат.

Ніхто не застрахований від того, що важливі дані можуть видалитися, пошкодитися і т.д. Звичайно, після того, як це вже сталося, махати руками пізно, необхідно заздалегідь захистити себе. Як це зробити? Все просто – використовувати резервне копіювання, його називають “бекап”. Особливо це важливо тим, що університет має багато важливих даних, які буде дуже важко або неможливо відновити без резервних копій. Для цього в університеті використовуються сервери резервних копій.

Бек-ап, резервне копіювання являє собою процес створення копії важливих файлів на додатковому носії. Напевно кожен стикався з тим, що дані з комп’ютера можуть пошкодитися або зруйнуватися в принципі і якщо у вас немає копії, то відновити важливі документи неможливо. Отже, таке копіювання служить своєрідним рятувним колом, яке допоможе відновити потрібні дані. Крім того, бек-ап знадобиться і в разі, якщо основний пристрій недоступний[10].

Сервер резервного копіювання – здійснює копіювання всіх сайтів університету(всю інформацію, яку вони зберігають) та копіювання інших серверів, які зберігають інформацію про акаунти користувачів.

Віртуалізація серверів – це процес поділу фізичного сервера на кілька віртуальних. Це ефективний і економічний спосіб використання серверних ресурсів і розгортання ІТ-сервісів в організації. Без віртуалізації серверів фізичні сервери використовують лише невелику частину своїх обчислювальних потужностей, внаслідок чого пристрої простоюють[11].

Сервер віртуальних машин використовують під різноманітні цілі університету.

DHCP – це стандартний протокол у мережі з архітектурою "клієнт-сервер", який динамічно призначає IP-адреси та іншу необхідну інформацію конфігурації для нових пристроїв у мережі. Кожен мережевий пристрій повинен мати власну, унікальну IP-адресу, щоб у мережі не виникали конфлікти. IP-адресу, звісно, можна прописати для комп’ютера вручну, тобто статично, і не змінювати її

					КРБКІ.001115.01.01 ПЗ	Арк. 29
Зм.	Арк.	№ докум.	Підпис	Дата		

надалі. У невеликих мережах, на 2-5 комп'ютерів, так іноді й робиться. Але якщо комп'ютерів у мережі десятки і сотні, то встежити за унікальністю мережевих адрес буде вельми проблематично. Хоча і в таких мережах теж можуть використовуватися статичні IP-адреси, наприклад, для принтерів.

Для автоматизації процесу призначення унікальних IP-адрес пристроям, що входять у мережу, було розроблено протокол DHCP, який працює на спеціальному сервері, що називається, відповідно, DHCP-сервер.

Користувач не помічає, як його пристрій отримує від DHCP-сервера IP-адресу і починає роботу в мережі. Бувають і ситуації, коли мережеву адресу пристрою краще прописувати постійно і не змінювати, якщо це, наприклад, основний сервер або принтер. Тому в протоколі DHCP використовується резервування, тобто область IP-адрес, зарезервована для статичного призначення певним пристроям.

DHCP-сервер автоматично розподіляє і оновлює IP-адреси та іншу інформацію конфігурації комп'ютерів (DHCP-клієнтів) у мережі. Для DHCP-клієнтів ця інформація надається за допомогою обміну повідомленнями, порядок яких визначається протоколом DHCP, і такий обмін називається DHCP-транзакцією. Якщо DHCP-сервер і DHCP-клієнт розташовані в різних підмережах (subnets), то використовується агент-ретранслятор DHCP (DHCP relay agent), щоб DHCP-транзакцію можна було провести між різними підмережами.

DHCP, як визначено в документі RFC 2131, був розроблений на базі протоколу BOOTP (Bootstrap Protocol), за допомогою якого клієнт може автоматично отримати IP-адресу, зазвичай, під час завантаження комп'ютера[12].

Університет також використовує DHCP-сервер, який забезпечує функціонування всіх мережевих пристроїв між собою.

Система доменних імен (DNS) – це телефонна книга Інтернету. Коли користувачі вводять доменні імена, такі як "google.com" або "nytimes.com" у веб-

					КРБКІ.001115.01.01 ПЗ	Арк. 30
Зм.	Арк.	№ докум.	Підпис	Дата		

браузери, DNS відповідає за пошук правильної IP-адреси для цих сайтів. Потім браузері використовують ці адреси для зв'язку з серверами походження або граничними серверами CDN, щоб отримати доступ до інформації веб-сайту. Все це відбувається завдяки DNS-серверам: машинам, призначеним для відповіді на DNS-запити[13].

Такий сервер є і в Хмельницькому Національному Університеті.

## 2.2 Вимоги до системи доступу до ресурсів університету та проектування її архітектури

Система доступу до інформаційних ресурсів університету повинна відповідати вимогам сучасного освітнього середовища, де швидкий та зручний доступ до різноманітної інформації є ключовим фактором для успішного навчання, досліджень та управління. Ось деякі вимоги, які можуть бути поставлені до такої системи:

- а) універсальний доступ;
- б) безпека і конфіденційність;
- в) легкість використання;
- г) масштабованість;
- д) швидкодія.

Система повинна бути доступною для всіх учасників університетської спільноти, включаючи студентів, викладачів, дослідників та адміністративний персонал. Також система повинна бути легкою в керуванні та адмініструванні, адже в університеті доволі часто змінюються дані про користувачів, які потрібно оновлювати.

Враховуючи чутливість деяких даних, система повинна забезпечувати високий рівень безпеки та конфіденційності, зокрема захист від несанкціонованого доступу та зловмисних атак.

Інтерфейс системи має бути інтуїтивно зрозумілим та зручним для користувачів різного рівня технічної підготовки.

Система повинна бути здатна ефективно масштабуватися для відповіді на зростаючі потреби університету, якщо це необхідно.

Час відклику системи повинен бути мінімальним, щоб забезпечити ефективне використання часу користувачів.

Основні компоненти архітектури:

- а) клієнтська частина;
- б) серверна частина;
- в) мережевий інфраструктурний рівень;
- г) централізоване управління.

В клієнській частині буде Веб-портал в якому буде представлений інтерфейс для користувачів, через який вони отримують доступ до ресурсів. Портал буде інтуїтивно зрозумілим та підтримувати різні типи пристроїв (ПК, планшети, смартфони).

В серверній частині будуть такі компоненти як: сервер аутентифікації та авторизації, сервери зберігання даних та сервери додатків.

Сервери авторизації та аутентифікації – це зовнішні джерела облікових записів користувачів, наприклад, LDAP-сервер, або сервери, що здійснюють автентифікацію для UserGate, наприклад Radius, TACACS+, Kerberos, SAML. Сервери зберігання даних – це сервери для зберігання навчальних матеріалів, дослідницьких даних, адміністративної інформації тощо[24].

Сервер додатків (англ. application server) – сервер, що виконує деякі прикладні програми. Термін також відноситься і до програмного забезпечення, встановленому на такому сервері й забезпечує виконання прикладного ПЗ[25].

Сервери для зберігання інформації та даних – забезпечення безпеки бізнесу за рахунок високого рівня централізації даних, конфіденційності, резервного копіюванню даних, тощо[26].

Мережевий інфраструктурний рівень включатиме в себе віртуальні приватні мережі (VPN) та брандмауери та системи захисту від вторгнень (IDS/IPS). Для безпечного віддаленого доступу та для захисту мережі від зовнішніх та внутрішніх загроз.

Централізоване управління являтиме собою систему моніторингу та управління і централізоване сховище облікових записів. В системі моніторингу будуть інструменти для моніторингу стану системи, управління ресурсами та виявлення потенційних проблем. Сховище облікових записів буде використовувати Active Directory для централізованого управління обліковими записами користувачів.

В моїй системі доступу до ресурсів університету будуть такі ролі як:

- а) системний адміністратор;
- б) адміністратор резервного копіювання;
- в) робітника бухгалтерії;
- г) робітника відділу кадрів;
- д) викладача;
- е) аспіранта;
- ж) студента;
- з) працівника робочого персоналу.

Системний адміністратор (від англ. system administrator, systems administrator) – працівник, посадові обов'язки якого передбачають забезпечення роботи комп'ютерної техніки, комп'ютерної мережі і програмного забезпечення в організації. Інша назва – сисадмін, sysadmin (прийшла з комп'ютерного сленгу). Системний адміністратор може бути, в залежності від розміру організації, або

працівником підрозділу інформаційних технологій, або окремою штатною одиницею[15].

В університеті він має найвищий ступінь прав та дозволів до інформаційних ресурсів, для того щоб забезпечувати безпеку та безперебійну роботу системи.

Ще повинні бути адміністратори резервного копіювання, які відповідають за бек-апи найрізноманітніших систем університету. Вони мають тільки ті права, які дозволяють їм виконувати свої обов'язки.

Далі потрібно додати ролі студента, викладача, аспірантів, відділу кадрів, бухгалтерії та робочий персонал(прибиральниці, охорона і інші).

Роль студента – може тільки переглядати свої дані, не може нічого вносити, окрім файлів на перевірку викладачу.

Роль викладача – може переглядати та змінювати дані по оцінках студентів, наповнення навчального матеріалу на своєму курсі.

Роль аспіранта – така ж як викладача, але з меншими можливостями.

Роль працівника відділу кадрів – має можливість додавати нових працівників університету, робити різні маніпуляції з даними працівників, але ніяк не можуть впливати на оцінки студентів.

Роль працівника бухгалтерії – мають доступ до інформації пов'язаної з фінансовими питаннями як студентів, так і інших працівників.

Роль працівника робочого персоналу – має можливість переглядати актуальні дані та відомості відносно нього.

### 2.3 Проєктування структури домену та планування домену

У контексті інформаційних систем домен — це логічна група комп'ютерів, користувачів та інших ресурсів, яка адмініструється як єдине ціле. Домени

					КРБКІ.001115.01.01 ПЗ	Арк.
						34
Зм.	Арк.	№ докум.	Підпис	Дата		

використовуються для централізованого управління доступом до ресурсів, підвищення безпеки та спрощення адміністрування мережі.

Огляд принципів доменної структури:

- а) єдиний домен;
- б) багатодоменна структура;
- в) дерево доменів;
- г) ліс доменів.

Єдиний домен включає всі ресурси організації в одному домені. Простота адміністрування та єдині політики безпеки. Підходить для невеликих організацій або відділів.

Багатодоменна структура – це кілька доменів, кожен з яких управляється окремо. Забезпечує масштабованість та покращену безпеку. Може використовуватися для розділення різних відділів або підрозділів.

Дерево доменів – це ієрархія доменів, де один домен є батьківським для інших. Дозволяє легко керувати складними організаційними структурами. Полегшує управління правами доступу між доменами.

Ліс доменів – це множина дерев доменів, які об'єднані спільними схемами та глобальним каталогом. Використовується для дуже великих організацій з численними відділами. Забезпечує високу гнучкість та масштабованість[16].

Моя система доступу до інформаційних ресурсів університету буде базуватись на домені – khmnu.edu.ua.

Інфраструктура домену і його піддоменів зображена на рисунку 2.2.

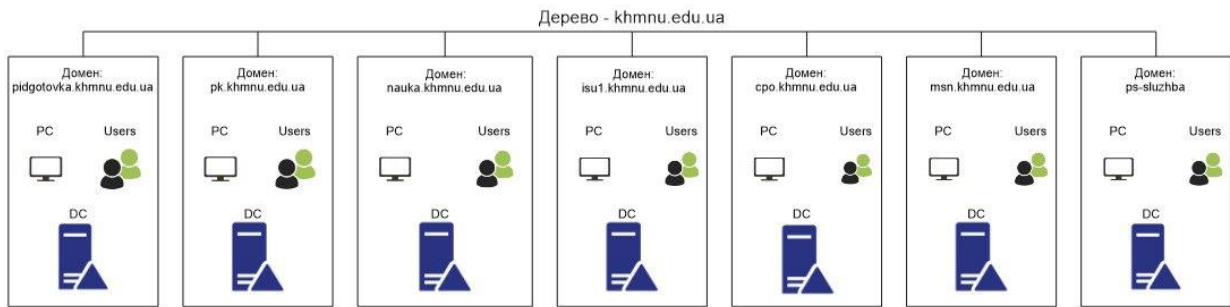


Рисунок 2.2 – Інфраструктура домену khmnu.edu.ua

В Хмельницькому Національному Університеті є такі піддомени:

- а) pk;
- б) nauka;
- в) isu1;
- г) pidgotovka;
- д) spro;
- е) msn;
- ж) ps-sluzhba та інші.

Pk – це піддомен на якому зосереджена інформація для абітурієнтів та вступникам до магістратури. Також там відображаються останні новини на тему вступу, нормативні документи, додаткова інформація для вступників та контакти приймальної комісії[17].

Nauka – це піддомен де відображається інформація про наукову діяльність університету, інформація про проректора з наукової роботи, посилання на наукову бібліотеку, положення, звіти з науки, послуги та на найкращих науковців[18].

Isu1 – це піддомен, який в себе включає інформаційну систему «Електронний університет». В ній користувачі можуть знайти інформацію про випускників, каталог вибіркових дисциплін, ЄКТС інформаційний пакет, положення про щорічне рейтингове оцінювання роботи науково-педагогічних

працівників, інструкцію по роботі з персональними даними, календар. Також на головній сторінці відображаються співробітники в яких недавно, або сьогодні день народження. Авторизовані користувачі мають більше доступу до різної інформації в залежності від їх ролі. Студенти мають право переглядати свій розклад предметів, оцінки по предметам, атестації, КР та інше. Викладачі в свою чергу мають інші права, які їм дозволяють змінювати інформацію таку як оцінки в журналах та інше[19].

Pidgotovka – це піддомен підготовчого відділення. На цьому піддомени можна знайти інформацію про курси з підготовки до єдиного вступного іспиту для бакалаврів, а саме – дати, адресу, телефон, положення про підготовче відділення, документи, які потрібні для зарахування на курси. Також ще є інформація і для учнів 9, 10, 11, класів школи, котрі можуть записатися на курси по підготовці до ЗНО, ДПА, творчих конкурсів, фахового іспиту з іноземної мови, курси з англійської мови для вступу до магістратури[20].

Сро – це піддомен центру післядипломної освіти. На ньому відображається інформація про підвищення кваліфікації педагогічних працівників[21].

Msn – це піддомен модульного середовища для навчання. Воно викисовується зокрема студентами та викладачами для обміну інформацією, щодо навчання. На головній сторінці відображаються останні новини сайту, календар, форма для входу в систему, кількість людей на сайті, посилання на інші системи та ресурси університету[22].

Ps-sluzhba – це піддомен психологічної служби. На ньому можна знайти інформацію про тренінги, які будуть/були проведені психологами ХНУ[23].

## 2.4 Висновки

У другому розділі дипломної роботи було проведено детальне дослідження та проектування системи доступу до інформаційних ресурсів університету. Основні аспекти, які були розглянуті, включають:

а) вивчено поточну інфраструктуру університету, включаючи сервери, мережеве обладнання та програмне забезпечення, що використовується для управління доступом до ресурсів;

б) проаналізовано існуючі інформаційні системи та визначено ключові потреби користувачів;

в) встановлено основні вимоги до системи доступу, які включають безпеку, зручність використання, масштабованість та інтеграцію з існуючими системами;

г) розроблено архітектуру системи, що забезпечує централізоване керування доступом до ресурсів, використовуючи сучасні технології;

д) розглянуто основні принципи побудови доменної структури, включаючи організацію доменів, піддоменів та об'єктів в Active Directory;

е) запропоновано оптимальну структуру домену для університету, враховуючи вимоги до безпеки та управління доступом.

Узагальнюючи, в цьому розділі було закладено фундамент для впровадження ефективної та надійної системи доступу до інформаційних ресурсів університету. Запропоновані рішення забезпечать високий рівень безпеки, зручність адміністрування та відповідатимуть сучасним стандартам інформаційної безпеки.

Це дозволить університету не лише оптимізувати процеси управління доступом, але й забезпечить надійний захист конфіденційної інформації та зручний доступ для всіх користувачів.

### 3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ СИСТЕМИ ДОСТУПУ ДО РЕСУРСІВ УНІВЕРСИТЕТУ

#### 3.1 Встановлення та налаштування серверної операційної системи Windows Server 2019

VirtualBox — це програма віртуалізації для операційних систем, розроблена німецькою фірмою Innotek, зараз вона належить Oracle Corporation. Вона встановлюється на наявну операційну систему, яка називається хостовою, усередину цієї програми встановлюється інша операційна система, яку називають гостьовою операційною системою[27].

Windows Server 2019 — це серверна операційна система від компанії Microsoft, яка є частиною сімейства Windows NT. Була анонсована 20 березня 2018 року. Від початку компанія хотіла випустити Windows Server 2016 R2[28].

Windows 10 – операційна система для персональних комп'ютерів та робочих станцій, розроблена корпорацією Microsoft у рамках сімейства Windows NT. Випущена у липні 2015 року. Після Windows 8.1 система отримала номер 10, міняючи 9. Серверні аналоги Windows 10 – Windows Server 2016, Windows Server 2019 та Windows Server 2022[29].

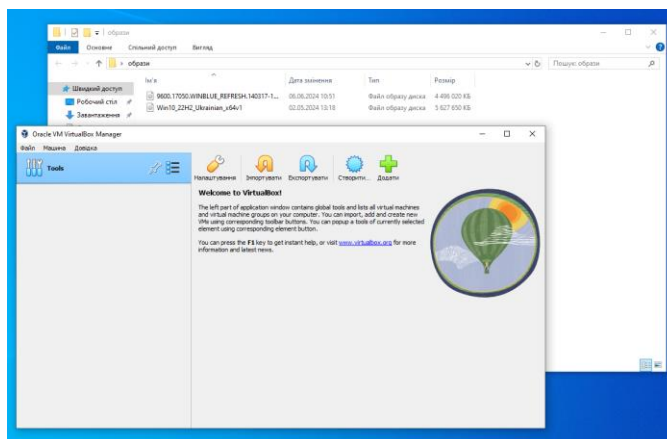


Рисунок 3.1 – Програма Oracle VM VirtualBox та образи ОС Windows Server та Windows 10 Pro

Для встановлення операційної системи Windows Server 2019 було інстальовано програму віртуалізації Oracle VM VirtualBox і завантажено образи ОС Windows Server 2019 та Windows 10 Pro, яка необхідна для тестування системи та імітування користувача. Цей процес відображено на рисунку 3.1.

У програмі VirtualBox було натиснуто кнопку «Створити» для створення віртуальної машини під назвою "Server 1 – основний сервер". Інші налаштування цієї віртуальної машини показані на рисунку 3.2. На рисунку 3.3 показані вибрані ім'я та пароль до облікового запису, який буде встановлено за замовчуванням.

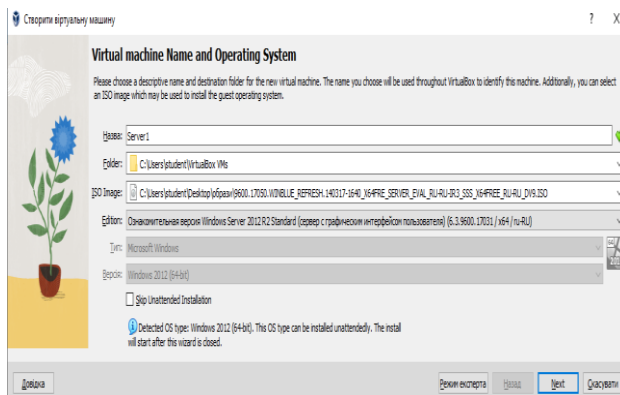


Рисунок 3.2 – Вибір назви, типу та образу ОС віртуальної машини

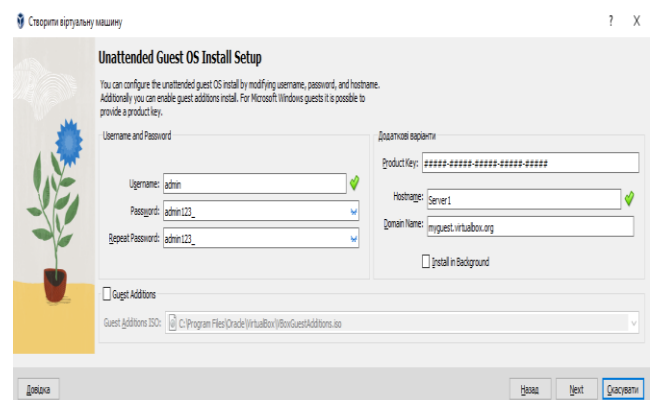


Рисунок 3.3 – Вибір ім'я та паролю облікового запису ОС

На наступному рисунку 3.4 показано вибір кількості оперативної пам'яті та кількості ядер процесора, які виділені для віртуальної машини. Оптимальними значеннями для цього завдання є 2048 МБ оперативної пам'яті та 2 ядра процесора. Цей вибір обумовлений необхідністю іноді використовувати 2 або 3 віртуальні машини одночасно на одному комп'ютері.

Далі, на рисунку 3.5 показано вибір типу пам'яті та її розміру для зберігання файлів віртуальної машини.



Рисунок 3.4 – Виділення оперативної пам'яті та ядер процесора на віртуальну машину

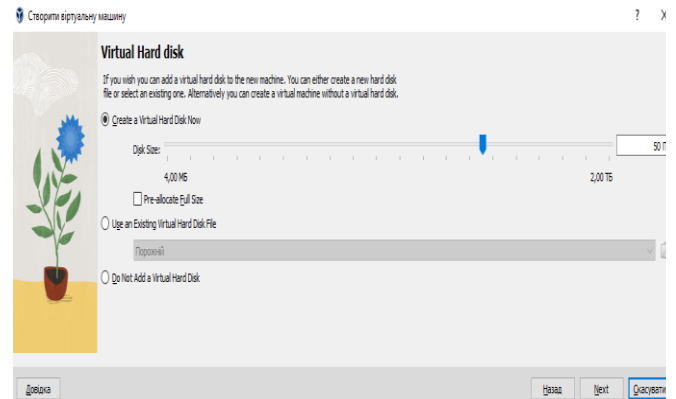


Рисунок 3.5 – Вибір типу та розміру виділення пам'яті під віртуальну машину

На рисунках 3.6-3.8 показано процес доналаштування віртуальної машини Server 1 шляхом вибору відповідних налаштувань.

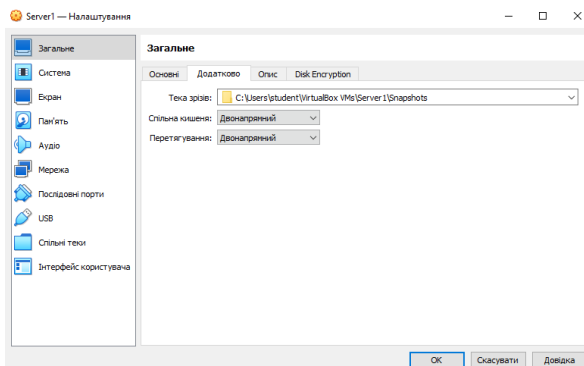


Рисунок 3.6 – Вікно «Загальне»

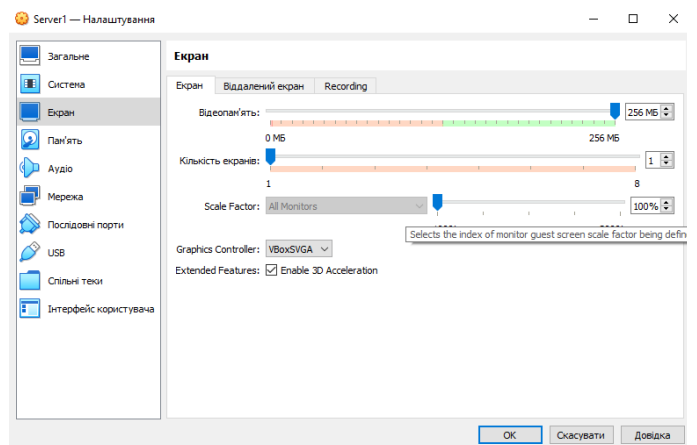


Рисунок 3.7 – Вікно «Екран»

Зм.	Арк.	№ докум.	Підпис	Дата

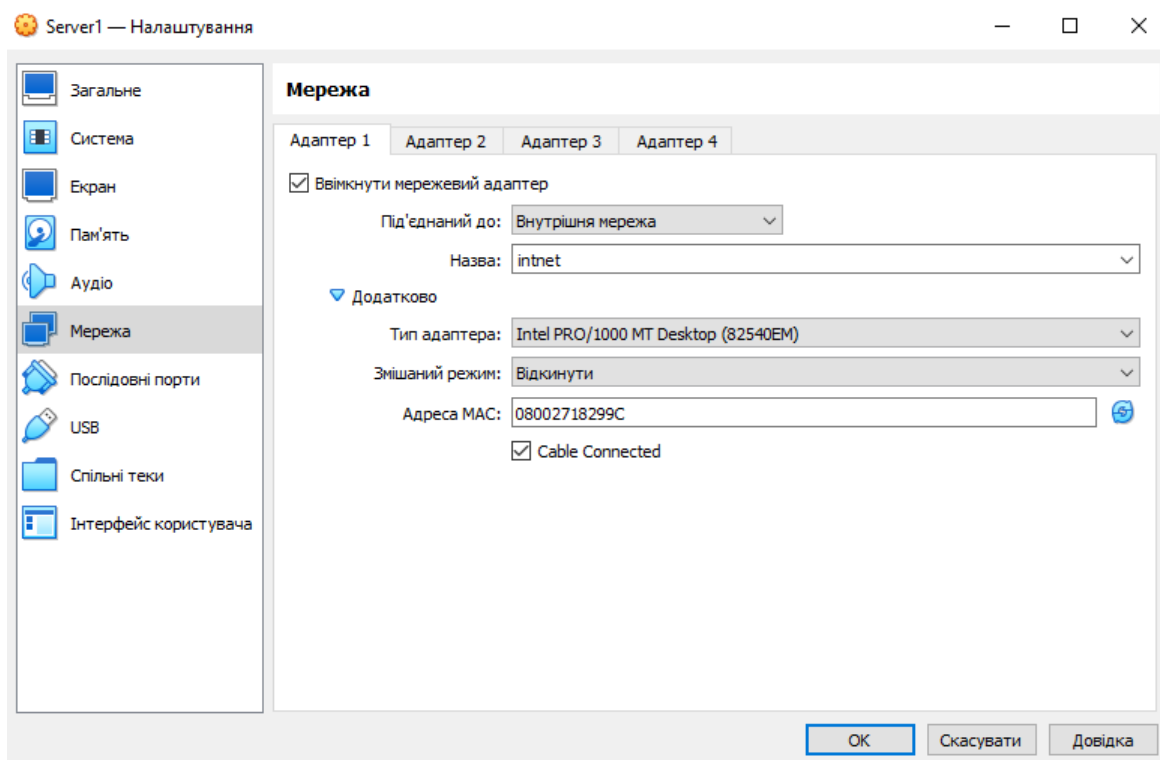


Рисунок 3.8 – Вікно «Мережа»

Після додаткових налаштувань віртуальну машину запущено шляхом натискання кнопки «Запустити». На рисунку 3.9 показано процес інсталяції операційної системи Windows Server 2019.

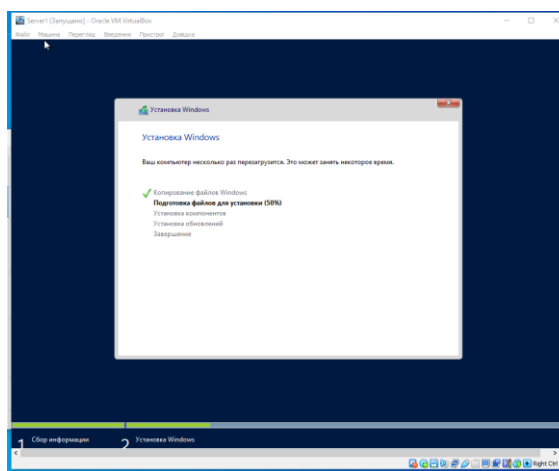


Рисунок 3.9 – Встановлення ОС Windows Server 2019

Після інсталяції та запуску операційної системи віртуальної машини було встановлено гостьові доповнення. Процес їх встановлення після перезапуску системи зображено на рисунках 3.10-3.13.

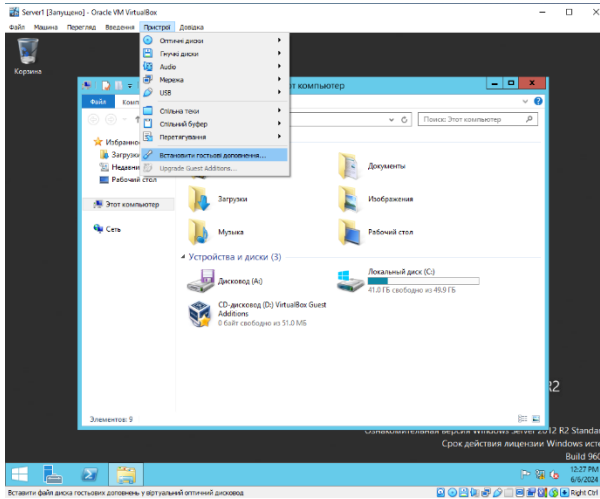


Рисунок 3.10 – Встановлення гостьових доповнень

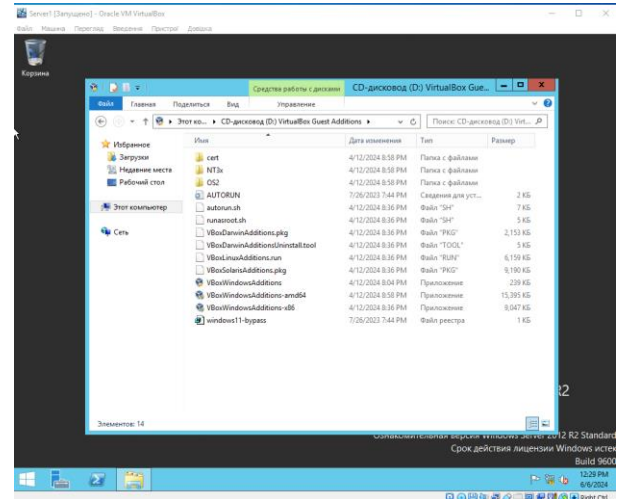


Рисунок 3.11 – Вибір 64-бітного встановлювача

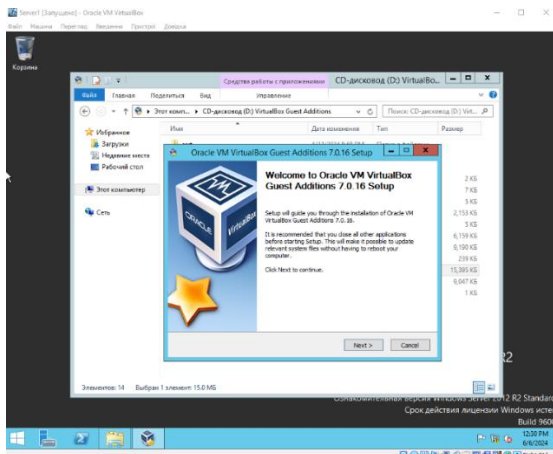


Рисунок 3.12 – Вітальне вікно встановлювача гостьових доповнень

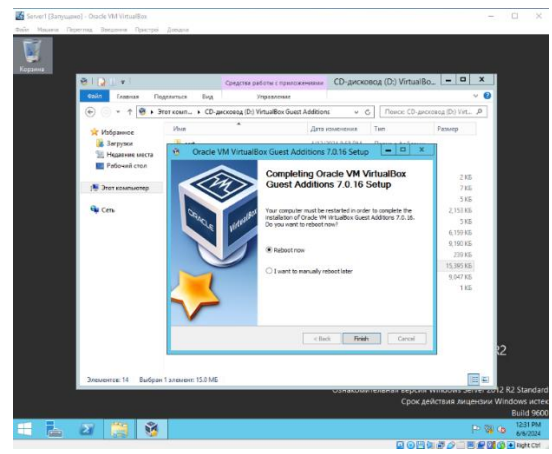


Рисунок 3.13 – Вибір чи робити перезапуск системи після встановлення

Зм.	Арк.	№ докум.	Підпис	Дата

Після виконання всіх маніпуляцій встановлено віртуальну машину з серверною ОС Windows Server 2019 успішно. Потім була встановлена ще одна ідентична віртуальна машина під назвою Server 2 для налаштування відмовостійкості системи. Після цього була встановлена клієнтська віртуальна машина з ОС Windows 10 Pro, названа Workstation. Налаштування Workstation ідентичні налаштуванням серверних машин, за винятком деяких параметрів, що показані на рисунку 3.14.

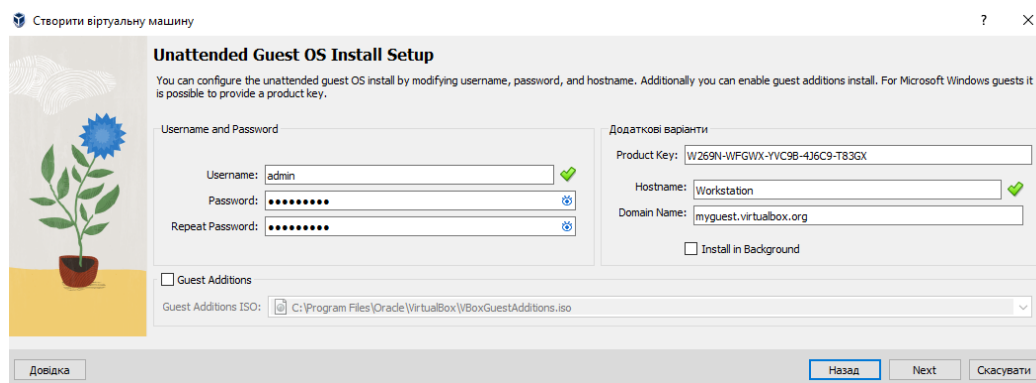


Рисунок 3.14 – Налаштування Windows 10 Pro

3.2 Розгортання служби Active Directory. Налаштування DHCP, DNS та другого сервера. Налаштування відмовостійкості на другому сервері

### 3.2.1 Розгортання служби Active Directory

Active Directory — LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows NT. Active Directory дозволяє адміністраторам використовувати групові політики (GPO) для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою Microsoft Systems Management Server 2003 (або System Center Configuration Manager)), встановлювати оновлення ОС,

						КРБКІ.001115.01.01 ПЗ	Арк. 44
Зм.	Арк.	№ докум.	Підпис	Дата			



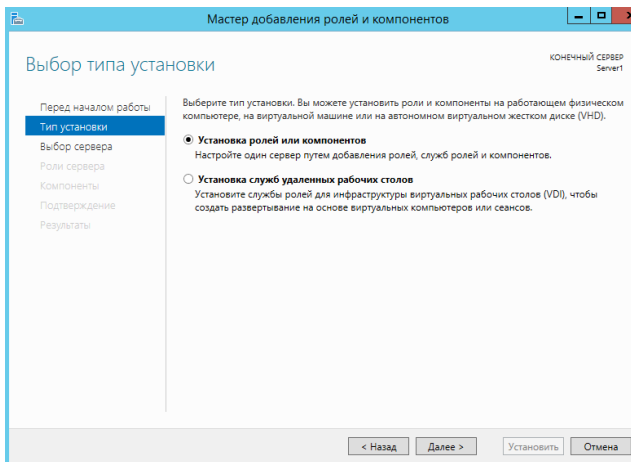


Рисунок 3.17 – Вибір типу встановлення

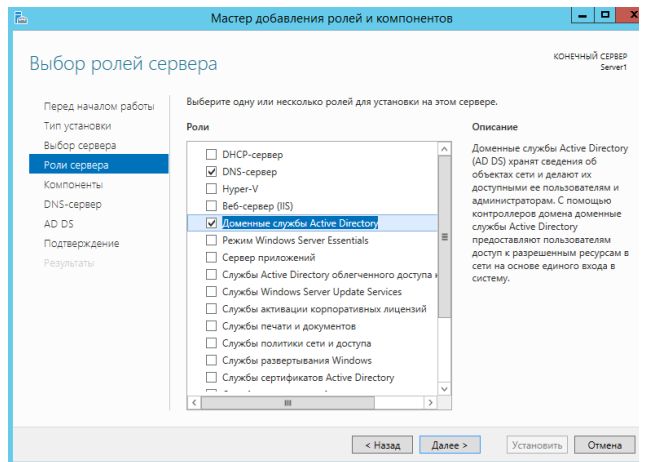


Рисунок 3.18 – Вибір ролей серверу

Після встановлення в Диспетчері серверів з'явилося повідомлення про необхідність завершити налаштування служби Active Directory. Тому було натиснуто на прапорець і обрано пункт «Підвищити роль цього сервера рівня контролера домену» (див. рис. 3.19).

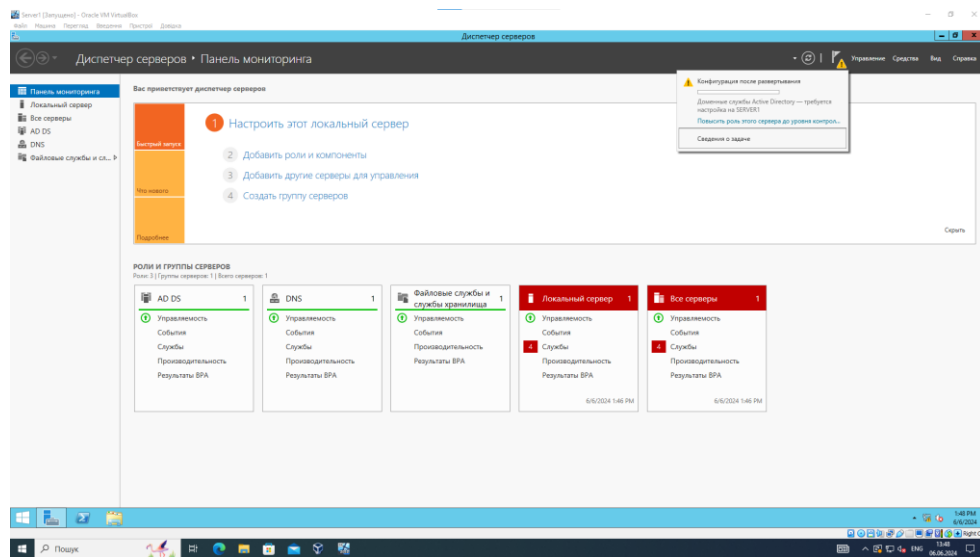


Рисунок 3.19 – Пункт «Підвищити роль цього сервера рівня контролера домену»

На рисунках 3.20-3.23 були обрані відповідні налаштування в майстрі налаштування доменних служб Active Directory.

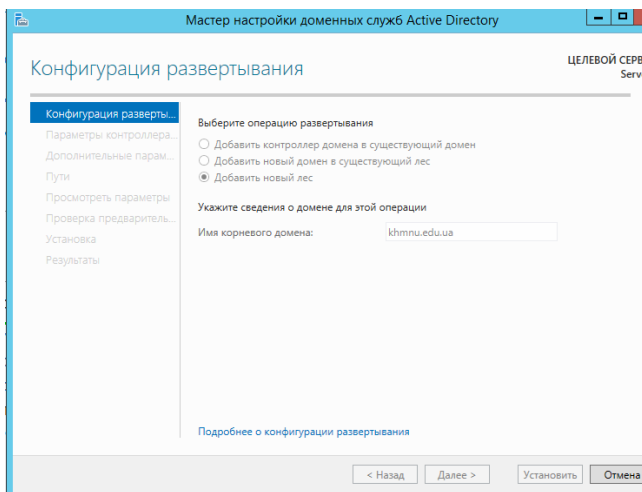


Рисунок 3.20 – Вкладка «Конфігурація розгортання»

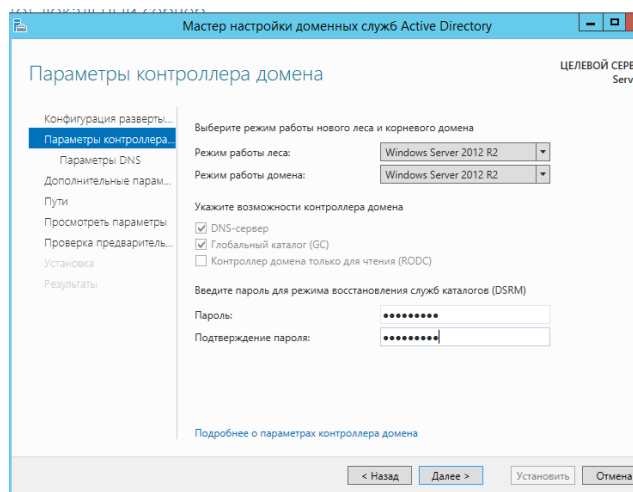


Рисунок 3.21 – Вкладка «Параметри контролера домену»

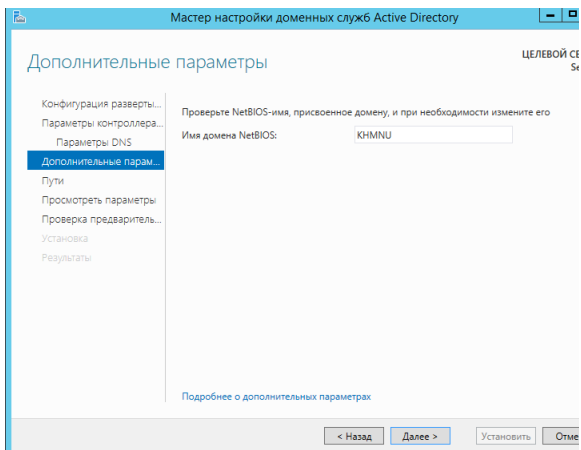


Рисунок 3.22 – Вкладка «Додаткові параметри»

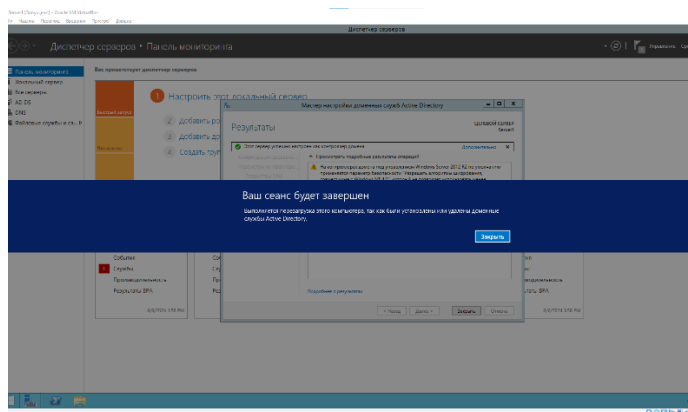


Рисунок 3.23 – Перезавантаження Server 1 після встановлення Active Directory

Після перезапуску системи обліковий запис адміністратора, який був створений за замовчуванням після інсталяції, було відключено, а новий обліковий запис було створено з усіма правами доступу та повноваженнями, як показано на рисунках 3.23-3.30.

На рисунку 3.24 було створено новий підрозділ під назвою "Khmel'nitskiy", в якому створено підрозділи Admins, Students та інші.

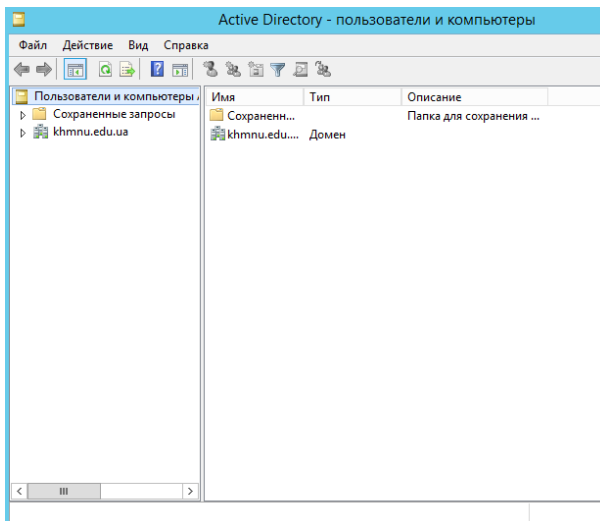


Рисунок 3.23 – Вікно «Active Directory – користувачі та комп'ютери»

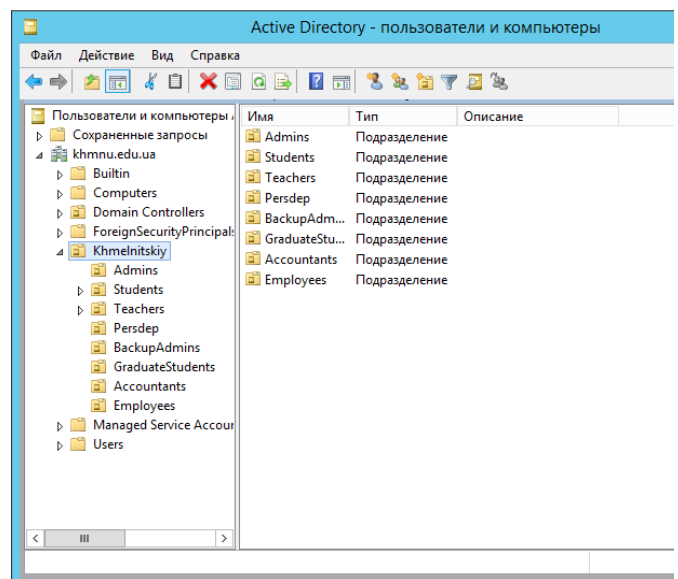


Рисунок 3.24 – Створення нових підрозділів

Обліковий запис адміністратора, який був створений за замовчуванням, було переміщено в підрозділ Admins, як показано на рисунку 3.25.

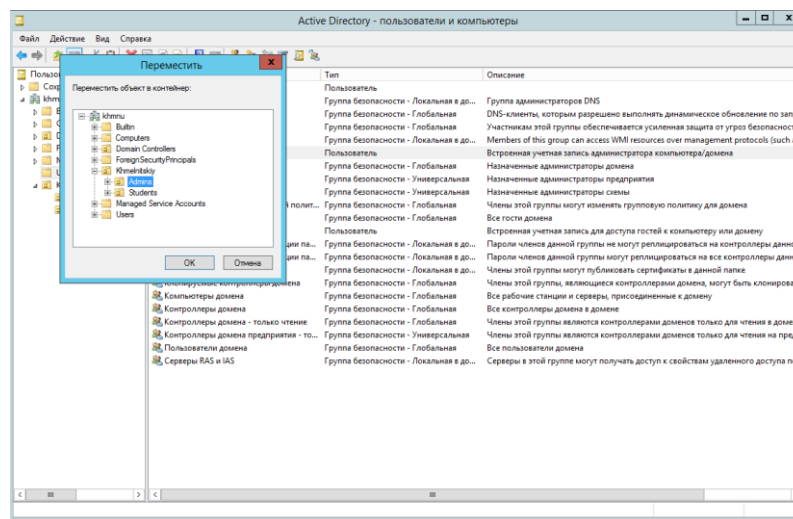


Рисунок 3.25 – Переміщення облікового запису адміністратора

Далі на рисунках 3.26-3.28 був створений новий обліковий запис адміністратора і налаштовані його права доступу.

Зм.	Арк.	№ докум.	Підпис	Дата

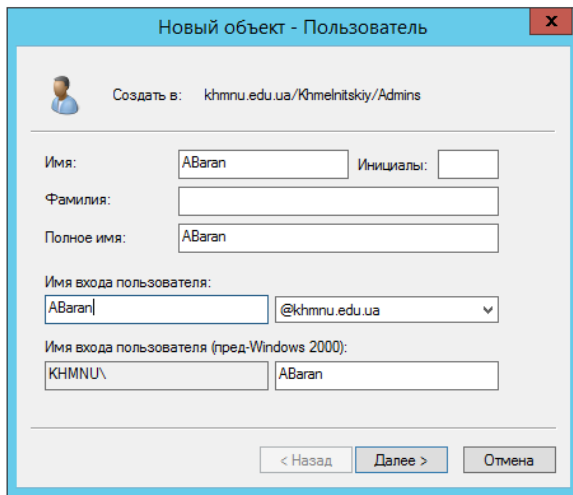


Рисунок 3.26 – Створення нового адміністратора

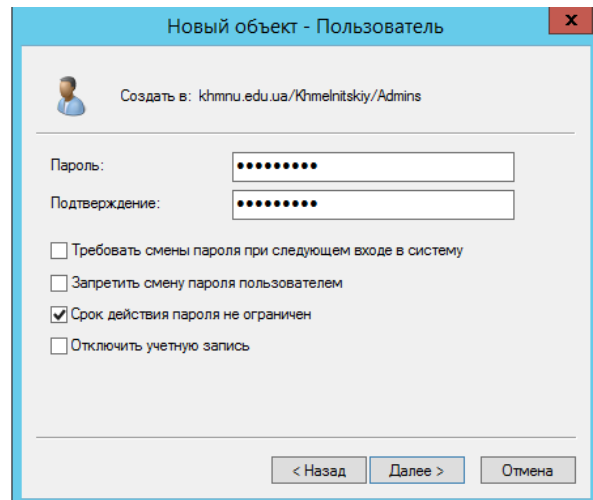


Рисунок 3.27 – Встановлення паролю адміністратора

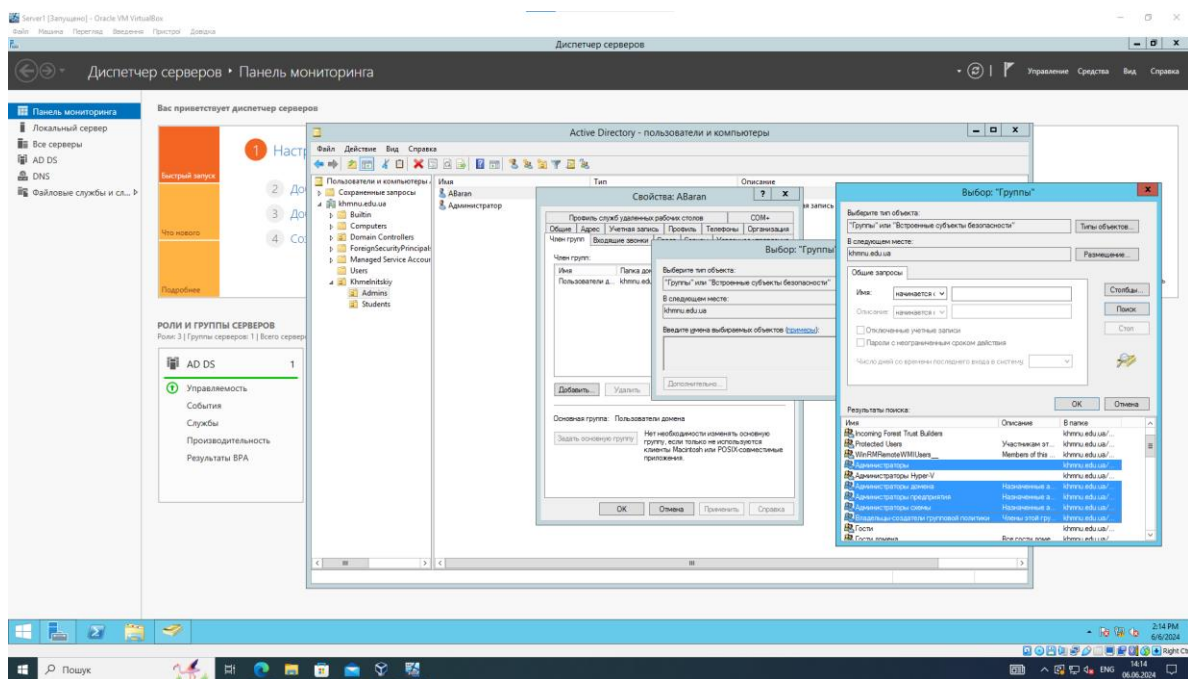


Рисунок 3.28 – Надання прав доступу адміністратору

Після цих дій авторизувалися в тільки що створений обліковий запис для того, щоб відключити обліковий запис, який був створений за замовчуванням, як показано на рисунках 3.29-3.30.

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

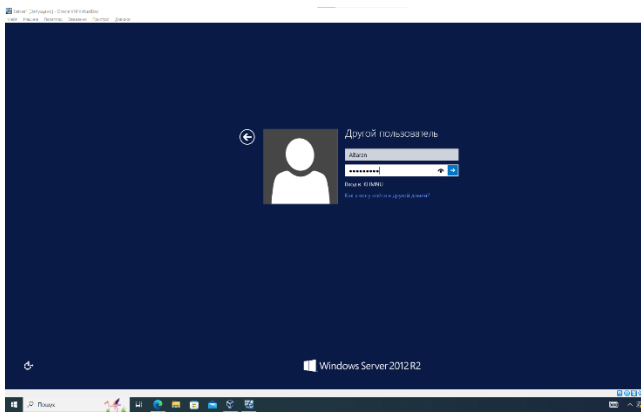


Рисунок 3.29 – Авторизация в новый  
обліковий запис

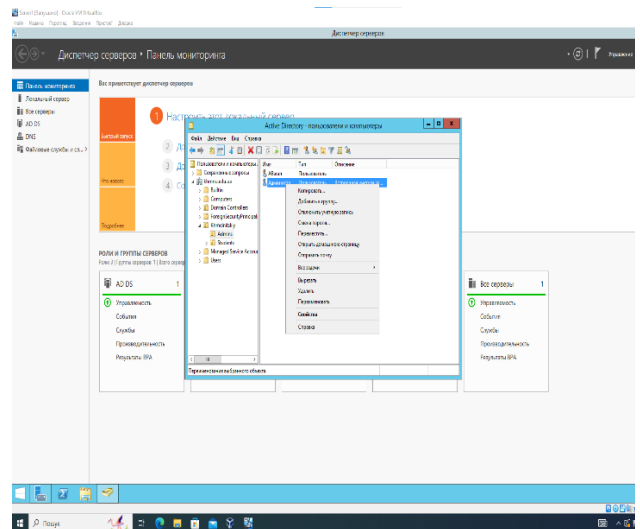


Рисунок 3.30 – Відключення старого  
облікового запису адміністратора

### 3.2.2 Налаштування DHCP, DNS та другого сервера

Для початку на Server 1 було інстальовано DHCP-сервер. Потім було відкрито «Майстер додавання ролей та компонентів», аналогічно до встановлення Active Directory, і обрав компонент DHCP-сервер.

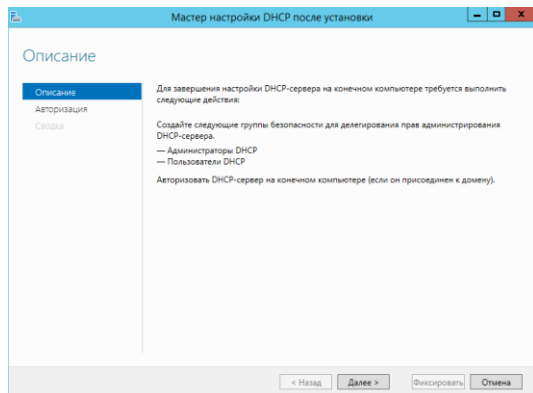


Рисунок 3.31 – «Майстер  
налаштування DHCP після  
встановлення»

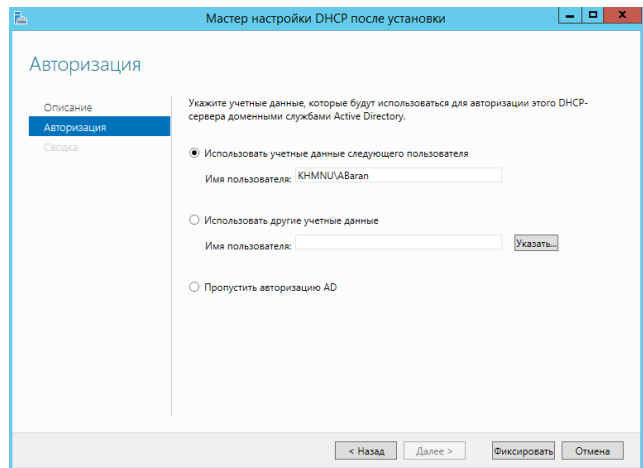


Рисунок 3.32 – Вкладка «Авторизация»

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

Після цього було натиснуто кнопку «Завершення налаштування DHCP» для завершення встановлення, як показано на рисунках 3.31-3.32.

Після встановлення було налаштовано DHCP. Для цього в меню «Засоби» обрано «DHCP» і в IPv4 я створено нову область. Це показано на рисунках 3.33-3.42.

Рисунок 3.33 – Вибір імені області

Рисунок 3.34 – Вибір діапазону адресів

Рисунок 3.35 – Вибір виключень та затримки

Рисунок 3.36 – Вибір строку дії оренди адреси

Зм.	Арк.	№ докум.	Підпис	Дата

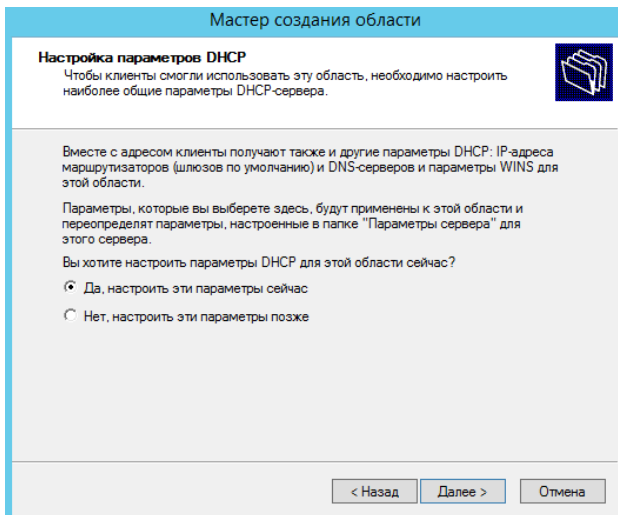


Рисунок 3.37 – Вибір налаштування параметрів DHCP

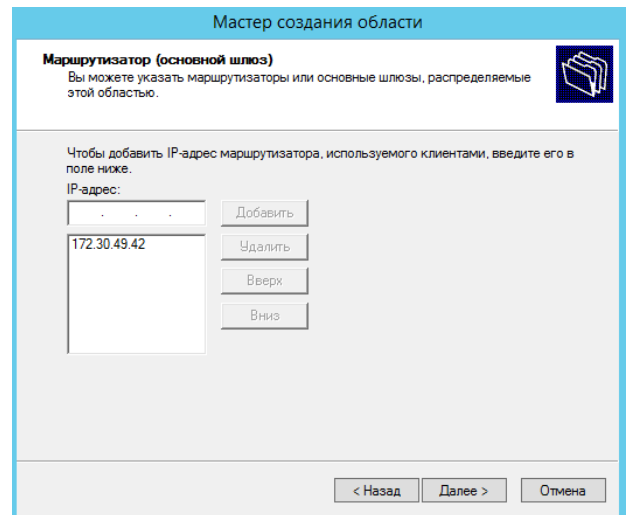


Рисунок 3.38 – Додавання IP-адреси основного шлюзу

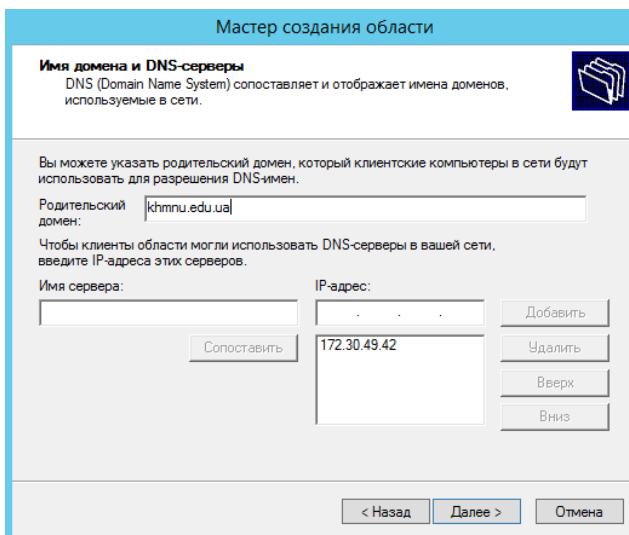


Рисунок 3.39 – Вибір домена та DNS-сервера

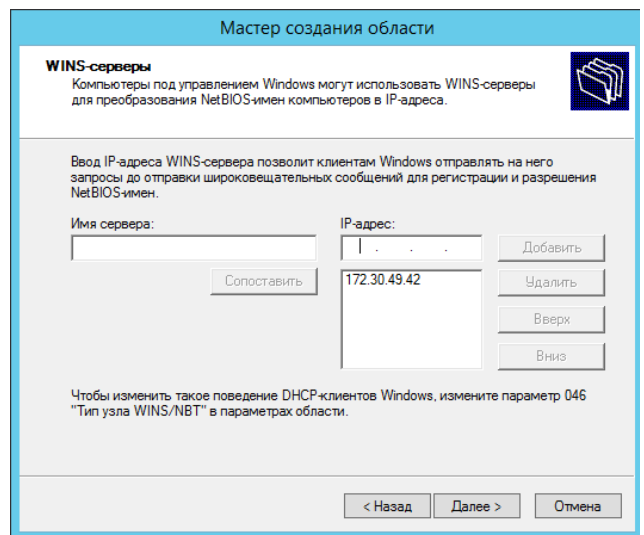


Рисунок 3.40 – Вибір WINS-сервера

Зм.	Арк.	№ докум.	Підпис	Дата

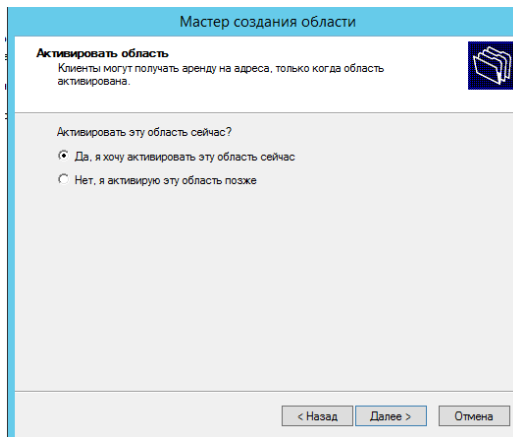


Рисунок 3.41 – Вибір активації області

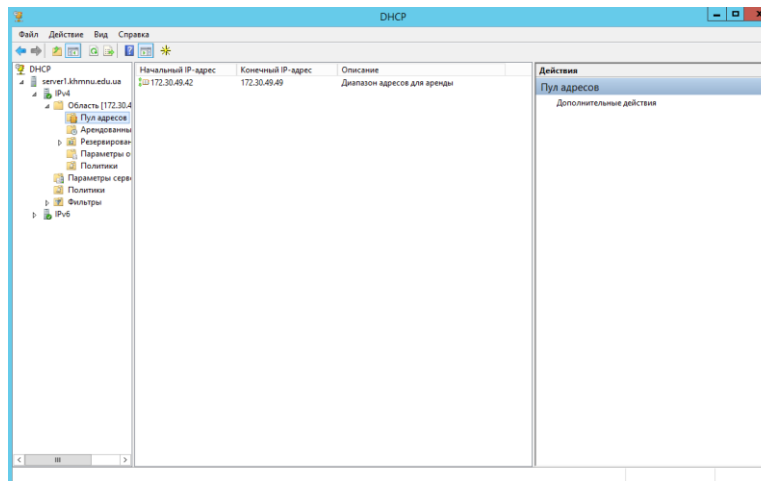


Рисунок 3.42 – Створена нова область

Далі було налаштовано DNS, а саме зон прямого та зворотного перегляду(рис. 3.43-3.48).

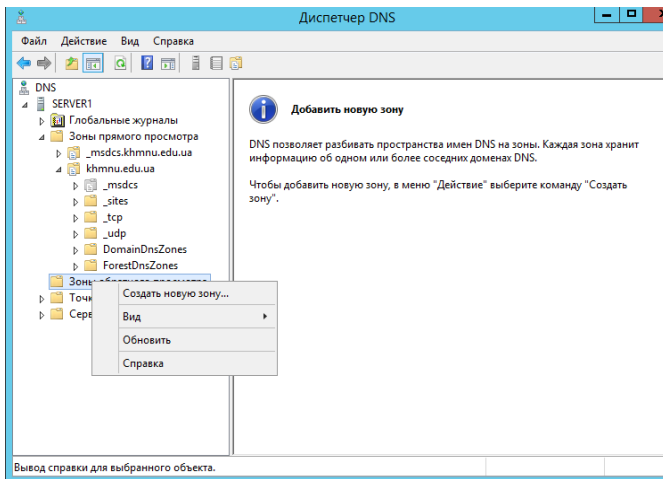


Рисунок 3.43 – Створення нової зони

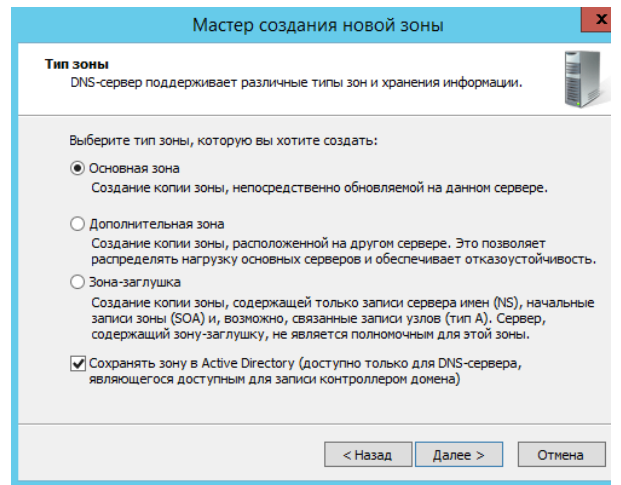


Рисунок 3.44 – Вибір типу зони

Зм.	Арк.	№ докум.	Підпис	Дата

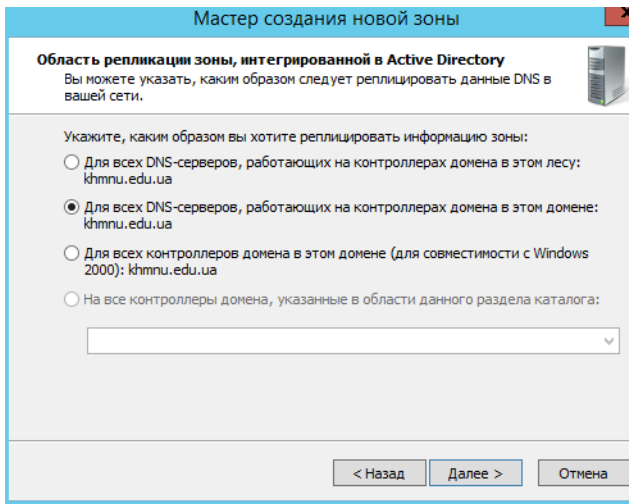


Рисунок 3.45 – Вибір області реплікації зони

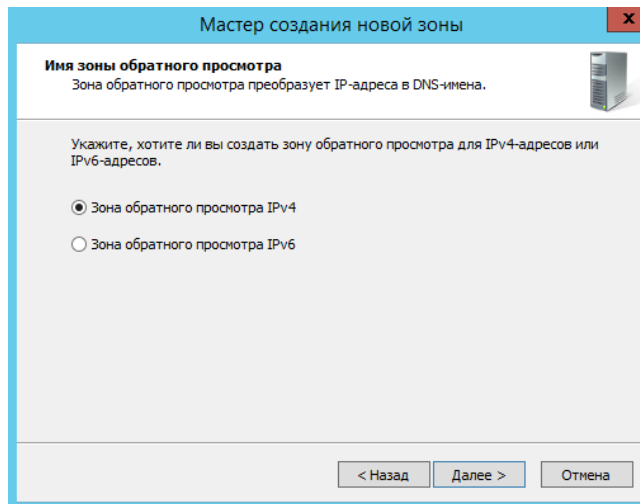


Рисунок 3.46 – Вибір версії IP-адресів

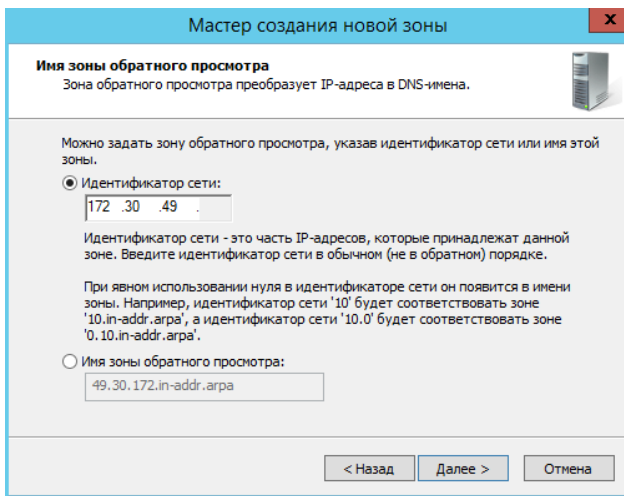


Рисунок 3.47 – Вибір імені зони зворотного перегляду

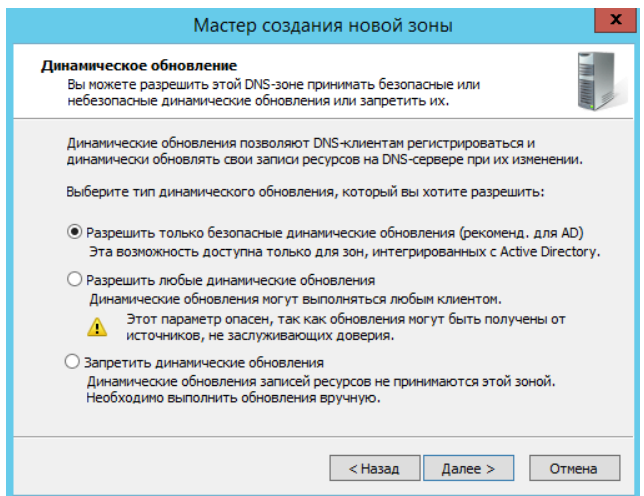


Рисунок 3.48 – Вибір типу динамічного оновлення

Після створення нової зони зворотного перегляду було здійснено автоматичне оновлення записів. На рисунках 3.49-3.51 знайдено в домені server1, де в його властивостях обиралась настройка «Оновити відповідний PTR-запис».

Зм.	Арк.	№ докум.	Підпис	Дата

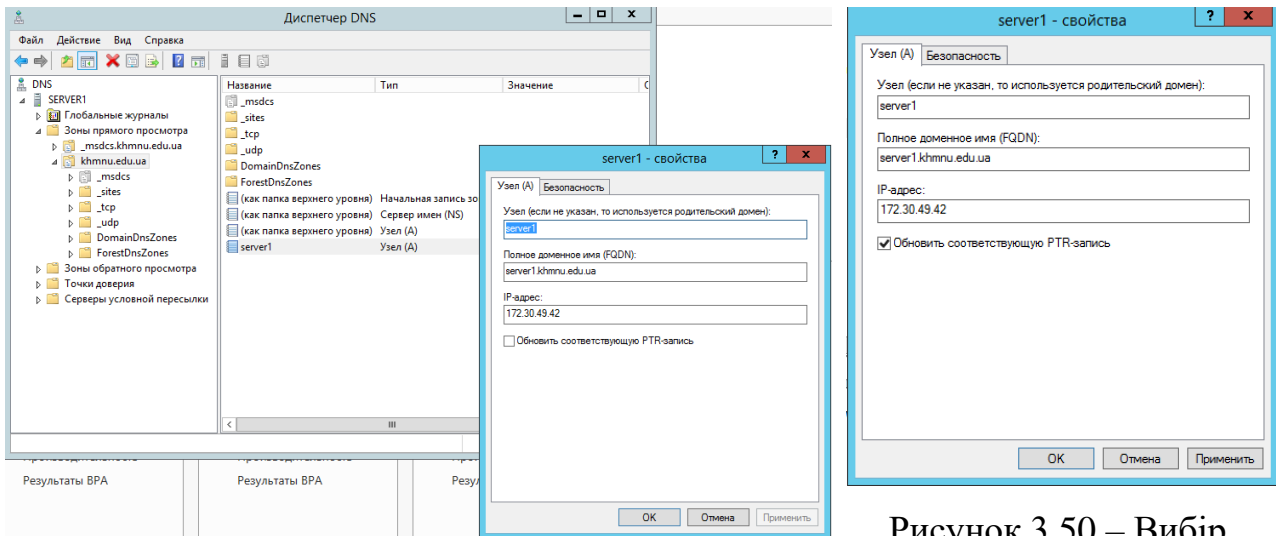


Рисунок 3.49 – Властивості server1

Рисунок 3.50 – Вибір налаштування «Оновити відповідний PTR-запис»

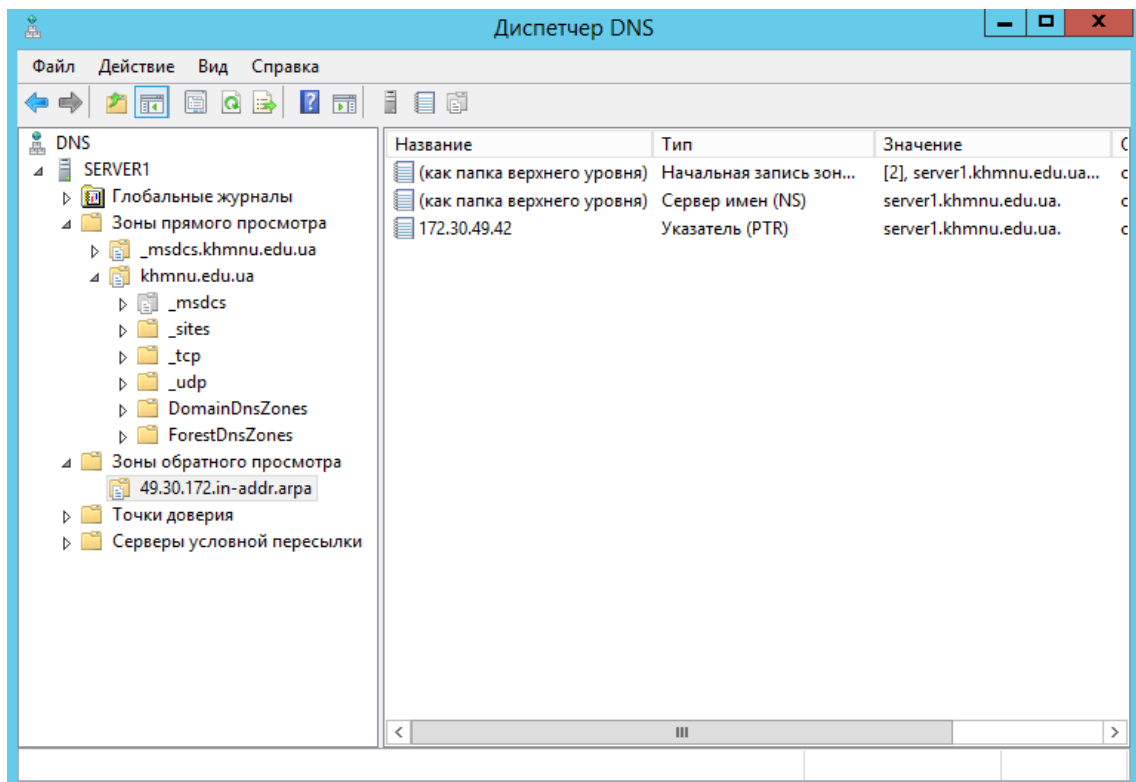


Рисунок 3.51 – Поява зони зворотного перегляду

На першому сервері було завершено налаштування DHCP та DNS. На другому сервері, який виступатиме в ролі запасного, було здійснено його

налаштування (рис. 3.52-3.58). На рисунку 3.53 додано server2 до server1 для управління другим сервером з першого і для встановлення компонентів та ролей на нього таким же чином.

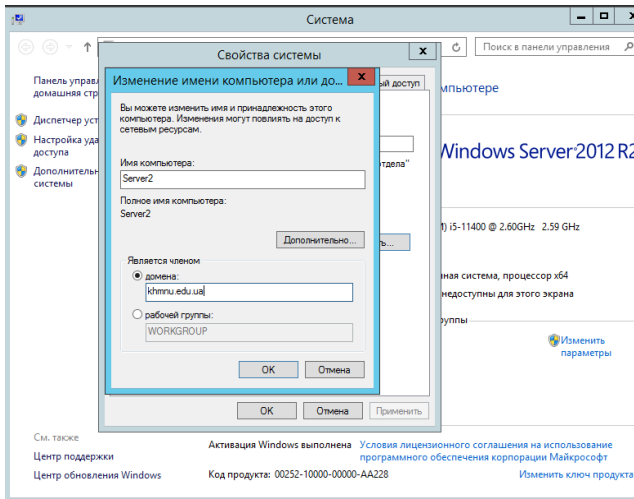


Рисунок 3.52 – Зміна імені другого серверу та включення його в домен

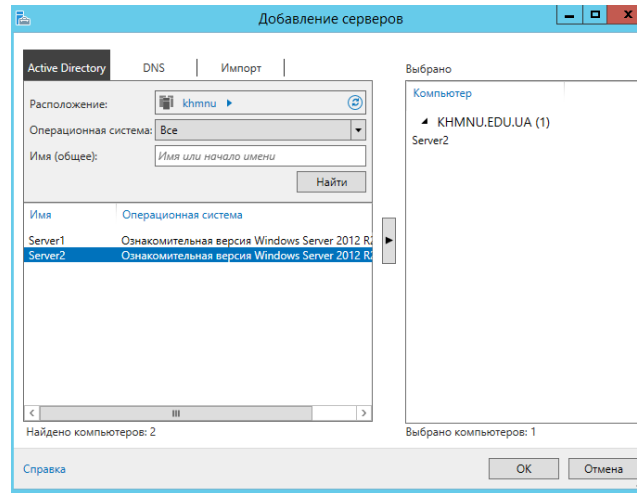


Рисунок 3.53 – Додавання server2 в server1

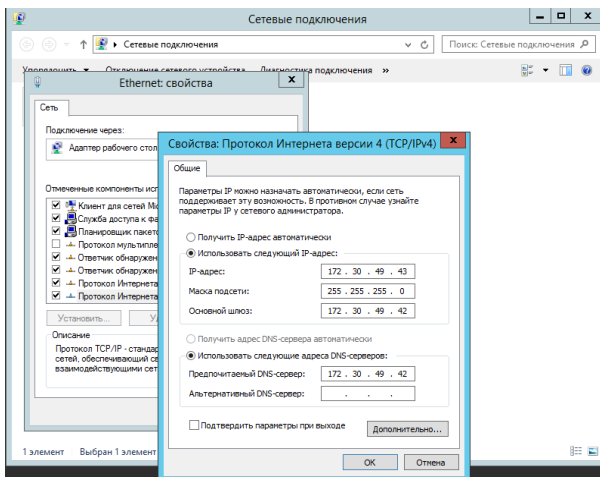


Рисунок 3.54 – Налаштування статичного IP-адресу на server2

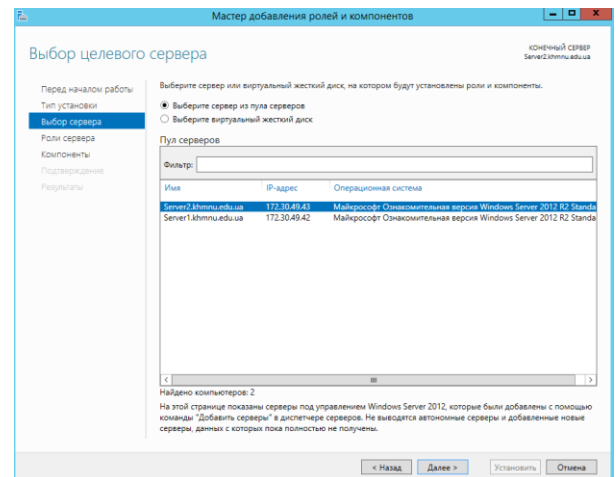


Рисунок 3.55 – Вибір server2 для додавання ролей та компонентів

Після встановлення, було натиснуто на кнопку «Підвищити роль цього сервера рівня контролера домену»(рис. 3.56).

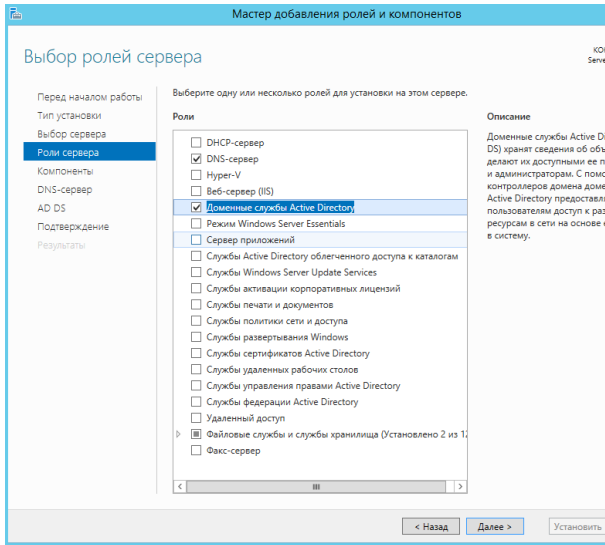


Рисунок 3.56 – Вибір ролей для server2

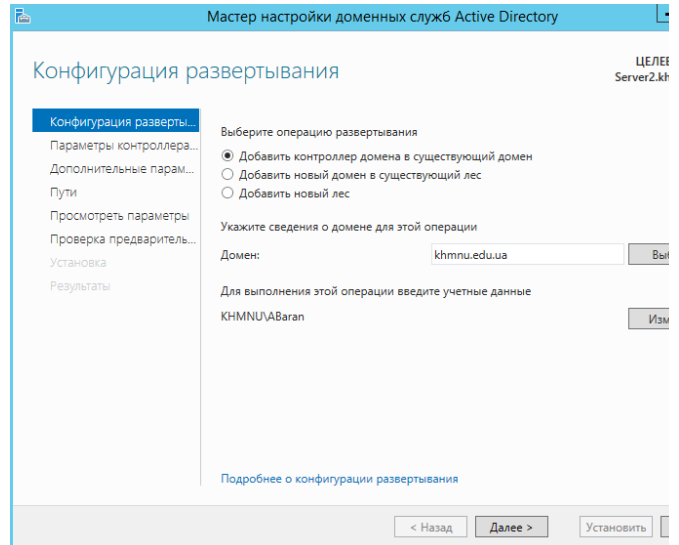


Рисунок 3.57 – Вибір налаштувань розгортання на server2

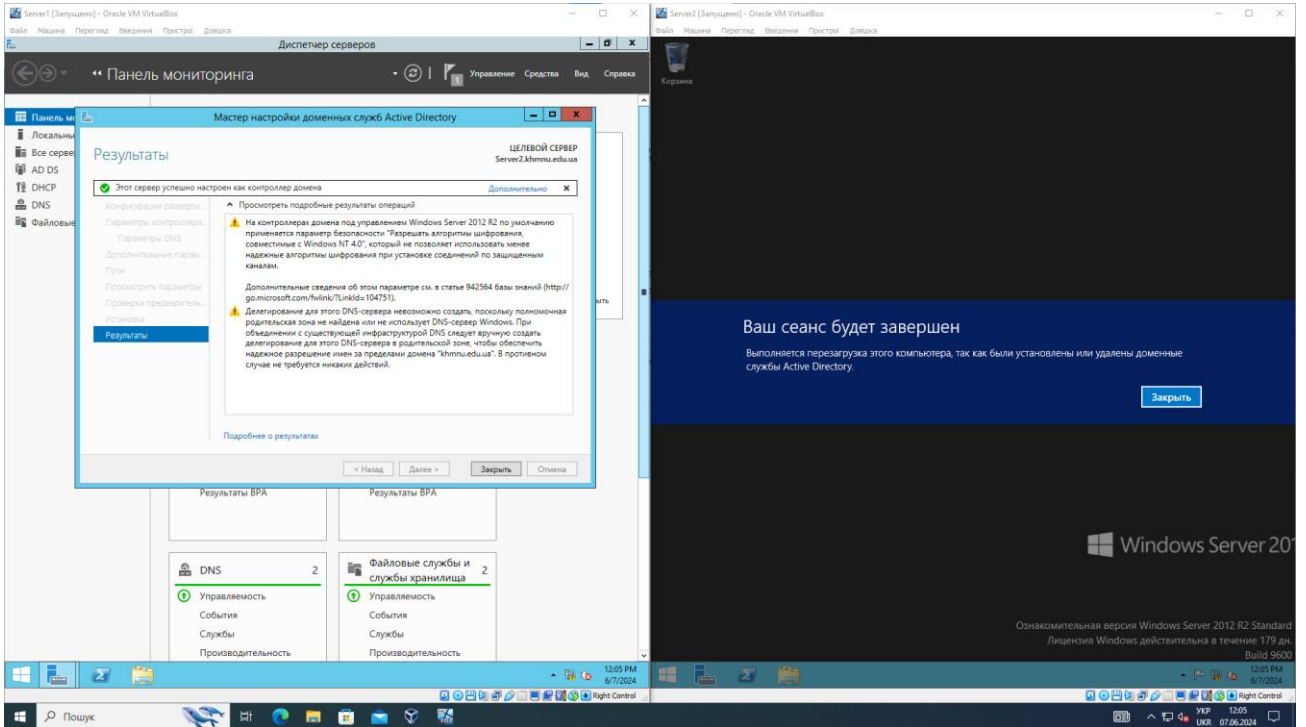


Рисунок 3.58 – Закінчення встановлення та перезапуск server2

					КРБКІ.001115.01.01 ПЗ	Арк. 57
Зм.	Арк.	№ докум.	Підпис	Дата		

Далі було встановлено також DHCP на server2 за таким же алгоритмом дій, як і на server1, через server1. Після всіх інсталювань обидва сервери були перезапущені.

### 3.2.3 Налаштування відмовостійкості на другому сервері

Відмовостійкість або поступова деградація (англ. graceful degradation), або поступове скорочення можливостей, або поступовий вихід із роботи, або плавне зніжжування ефективності це властивість системи (часто комп'ютерної), що дозволяє їй продовжувати правильно діяти у випадку помилки або декількох помилок в деяких її частинах[31].

Для початку було відкрито в меню «Засоби» DHCP, далі було вибрано домен khmnu.edu.ua та на IPv4 було натиснуто ПКМ і в випадяючому меню було обрано «Налаштування обробки відмови». Всі налаштування були зображені на рисунках 3.59-3.60.

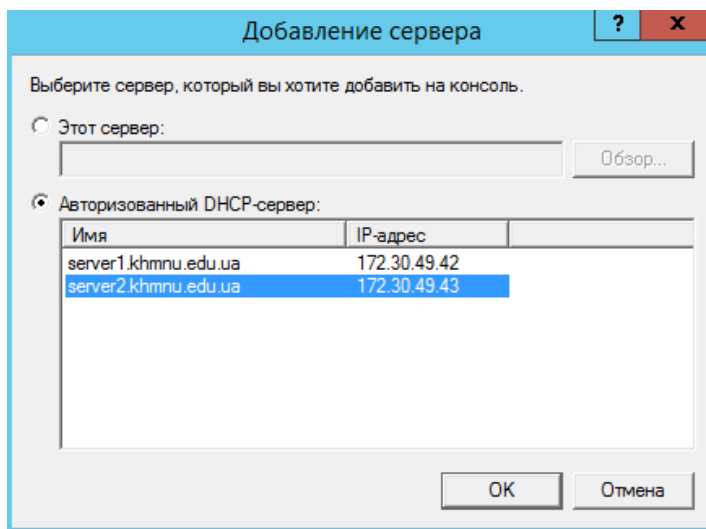


Рисунок 3.59 – Вікно «Додавання сервера»

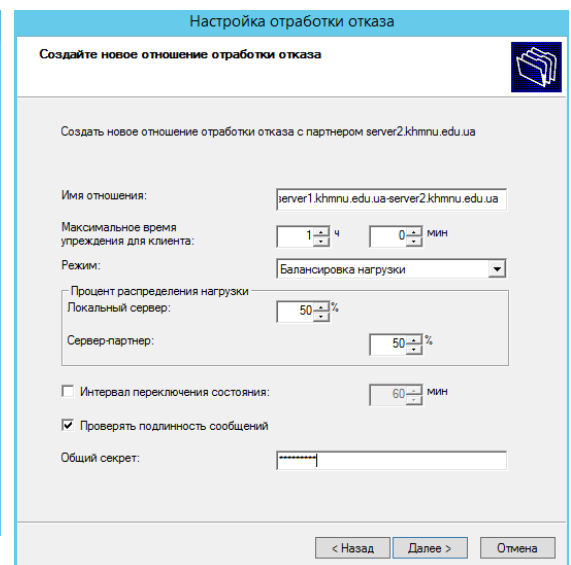


Рисунок 3.60 – Вікно створення нового відношення до server2

Через консоль MMC було перевірено, чи правильно встановились всі компоненти на server2. Для цього було натиснуто ПКМ по Пуск, обрано пункт «Виконати» і введено туди – mmc. Відкрилась консоль MMC, в якій було обрано «Файл» та пункт меню «Додати або видалити оснащення...». Серед оснащень було обрано «DHCP», «DNS» та «Користувачі та комп'ютери Active Directory».

До DHCP було додано також server2, а до DNS створено нове підключення від server2. Для цього було натиснуто ПКМ по DNS та обрано «Підключення до DNS-сервера», вибрано інший комп'ютер та введено server2. Для DHCP також було натиснуто ПКМ і обрано підпункт «Додати сервер...», обравши server2. Як показано на рисунку 3.61, всі галочки DNS та DHCP світяться зеленим, отже все працює коректно.

Для перевірки AD було натиснуто ПКМ по домену та обрано пункт «Змінити контролер домену...» та вибрано server2 і натиснуто «ОК». Після цього, як показано на рисунку 3.61, реплікація пройшла успішно і підрозділи почали з'являтися, отже все працює правильно.

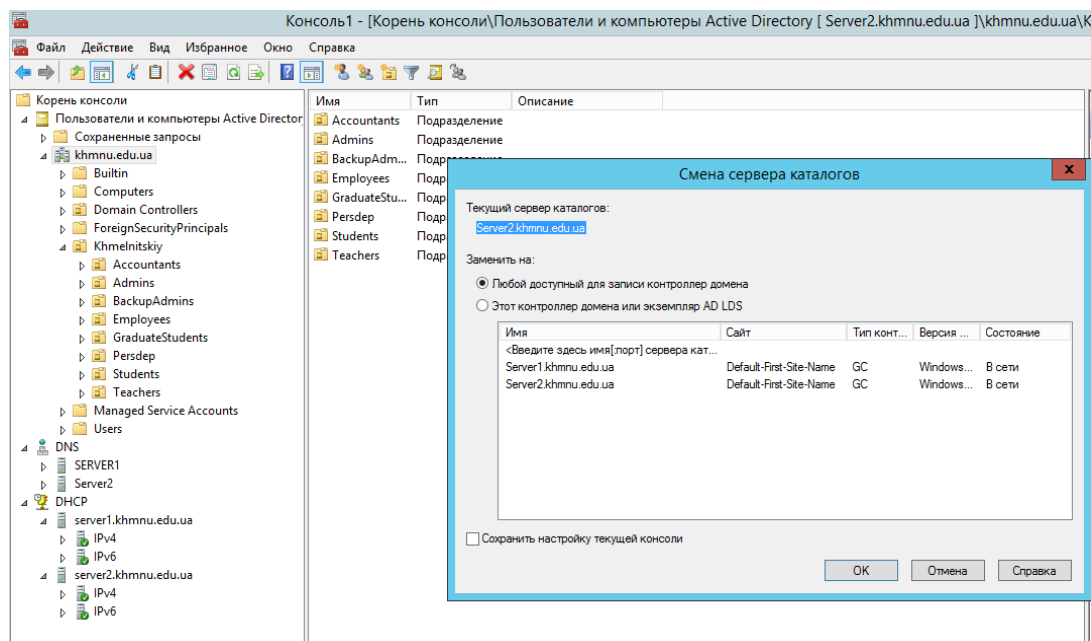


Рисунок 3.61 – Вікно консолі MMC

### 3.3 Створення та керування груповою політикою безпеки для реалізації системи доступу до ресурсів

#### 3.3.1 Зіставлення дисків на сервері. Загальні папки

Групова політика – важливий елемент будь-якого середовища Microsoft Active Directory (AD). Її основна мета – дати IT-адміністраторам можливість централізовано керувати користувачами та комп'ютерами в домені. Групова політика, зі свого боку, складається з набору політик, які називаються об'єктами групової політики (GPO). У Microsoft реалізовано тисячі різних політик і налаштувань, у яких можна потонути і потім не спливати. Усі вони детально описані в довідковій таблиці.

Під час створення домену AD автоматично створюються два об'єкти групової політики:

а) політика домену за замовчуванням встановлює базові параметри для всіх користувачів і комп'ютерів у домені в трьох площинах: політика паролів, політика блокування облікових записів і політика Kerberos.

б) політика контролерів домену за замовчуванням встановлює базові параметри безпеки та аудиту для всіх контролерів домену в межах домену.

Для набуття чинності налаштувань, об'єкт групової політики необхідно застосувати (пов'язати) з одним або декількома контейнерами Active Directory: сайт, домен або підрозділ (OU). Наприклад, можна використовувати групову політику, щоб вимагати від усіх користувачів у певному домені використовувати складніші паролі або заборонити використання знімних носіїв на всіх комп'ютерах тільки у фінансовому підрозділі цього домену.

Об'єкт групової політики не діє, доки не буде пов'язаний із контейнером Active Directory, наприклад, сайтом, доменом або підрозділом. Будь-який об'єкт групової політики може бути пов'язаний з кількома контейнерами, і, навпаки, з конкретним контейнером може бути пов'язано кілька об'єктів групової політики.

					КРБКІ.001115.01.01 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		60

Крім того, контейнери успадковують об'єкти групової політики, наприклад, об'єкт групової політики, пов'язаний із підрозділом, застосовується до всіх користувачів і комп'ютерів у його дочірніх підрозділах. Аналогічним чином, об'єкт групової політики, що застосовується до ОУ, застосовується не тільки до всіх користувачів і комп'ютерів у цьому ОУ, а й успадковується всім користувачам і комп'ютерам у дочірніх ОУ.

Налаштування різних об'єктів групової політики можуть перекриватися або конфліктувати. За замовчуванням об'єкти групової політики обробляються в такому порядку (причому створені пізніше мають пріоритет над створеними раніше):

- а) локальний (індивідуальний комп'ютер);
- б) сайт;
- в) домен;
- г) організаційна одиниця.

У цю послідовність можна і потрібно втручатися, виконавши будь-яку з таких дій:

а) зміна послідовності GPO. Об'єкт групової політики, створений пізніше, обробляється останнім і має найвищий пріоритет, перезаписуючи налаштування в створених раніше об'єктах. Це працює в разі виникнення конфліктів;

б) блокування успадкування. За замовчуванням дочірні об'єкти успадковують усі об'єкти групової політики від батьківського, але ви можете заблокувати це успадкування;

в) примусове ігнорування зв'язку GPO. За замовчуванням параметри батьківських політик перезаписуються будь-якими конфліктуючими політиками дочірніх об'єктів. Ви можете перевизначити цю поведінку;

г) вимкнення зв'язків GPO. За замовчуванням, обробку ввімкнено для всіх зв'язків GPO. Ви можете запобігти застосуванню об'єкта групової політики для

конкретного контейнера, вимкнувши зв'язок з об'єктом групової політики цього контейнера.

Іноді складно зрозуміти, які політики фактично застосовуються до конкретного користувача або комп'ютера, визначити так званий результуючий набір політик (Resultant Set of Policy, RSoP). Microsoft пропонує утиліту командного рядка GPRresult, який вміє генерувати звіт RSoP.

Для управління груповими політиками Microsoft надає консоль управління груповими політиками (GPMC). Використовуючи цей безкоштовний редактор групової політики, IT-адміністратори можуть створювати, копіювати, імпортувати, створювати резервні копії та відновлювати об'єкти групової політики, а також складати звіти щодо них. Microsoft також пропонує цілий набір інтерфейсів GPMC, які можна використовувати для програмного доступу до багатьох операцій, підтримуваних консоллю.

За замовчуванням будь-який член групи адміністраторів домену може створювати об'єкти групової політики та керувати ними. Крім того, існує глобальна група під назвою "Власники-творці групових політик"; її члени можуть створювати об'єкти групової політики, але вони можуть змінювати тільки створені ними політики, якщо їм спеціально не надано дозволів на редагування інших об'єктів групової політики.

У цій же консолі можна делегувати допоміжним IT-адміністраторам дозволи для різних дій: створення, редагування та створення зв'язків для певних об'єктів групової політики. Делегування – цінний інструмент; наприклад, можна надати групі, відповідальній за управління Microsoft Office, можливість редагувати об'єкти групової політики, що використовуються для управління налаштуваннями Office на робочому столі користувачів[14].

Загальний ресурс, або загальний мережевий ресурс(загальна, спільна папка) — в інформатиці, це пристрій або частина інформації, до якої може бути здійснений віддалений доступ з іншого комп'ютера, зазвичай через локальну

					КРБКІ.001115.01.01 ПЗ	Арк. 62
Зм.	Арк.	№ докум.	Підпис	Дата		

комп'ютерну мережу або за допомогою корпоративного інтернету, наче якби ресурс перебував на локальній машині[33].

Для початку було запущено віртуальну машину з клієнтською ОС та перейменовано її на Workstation та додано її до домену(рис.3.62). Після цього перезавантажено систему, та відкрито консоль MMC(рис.3.63).

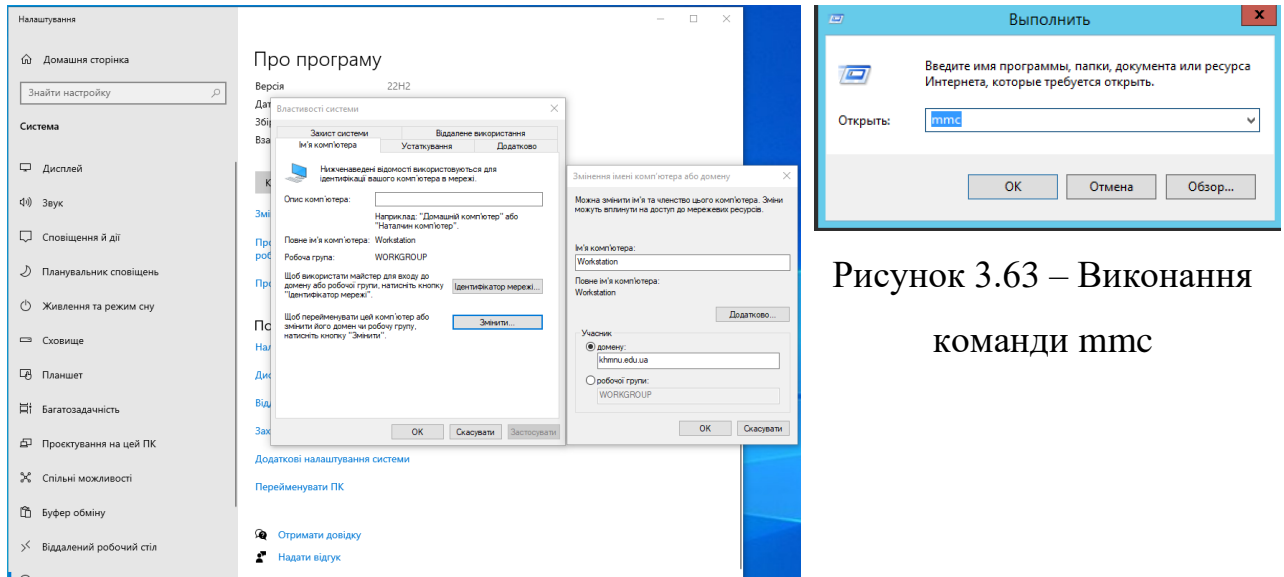


Рисунок 3.63 – Виконання команди mmc

Рисунок 3.62 – Вікно «Властивості системи»

У самій консолі було обрано оснащення "Редактор керування груповими політиками", як показано на рисунку 3.64.

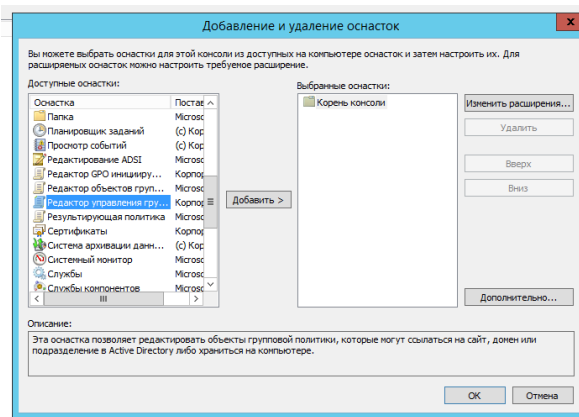


Рисунок 3.64 – Вікно «Властивості системи»

Далі було додано об'єкт групової політики, його налаштування показані на рисунках 3.65-3.68.

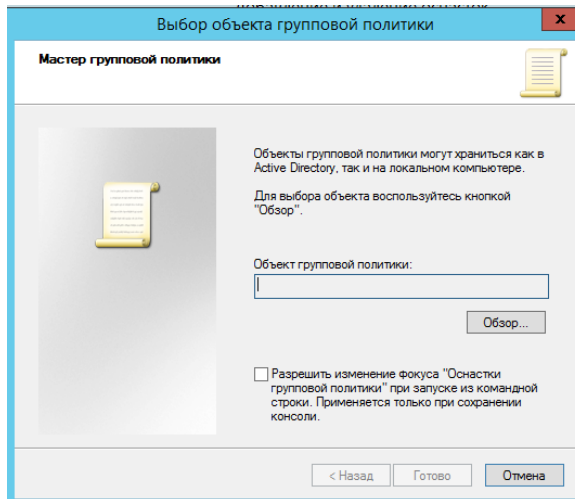


Рисунок 3.65 – Вікно «Майстра групової політики»

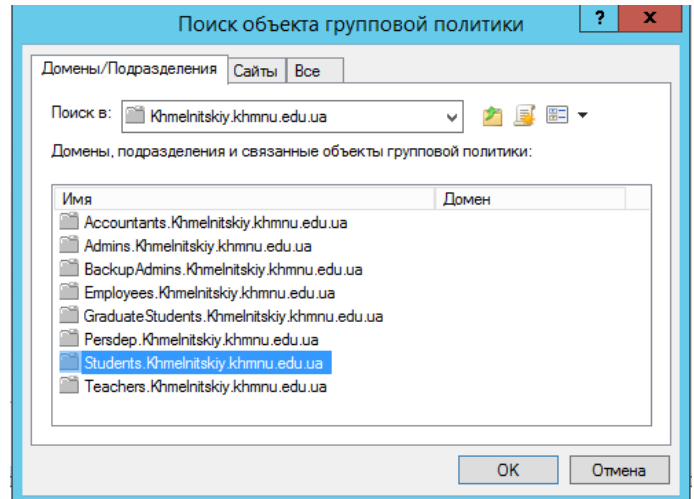


Рисунок 3.66 – Вікно «Пошук об'єкта групової політики»

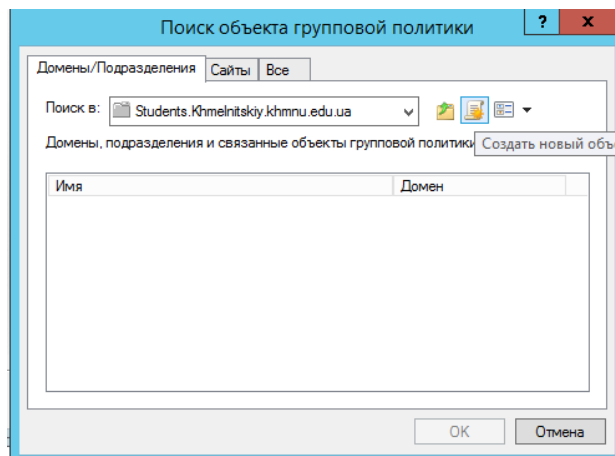


Рисунок 3.67 – Створення нового об'єкту

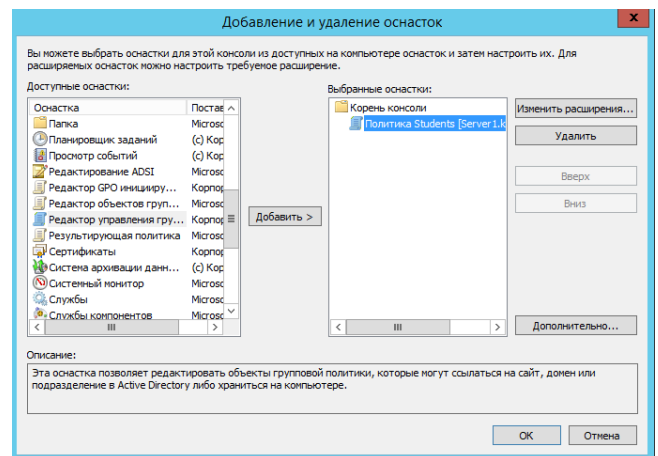


Рисунок 3.68 – Створена нова група політика Students

Після створення групової політики, для зіставлення дисків була створена нова папка, та змінено її налаштування спільного доступу та безпеки на рисунках 3.69-3.76. На рисунку 3.70 було натиснуто кнопку «Розширені налаштування».

Зм.	Арк.	№ докум.	Підпис	Дата

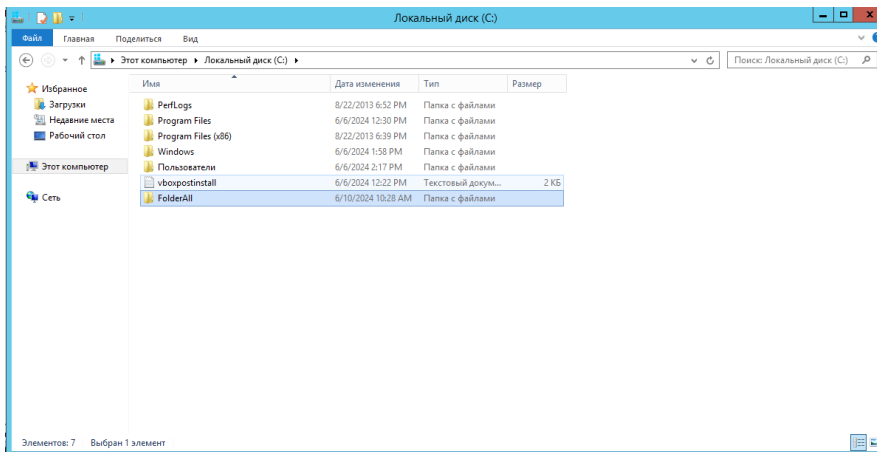


Рисунок 3.69 – Створення нової папки з назвою FolderAll

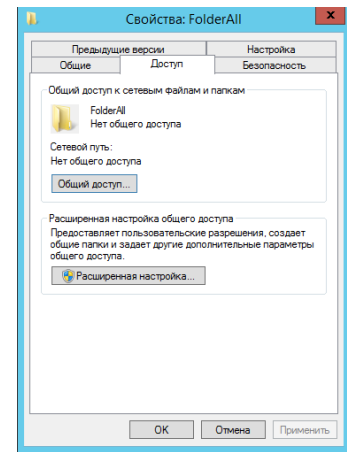


Рисунок 3.70 – Властивості FolderAll

Далі після налаштувань було натиснуто кнопку «Дозволи» на рисунку 3.71 і було обрано всі дозволи на рисунку 3.72.

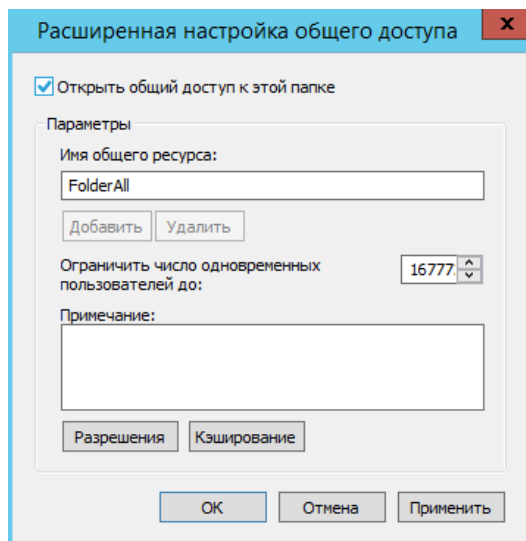


Рисунок 3.71 – Вікно «Розширене налаштування загального доступу»

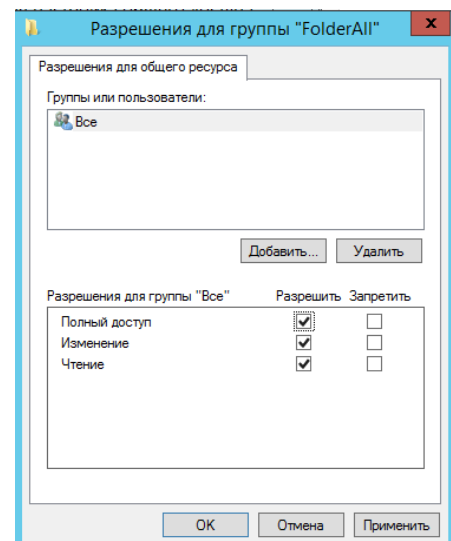


Рисунок 3.72 – Дозволи для групи FolderAll

Всі налаштування було застосовано та збережено. Далі була обрана вкладка «Безпека» і її налаштовано на рисунках 3.73-3.76. На рисунку 3.73 було натиснуто кнопку «Додати», а на рисунку 3.74 – «Додатково...».

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

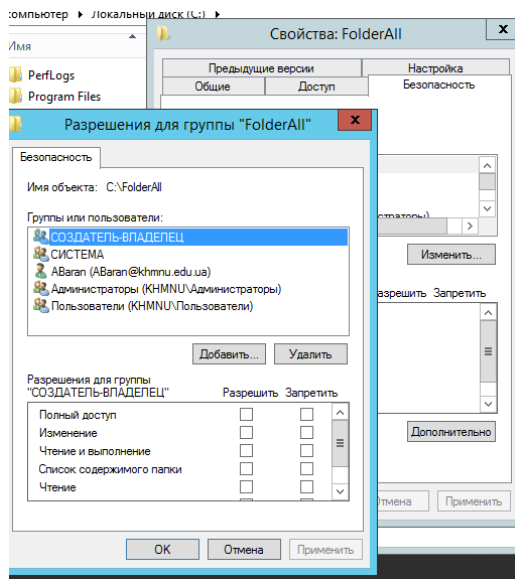


Рисунок 3.73 – Вікно дозволів для групи FolderAll

На рисунку 3.75 було натиснуто кнопку «Пошук» та обрано користувача «Всі», подвійним натисканням по ньому, та збережено налаштування. Потім, на рисунку 3.76 було встановлено прапорці на пункт «Зміни», щоб всі могли вносити зміни до цієї папки.

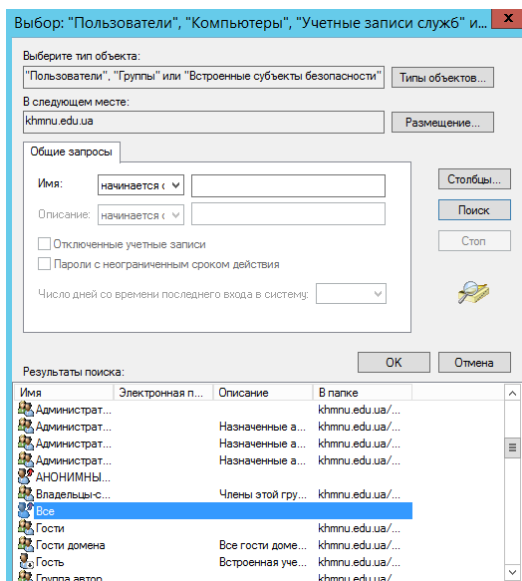


Рисунок 3.75 – Вибір користувача «Всі»

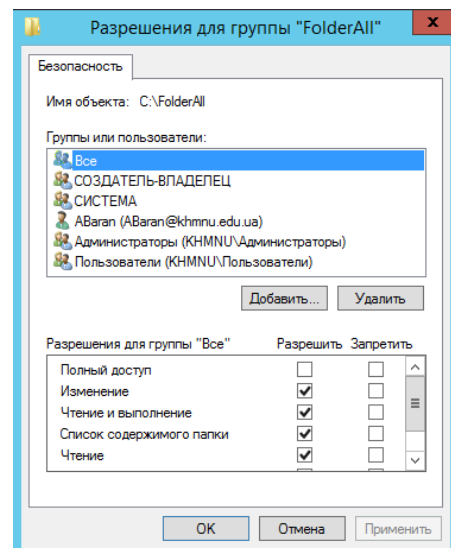


Рисунок 3.76 – Вибір пункту «Зміни»

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

Всі налаштування було збережено та закрито вікна налаштування. Аналогічно була створена папка Personal та були проведені всі ті ж маніпуляції, що і з папкою FolderAll.

Далі було відкрито, через меню «Засоби», меню «Користувачі та комп'ютери Active Directory», для створення в домені, в підрозділі Students, нової спільної папки. На рисунках 3.77-3.78 були показані всі налаштування.

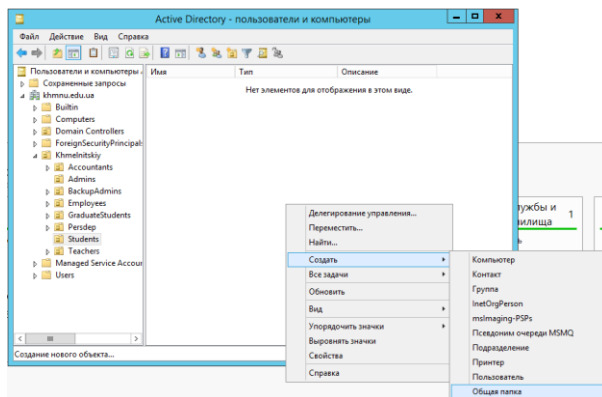


Рисунок 3.77 – Створення нової спільної папки

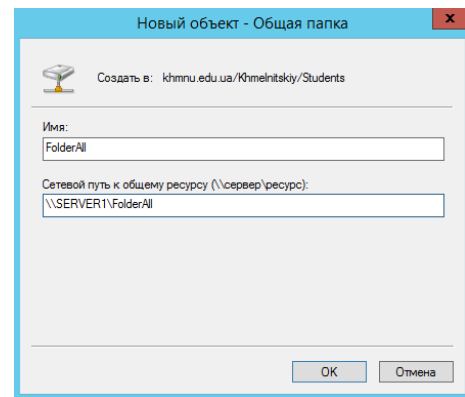


Рисунок 3.78 – Задання імені та шляху спільної папки

Для перевірки було додано три облікових записи студентів – Student1, Student2, Student3 (рис. 3.79-3.80).

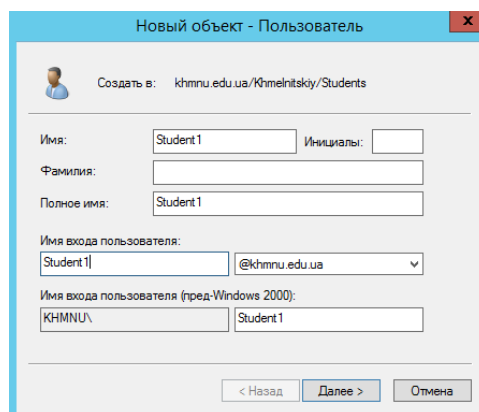


Рисунок 3.79 – Створення нового студента

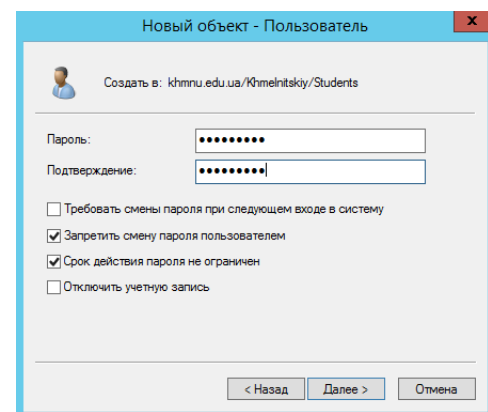


Рисунок 3.80 – Налаштування паролю студента

Повертаємось до зіставлення дисків, для цього було відкрито вікно консолі MMC, вибрано в конфігурації користувача папку «Налаштування», а в ній пункт «Зіставлення дисків». В вікні яке щойно відкрилось натиснуто ПКМ та вибрано «Створити» і «Зіставлений диск» та налаштовано(рис. 3.81-3.82).

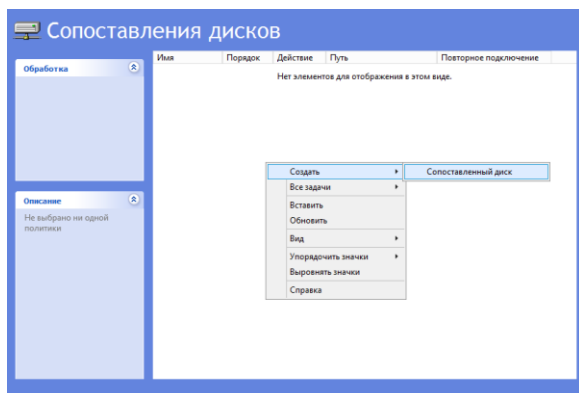


Рисунок 3.81 – Створення нового зіставленого диску

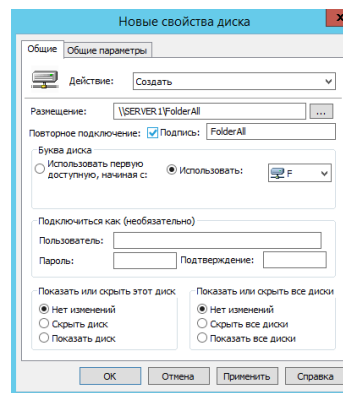


Рисунок 3.82 – Налаштування зіставленого диску

Таким же чином потрібно створити папку для персональних даних, тому було перейдено до пункту «Папки», створено нову та задано відповідні параметри (рис. 3.83-3.84). Оскільки ця папка повинна бути персональною для кожного користувача, в шлях папки було вставлено спеціальне ключове слово %Logonuser%.

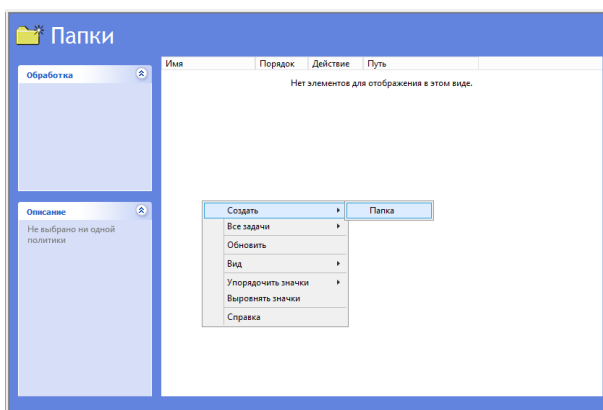


Рисунок 3.83 – Створення нової папки

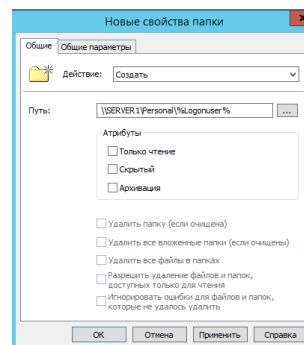


Рисунок 3.84 – Налаштування нової папки

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------



Отже як видно вище, персональні папки працюють коректно. На рисунку 3.88 показано як було, будучи в обліковому записі Student2, створено в папці FolderAll нову папку з назвою – student2 create this folder та переавторизувавшись в інший обліковий запис(Student1), знайдено цю ж папку. Це означає, що все працює правильно.

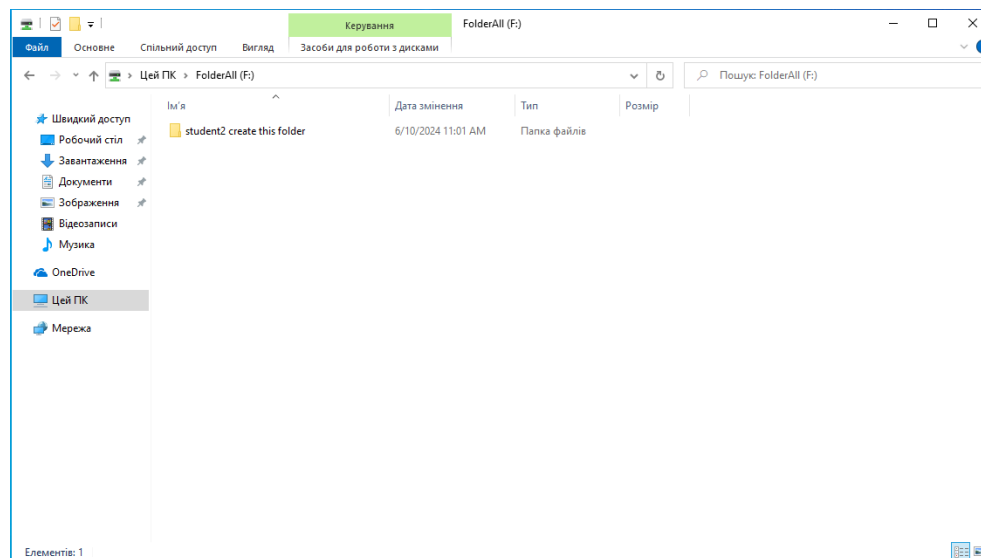


Рисунок 3.88 – Перегляд загальної папки студентів

### 3.3.2 Встановлення квот на папки

Для встановлення квот на деякі папки користувачів, потрібно було встановити «Диспетчер ресурсів файлового серверу». Для цього було відкрито «Майстра додавання ролей та компонентів» і вибрано потрібну роль (рис. 3.89).

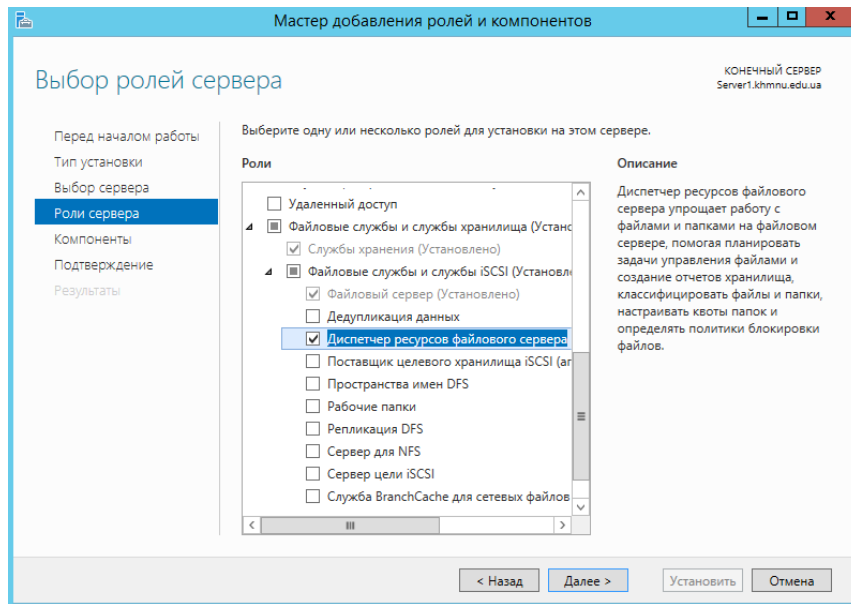


Рисунок 3.89 – Інсталювання «Диспетчер ресурсів файлового серверу»

Після інсталювання було перезапущено систему та відкрито «Диспетчер ресурсів файлового серверу». Далі вибрано «Керування квотами» і «Шаблони квот» та створено новий шаблон квот(рис. 3.90-3.91).

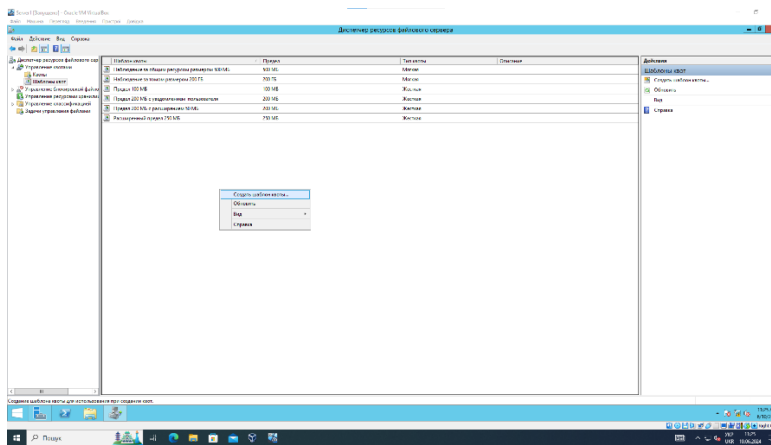


Рисунок 3.90 – Створення нового шаблону  
КВОТ

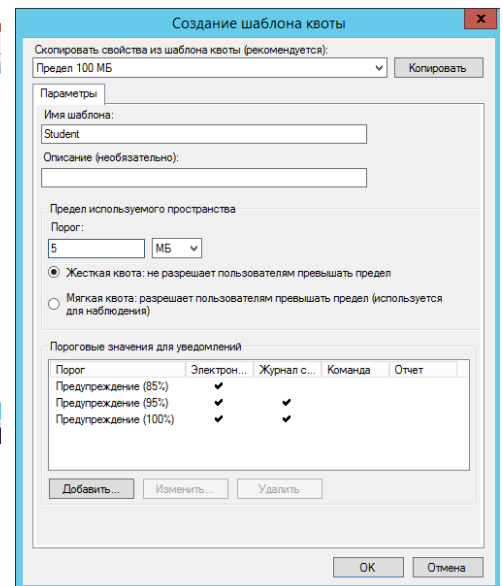


Рисунок 3.91 –  
Налаштування нового  
шаблону квот

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

Після створення шаблону було перейдено до меню «Квоти» та створено нову квоту(рис. 3.92-3.93).

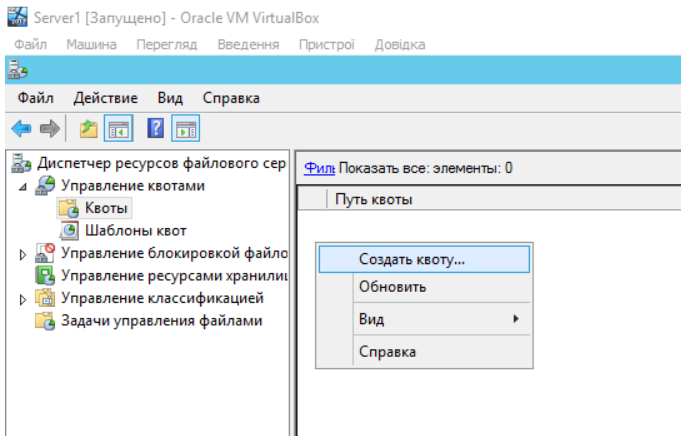


Рисунок 3.92 – Створення нової квоти

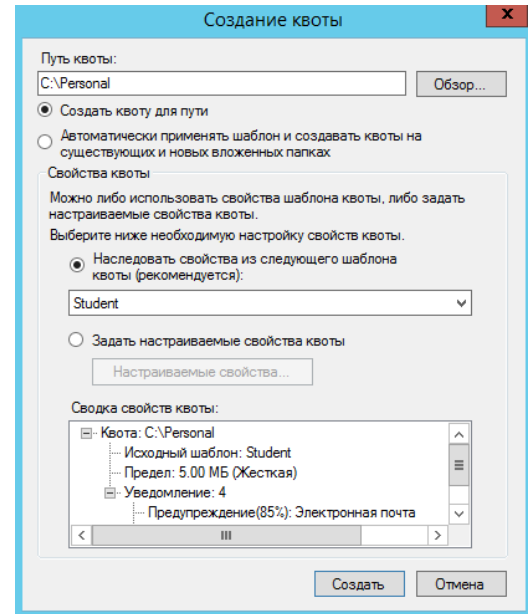


Рисунок 3.93 – Налаштування нової квоти

На наступному малюнку 3.94 зображено, що папка Personal для всіх студентів має фіксований розмір – 5 МБ. Так можна налаштувати багато різних папок для різних користувачів для оптимізації ресурсів серверу.

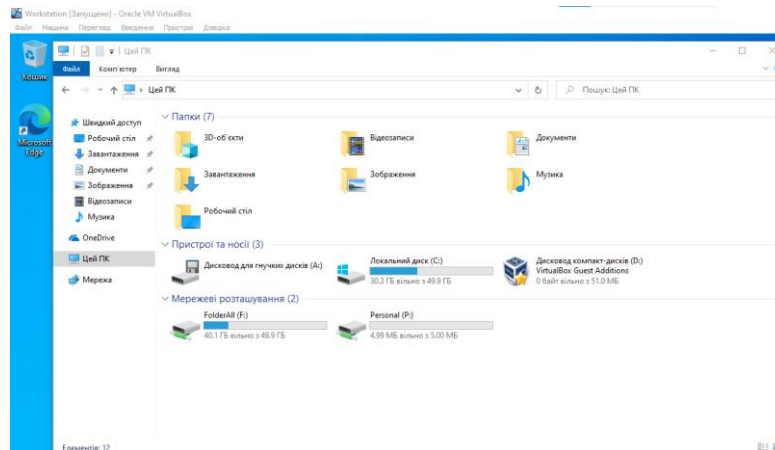


Рисунок 3.94 – Перегляд результатів створення нової квоти

### 3.3.3 Встановлення та налаштування DFS

Distributed File System (DFS) — компонент Microsoft Windows, який використовується для спрощення доступу та керування файлами, фізично розподіленими по мережі. При її використанні файли, розподілені по серверам, видаються в одному місці[32].

Для початку було інстальовано роль «Простори імен» через «Майстра додавання ролей та компонентів»(рис. 3.95).

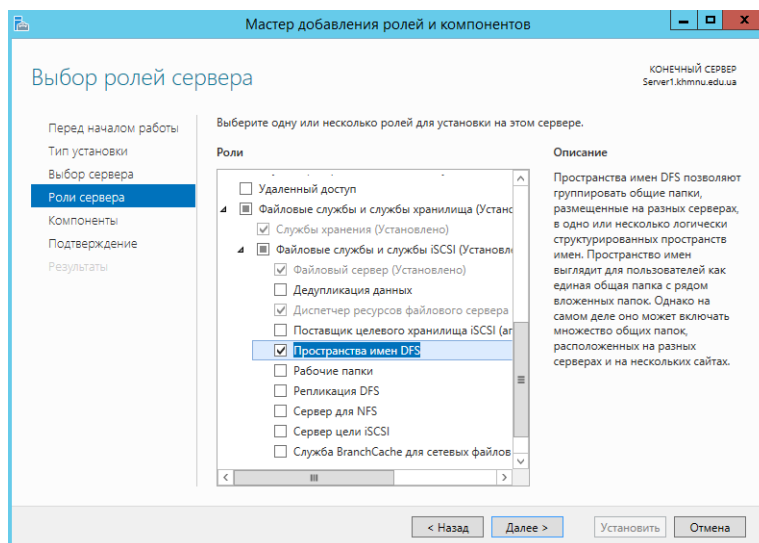


Рисунок 3.95 – Інсталювання «Простори імен DFS»

Потім запущено server2 та на server1 відкрито меню «Засоби», «Управління DFS». Далі вибрано підпункт «Простори імен» та вище натиснено на кнопку «Створити простір імен...». Всі інші налаштування зображено на рисунках 3.96-3.97.

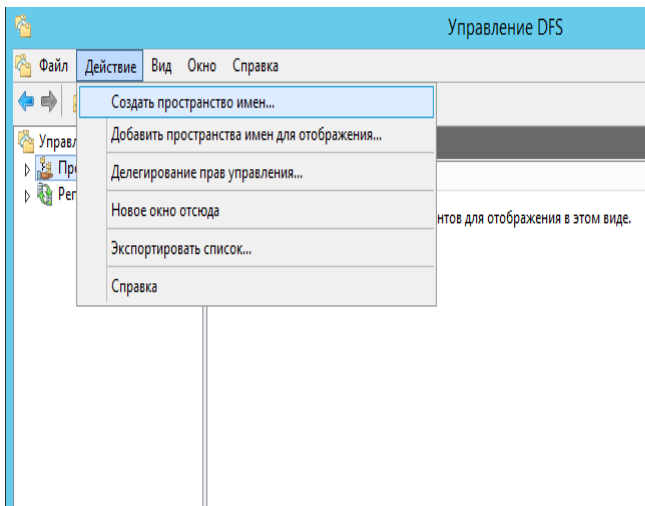


Рисунок 3.96 – Створення нового простору імен

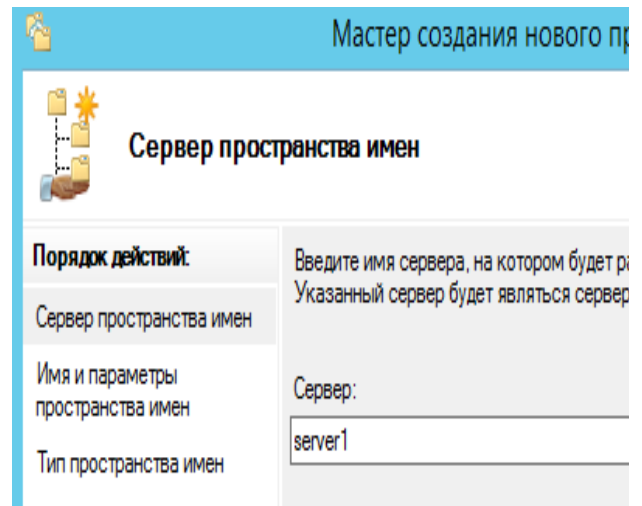


Рисунок 3.97 – Вибір на якому сервері буде створений простір імен

Назву новому простору імен надано таку – HomeDFS. Всі інші налаштування залишаються за замовчуванням. Наступним кроком створено нові папки, які будуть додані в цей простір імен. Створено ще 3 нові папки на server1 та 3 на server2(рис. 3.98-3.99). Цим папкам також потрібно відкрити загальний доступ та змінити налаштування безпеки, так як це було зроблено в попередніх підрозділах.

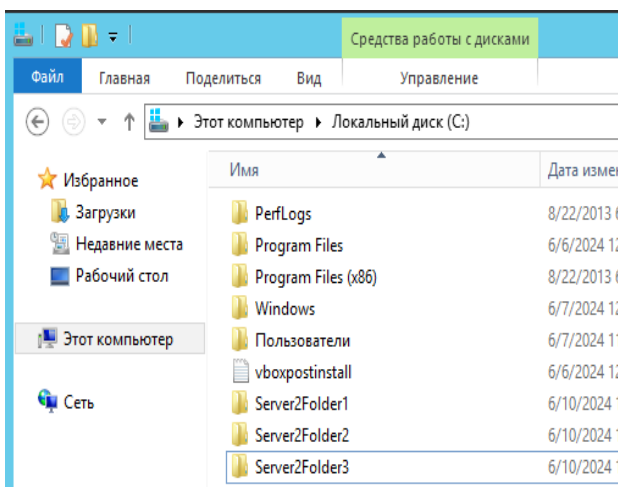


Рисунок 3.98 – Створені нові папки на server2

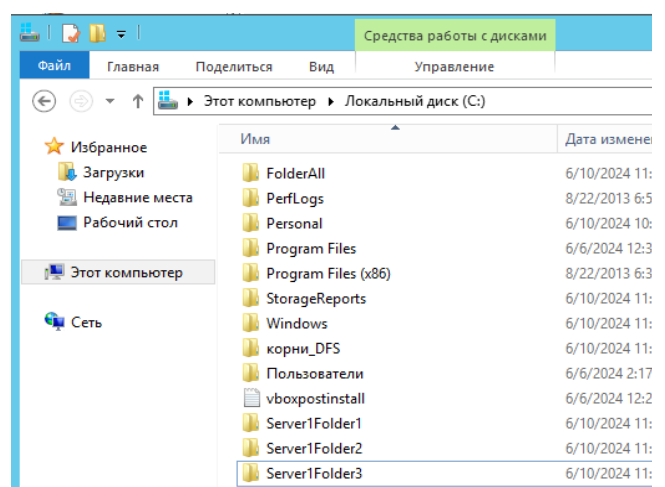


Рисунок 3.99 – Створені нові папки на server1

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

Папки створені, тепер потрібно їх додати до простору імен. Для цього було відкрито вікно «Управління DFS» вибрано створений простір імен. Далі натиснено ПКМ та обрано «Створити папку...»(рис. 3.100). Далі введено ім'я папки та відносний шлях до неї(рис. 3.101) і так додано кожен папку.

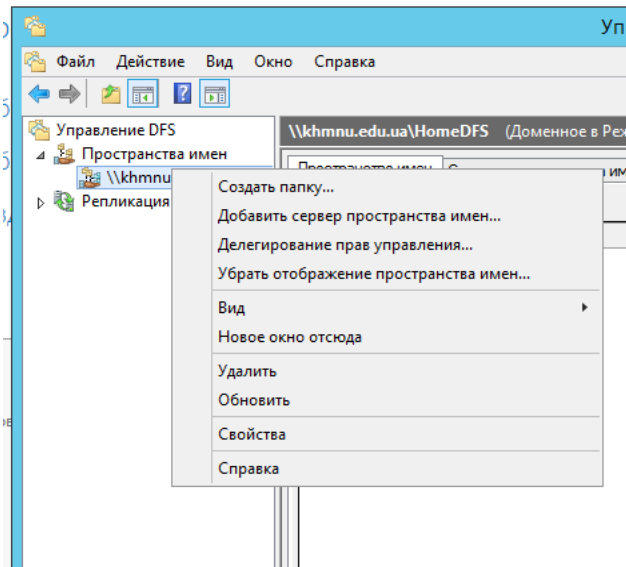


Рисунок 3.100 – Створення нової папки в просторі імен

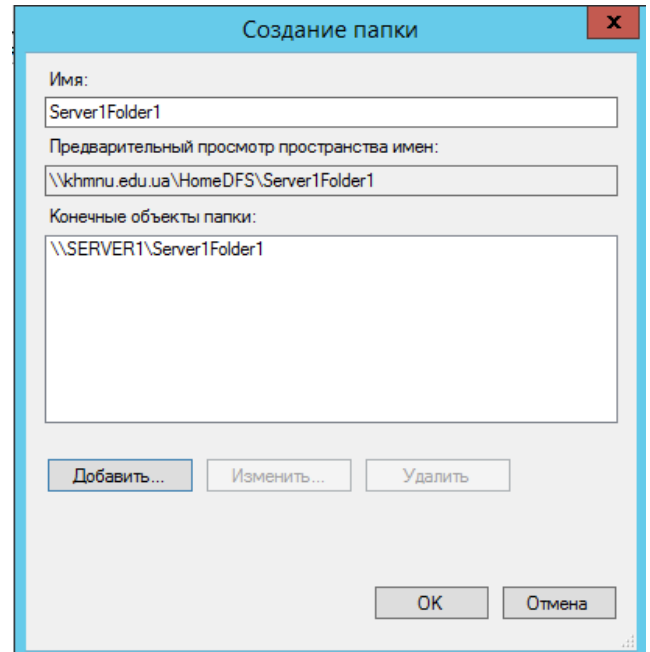


Рисунок 3.101 – Налаштування нової папки в просторі імен

Після цього додано загальну папку. Консоль MMC було відкрито і вибрано оснащення «Редактор керування груповими політиками» та оснащення «Active Directory – користувачі та комп'ютери». На рисунку 3.102 показано вибір об'єкта групової політики – «Default Domain Policy». Це було зроблено для забезпечення доступу кожного користувача до вибраних папок, незалежно від його ролі та прав. Ці папки можуть розміщуватись на різних серверах, проте до них все одно є доступ з різних користувацьких машин, що належать до домену khmelnitskiy.edu.ua.

Далі було створено загальну папку в головному підрозділі «Khmelnitskiy», і задано її ім'я та відносний шлях (рис. 3.103).

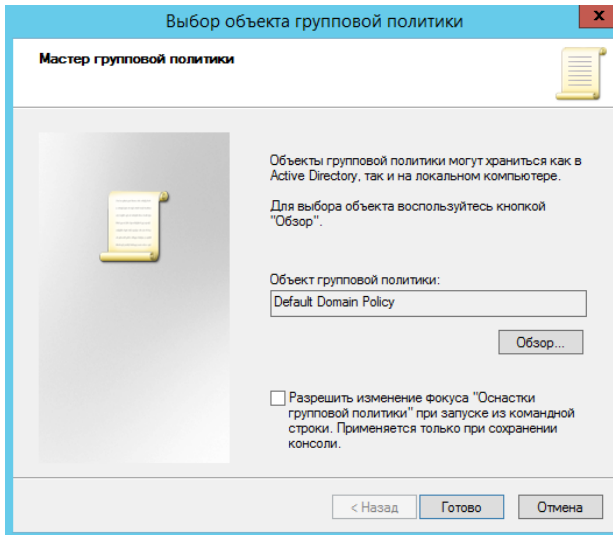


Рисунок 3.102 – Створення нової папки в просторі імен

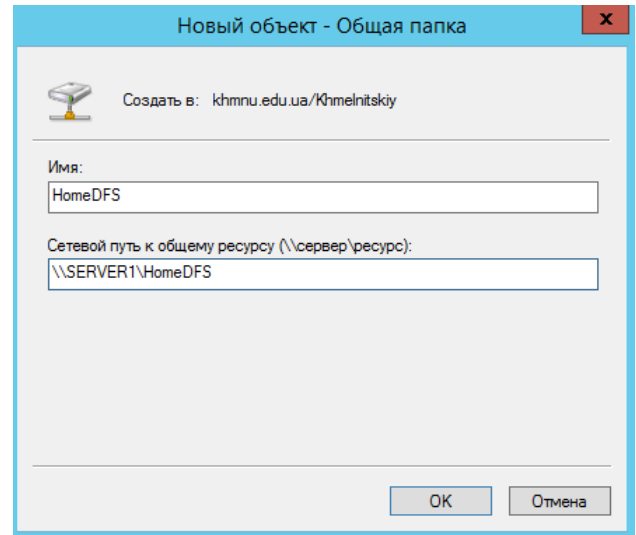


Рисунок 3.103 – Налаштування загальної папки

Потім було створено та налаштовано зіставлений диск на основі папки HomeDFS(рис. 3.104-3.105).

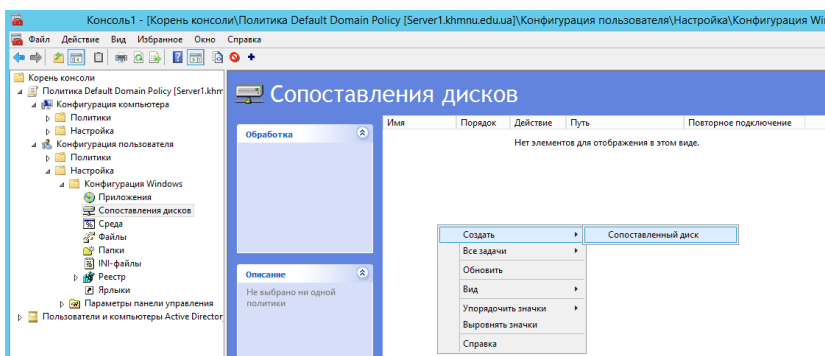


Рисунок 3.104 – Створення зіставленого диску на основі папки HomeDFS

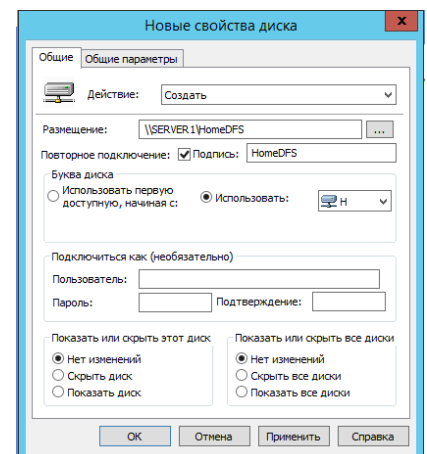


Рисунок 3.105 – Налаштування нового зіставленого диску

Зм.	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

Для того, щоб побачити зміни, було здійснено переавторизацію на server2 та відкрито «Цей комп'ютер». Там було відображено загальну папку HomeDFS і з'явився доступ до всіх її папок (рис. 3.106-3.108). Отже все працює коректно.

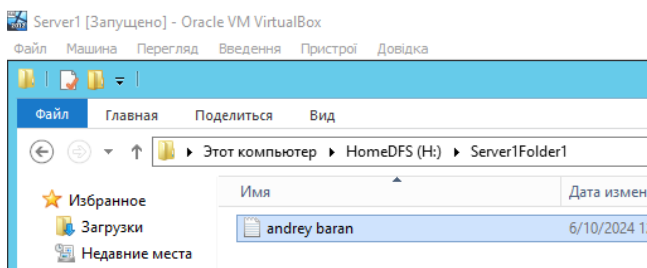


Рисунок 3.106 – Створення тестового файлу на server1

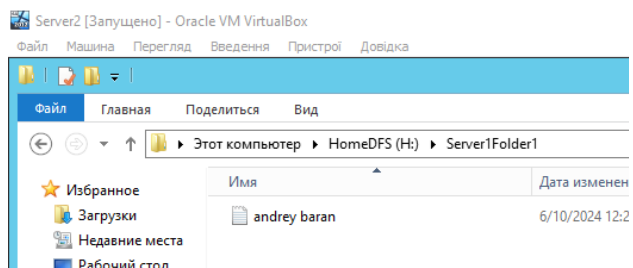


Рисунок 3.107 – Відображення тестового файлу на server2

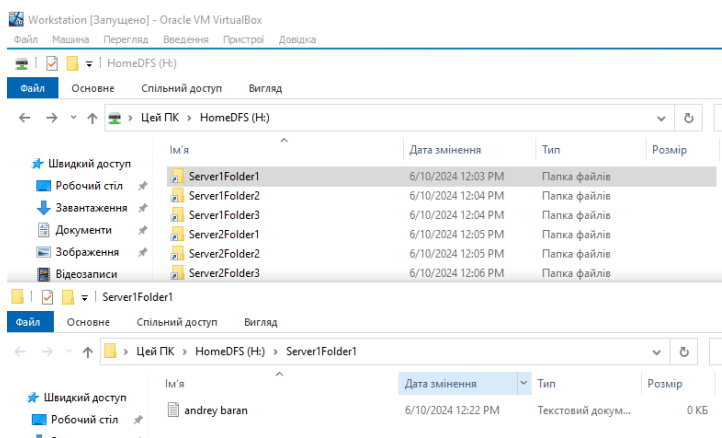


Рисунок 3.108 – Відображення тестового файлу на Workstation

### 3.4 Висновки

На основі проведених досліджень та виконаних налаштувань можна зробити наступні висновки:

а) встановлення та налаштування серверної операційної системи Windows Server 2019 було успішно виконане за допомогою віртуалізаційного програмного

забезпечення Oracle VM VirtualBox. Вибір відповідних параметрів віртуальної машини дозволив забезпечити оптимальну роботу серверної ОС навіть при одночасному використанні декількох віртуальних машин;

б) налаштування Active Directory Domain Services (ADDS) дозволило створити та налаштувати доменну структуру, що включає нові облікові записи адміністратора та організаційні підрозділи. Це забезпечує централізоване управління користувачами та ресурсами мережі, що є критично важливим для ефективного функціонування IT-інфраструктури університету;

в) встановлення та налаштування DHCP та DNS-серверів забезпечило автоматичний розподіл IP-адрес серед клієнтів мережі та правильну маршрутизацію запитів до доменів. Це значно полегшує управління мережею та підвищує її стабільність і надійність;

г) налаштування Distributed File System (DFS) дозволило створити єдину файловою систему, доступну з будь-якого місця мережі. Це сприяє покращенню доступу до навчальних матеріалів та інших ресурсів для студентів і співробітників університету.

Загалом, реалізація описаних налаштувань створює міцну основу для ефективного управління та забезпечення доступу до інформаційних ресурсів університету, що сприяє підвищенню продуктивності та якості освітнього процесу.

					КРБКІ.001115.01.01 ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		78

## ВИСНОВКИ

На основі проведених досліджень та виконаних налаштувань у межах даної кваліфікаційної роботи можна зробити наступні висновки:

- а) створена система доступу до інформаційних ресурсів університету;
- б) успішно встановлено та налаштовано серверну операційну систему Windows Server 2019;
- в) реалізовано централізоване управління користувачами за допомогою Active Directory та ресурсами мережі;
- г) була проведена оптимізація управління мережею через DHCP та DNS-сервери;
- д) здійснено поліпшення доступу до навчальних матеріалів через Distributed File System (DFS).

Було створено систему доступу до ресурсів університету, яка надає весь функціонал потрібний для централізованого керування користувачами та інформаційними ресурсами, а також має надійний захист від непередбачуваних втрат даних.

Використання віртуалізаційного програмного забезпечення Oracle VM VirtualBox дозволило ефективно налаштувати серверну ОС, забезпечуючи стабільну роботу навіть при одночасному використанні декількох віртуальних машин. Це підвищило гнучкість і адаптивність ІТ-інфраструктури університету.

Налаштування Active Directory Domain Services (ADDS) дозволило створити доменну структуру з новими обліковими записами адміністратора та організаційними підрозділами. Це значно спростило управління користувачами та ресурсами мережі, забезпечуючи високу ефективність функціонування ІТ-інфраструктури університету.

Встановлення та налаштування DHCP і DNS-серверів забезпечило автоматичний розподіл IP-адрес серед клієнтів мережі та правильну

					КРБКІ.001115.01.01 ПЗ	Арк.
						79
Зм.	Арк.	№ докум.	Підпис	Дата		

маршрутизацію запитів до доменів. Це сприяло підвищенню стабільності і надійності мережі, що є критично важливим для безперебійної роботи навчального процесу.

Налаштування DFS дозволило створити єдину файлову систему, доступну з будь-якої точки мережі. Це значно полегшило доступ до навчальних матеріалів та інших ресурсів для студентів і співробітників університету, підвищуючи загальну ефективність освітнього процесу.

Загалом, реалізація зазначених налаштувань створила міцну основу для ефективного управління та забезпечення доступу до інформаційних ресурсів університету. Виконані роботи сприяли поліпшенню якості та доступності освітніх послуг, що в свою чергу підвищує конкурентоспроможність університету в умовах сучасного інформаційного суспільства.

Ці висновки відображають досягнення основних цілей дослідження і демонструють важливість інтеграції сучасних інформаційних технологій в освітній процес для забезпечення його ефективності та безперервного розвитку.

					КРБКІ.001115.01.01 ПЗ	Арк.
						80
Зм.	Арк.	№ докум.	Підпис	Дата		

## ПЕРЕЛІК ЛІТЕРАТУРНИХ ПОСИЛАНЬ

1. Інформаційний вибух [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9\\_%D0%B2%D0%B8%D0%B1%D1%83%D1%85#cite\\_note-9](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9_%D0%B2%D0%B8%D0%B1%D1%83%D1%85#cite_note-9) (дата звернення 08.05.2024).

2. Дистанційне навчання: сучасний формат освіти, який має лишитися [Електронний ресурс]. – Режим доступу: <https://life.pravda.com.ua/society/2020/07/2/241517/> (дата звернення 08.05.2024).

3. ТЕМА 1. ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, 1.1 Характеристика інформаційної безпеки с.6 [Електронний ресурс]. – Режим доступу: <https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3%D0%91%20.pdf> (дата звернення 08.05.2024).

4. ІНФОРМАЦІЙНІ РЕСУРСИ ОСВІТИ – 2. ІНФОРМАТИЗАЦІЯ УПРАВЛІННЯ [Електронний ресурс]. – Режим доступу: <http://education-ua.org/ua/analytics/428-informatsijni-resursi-osviti-2-informatizatsiya-upravlinnya> (дата звернення 08.05.2024).

5. Яку ОС вибрати для сервера? [Електронний ресурс]. – Режим доступу: <https://deltahost.ua/ua/yaku-os-vibrati-dlya-servera.html> (дата звернення 09.05.2024).

6. Що таке логічна топологія? [Електронний ресурс]. – Режим доступу: <https://portalcripto.com.br/uk/%D1%81%D0%BB%D0%BE%D0%B2%D0%BD%D0%B8%D0%BA/%D0%A9%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BB%D0%BE%D0%B3%D1%96%D1%87%D0%BD%D0%B0-%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F/> (дата звернення 22.05.2024).

					КРБКІ.001115.01.01 ПЗ	Арк. 81
Зм.	Арк.	№ докум.	Підпис	Дата		

7. Модульне середовище для навчання [Електронний ресурс]. – Режим доступу: <https://msn.khmnu.edu.ua/mod/page/view.php?id=10201> (дата звернення 22.05.2024).

8. Overview [Електронний ресурс]. – Режим доступу: <https://ldapwiki.com/wiki/Wiki.jsp?page=LDAP#section-LDAP-Overview> (дата звернення 22.05.2024).

9. What is LDAP [Електронний ресурс]. – Режим доступу: <https://ldapwiki.com/wiki/Wiki.jsp?page=LDAP%20Overview> (дата звернення 22.05.2024).

10. Що таке бекап і навіщо потрібно робити резервне копіювання? [Електронний ресурс]. – Режим доступу: <https://brainlab.com.ua/uk/blog-uk/shho-take-rezervna-i-navishho-potribno-robiti-rezervne-kopiyuvannya> (дата звернення 22.05.2024).

11. Какие существуют типы виртуализации? [Електронний ресурс]. – Режим доступу: <https://aws.amazon.com/ru/what-is/virtualization/#:~:text=%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F%20%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%BE%D0%B2&text=%D0%AD%D1%82%D0%BE%20%D1%8D%D1%84%D1%84%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D0%B9%20%D0%B8%20%D1%8D%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D1%87%D0%BD%D1%8B%D0%B9%20%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1,%D0%B2%20%D1%80%D0%B5%D0%B7%D1%83%D0%BB%D1%8C%D1%82%D0%B0%D1%82%D0%B5%20%D1%87%D0%B5%D0%B3%D0%BE%20%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0%20%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%B0%D0%B8%D0%B2%D0%B0%D1%8E%D1%82>. (дата звернення 22.05.2024).

12. DHCP-сервер [Электронный ресурс]. – Режим доступа: <https://itelon.ru/blog/dhcp-server/> (дата звернення 22.05.2024).

13. What is a DNS server? [Электронный ресурс]. – Режим доступа: <https://www.cloudflare.com/learning/dns/what-is-a-dns-server/> (дата звернення 22.05.2024).

14. Групповые политики (GPO) Active Directory: разбираемся почему это важно и как ими управлять в GPOAdmin [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/companies/galssoftware/articles/543588/> (дата звернення 22.05.2024).

15. Системний адміністратор [Электронный ресурс]. – Режим доступа: [https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D0%B8%D0%B9\\_%D0%B0%D0%B4%D0%BC%D1%96%D0%BD%D1%96%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B0%D0%B4%D0%BC%D1%96%D0%BD%D1%96%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80) (дата звернення 23.05.2024).

16. Доменные службы Active Directory [Администрирования Windows Server] [Электронный ресурс]. – Режим доступа: <https://www.youtube.com/watch?v=xNwvcsT6YcA&list=PLy5XrqLTpeSsA2STtGeLMVbwJBPCevr3D&index=4> (дата звернення 05.06.2024).

17. Приймальна комісія Хмельницький Національний Університет [Электронный ресурс]. – Режим доступа: [https://pk.khmnu.edu.ua/?\\_gl=1%2A1loi5db%2A\\_ga%2AODc3NjU5NzEuMTcxNTY3MDI5NQ..%2A\\_ga\\_LYXCXPXQWQ%2AMTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA](https://pk.khmnu.edu.ua/?_gl=1%2A1loi5db%2A_ga%2AODc3NjU5NzEuMTcxNTY3MDI5NQ..%2A_ga_LYXCXPXQWQ%2AMTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA) (дата звернення 15.06.2024).

18. Наука Хмельницький Національний Університет [Электронный ресурс]. – Режим доступа: [https://nauka.khmnu.edu.ua/?\\_gl=1%2A1loi5db%2A\\_ga%2AODc3NjU5NzEuMTcxNTY3MDI5NQ..%2A\\_ga\\_LYXCXPXQWQ%2AMTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA](https://nauka.khmnu.edu.ua/?_gl=1%2A1loi5db%2A_ga%2AODc3NjU5NzEuMTcxNTY3MDI5NQ..%2A_ga_LYXCXPXQWQ%2AMTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA) (дата звернення 15.06.2024).

					КРБКІ.001115.01.01 ПЗ	Арк. 83
Зм.	Арк.	№ докум.	Підпис	Дата		

19. Інформаційна система «Електронний університет» [Електронний ресурс]. – Режим доступу: [https://isu1.khmnu.edu.ua/isu/?\\_gl=1\\*1loi5db\\*\\_ga\\*ODc3NjU5NzEuMTcxNTY3MDI5NQ..\\*\\_ga\\_LYXCXPXQWQ\\*MTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA](https://isu1.khmnu.edu.ua/isu/?_gl=1*1loi5db*_ga*ODc3NjU5NzEuMTcxNTY3MDI5NQ..*_ga_LYXCXPXQWQ*MTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA) (дата звернення 15.06.2024).

20. Підготовче відділення Хмельницький Національний Університет [Електронний ресурс]. – Режим доступу: [https://pidgotovka.khmnu.edu.ua/?\\_ga=2.3624312.955426337.1672832565-147095575.1669619147&\\_gl=1%2Arnlnep%2A\\_ga%2AODc3NjU5NzEuMTcxNTY3MDI5NQ..%2A\\_ga\\_LYXCXPXQWQ%2AMTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA](https://pidgotovka.khmnu.edu.ua/?_ga=2.3624312.955426337.1672832565-147095575.1669619147&_gl=1%2Arnlnep%2A_ga%2AODc3NjU5NzEuMTcxNTY3MDI5NQ..%2A_ga_LYXCXPXQWQ%2AMTcxODQ0NzQ2My43LjEuMTcxODQ0NzQ4NC4wLjAuMA) (дата звернення 15.06.2024).

21. Центр післядипломної освіти Хмельницький Національний Університет [Електронний ресурс]. – Режим доступу: [https://spo.khmnu.edu.ua/pidvyshhennya-kvalifikacziyi-pedahohichnykh-pratsivnykiv/?\\_ga=2.3624312.955426337.1672832565-147095575.1669619147&\\_gl=1\\*1k08d1e\\*\\_ga\\*ODc3NjU5NzEuMTcxNTY3MDI5NQ..\\*\\_ga\\_LYXCXPXQWQ\\*MTcxODQ0NzQ2My43LjEuMTcxODQ0NzU1NS4wLjAuMA](https://spo.khmnu.edu.ua/pidvyshhennya-kvalifikacziyi-pedahohichnykh-pratsivnykiv/?_ga=2.3624312.955426337.1672832565-147095575.1669619147&_gl=1*1k08d1e*_ga*ODc3NjU5NzEuMTcxNTY3MDI5NQ..*_ga_LYXCXPXQWQ*MTcxODQ0NzQ2My43LjEuMTcxODQ0NzU1NS4wLjAuMA) (дата звернення 15.06.2024).

22. Модульне середовище для навчання [Електронний ресурс]. – Режим доступу: <https://msn.khmnu.edu.ua/> (дата звернення 15.06.2024).

23. Психологічна служба [Електронний ресурс]. – Режим доступу [https://ps-sluzhba.khmnu.edu.ua/category/novyny/?\\_ga=2.229129556.955426337.1672832565-147095575.1669619147&\\_gl=1\\*g8i6yi\\*\\_ga\\*ODc3NjU5NzEuMTcxNTY3MDI5NQ..\\*\\_ga\\_LYXCXPXQWQ\\*MTcxODQ0NzQ2My43LjEuMTcxODQ0NzYzNS4wLjAuMA](https://ps-sluzhba.khmnu.edu.ua/category/novyny/?_ga=2.229129556.955426337.1672832565-147095575.1669619147&_gl=1*g8i6yi*_ga*ODc3NjU5NzEuMTcxNTY3MDI5NQ..*_ga_LYXCXPXQWQ*MTcxODQ0NzQ2My43LjEuMTcxODQ0NzYzNS4wLjAuMA) (дата звернення 15.06.2024).

24. Сервери авторизації [Електронний ресурс]. – Режим доступу: <https://support.usergate.com/ru/docs/version/5x/usergate-5/63-servery-avtorizacii> (дата звернення 18.06.2024).

					КРБКІ.001115.01.01 ПЗ	Арк. 84
Зм.	Арк.	№ докум.	Підпис	Дата		

25. Сервер застосунків [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80\\_%D0%B7%D0%B0%D1%81%D1%82%D0%BE%D1%81%D1%83%D0%BD%D0%BA%D1%96%D0%B2](https://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_%D0%B7%D0%B0%D1%81%D1%82%D0%BE%D1%81%D1%83%D0%BD%D0%BA%D1%96%D0%B2) (дата звернення 18.06.2024).

26. Сервер для зберігання даних (СЗД) [Електронний ресурс]. – Режим доступу: <https://it-solutions.ua/it-infrastruktura/fizichna/zberigannya/> (дата звернення 18.06.2024).

27. VirtualBox [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/VirtualBox> (дата звернення 18.06.2024).

28. Windows Server 2019 [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/Windows\\_Server\\_2019](https://uk.wikipedia.org/wiki/Windows_Server_2019) (дата звернення 18.06.2024).

29. Windows 10 [Електронний ресурс]. – Режим доступу: [https://ru.wikipedia.org/wiki/Windows\\_10](https://ru.wikipedia.org/wiki/Windows_10) (дата звернення 18.06.2024).

30. Active Directory [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/Active\\_Directory](https://uk.wikipedia.org/wiki/Active_Directory) (дата звернення 18.06.2024).

31. Відмовостійкість [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%BC%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D1%96%D0%B9%D0%BA%D1%96%D1%81%D1%82%D1%8C> (дата звернення 18.06.2024).

32. Distributed File System [Електронний ресурс]. – Режим доступу: [https://ru.wikipedia.org/wiki/Distributed\\_File\\_System](https://ru.wikipedia.org/wiki/Distributed_File_System) (дата звернення 18.06.2024).

33. Загальний ресурс [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9\\_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81](https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81) (дата звернення 18.06.2024).

34. FreeBSD [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/FreeBSD> (дата звернення 18.06.2024).

35. Debian [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/Debian> (дата звернення 18.06.2024).

36. Red Hat Enterprise Linux [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/Red\\_Hat\\_Enterprise\\_Linux](https://uk.wikipedia.org/wiki/Red_Hat_Enterprise_Linux) (дата звернення 18.06.2024).

37. CentOS [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/CentOS> (дата звернення 18.06.2024).

38. Ubuntu [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/Ubuntu> (дата звернення 18.06.2024).

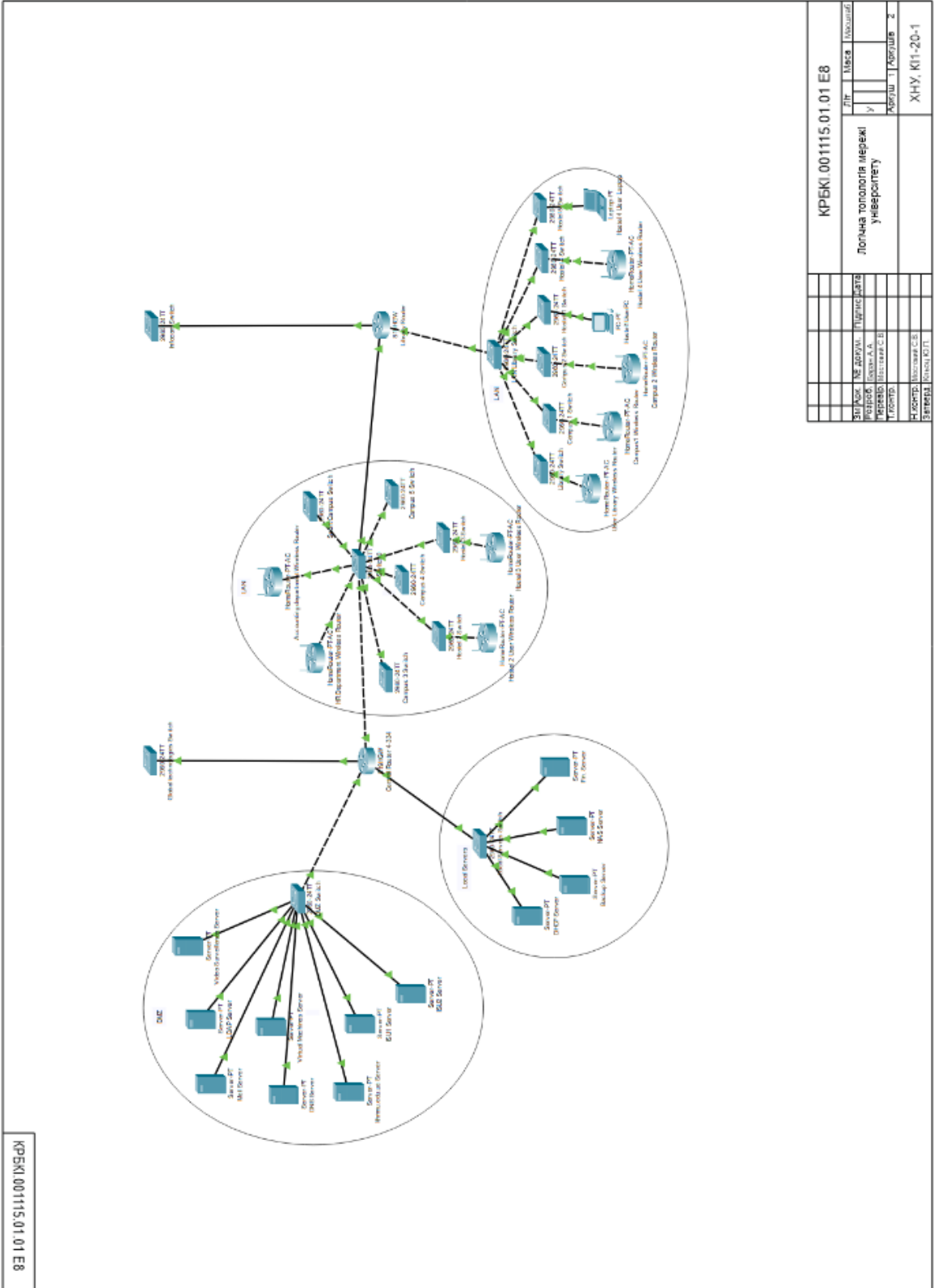
39. Ядро операційної системи [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/%D0%AF%D0%B4%D1%80%D0%BE\\_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97\\_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8](https://uk.wikipedia.org/wiki/%D0%AF%D0%B4%D1%80%D0%BE_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8) (дата звернення 18.06.2024).

40. Файлова система [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0\\_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0](https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) (дата звернення 18.06.2024).

41. Linux [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/Linux> (дата звернення 18.06.2024).

42. Microsoft Windows [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/Microsoft\\_Windows](https://uk.wikipedia.org/wiki/Microsoft_Windows) (дата звернення 18.06.2024).

# ДОДАТОК А (обов'язковий) Копія графічної частини

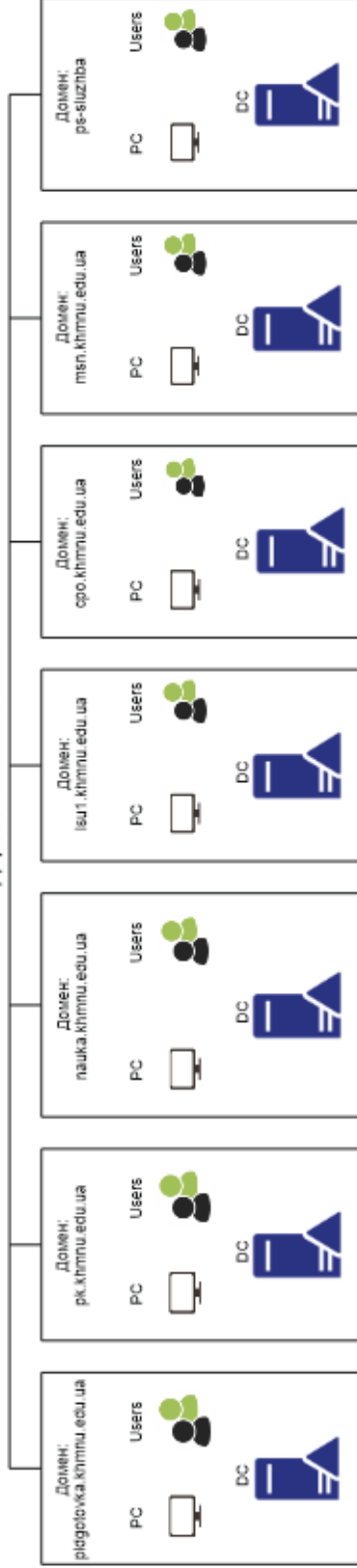


КРБК.001115.01.01.E8

КРБК.001115.01.01.E8	
ДП	Місяць
У	Рік
Квартал 1	Квартал 2
Логічна топологія мережі університету	
ХНУ, КІТ-20-1	

КРБКІ.001115.01.01 Е8

Дерево - khmnu.edu.ua



Літ.	Місяц	Масштаб
У		
Август	2	Август
2		
КРБКІ.001115.01.01 Е8		
Інфраструктура домену khmnu.edu.ua		
ХНУ, КІТ-20-1		

Завідувачу кафедри кібербезпеки  
к.т.н., доц. Кльоцу Ю.П.  
Барана Андрія Андрійовича

ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КІ1-20-1

### ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

17.06.2024

Дата



Підпис

## Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en\_US, ru\_RU, ua\_UA. Помилки в документах: 9%

ID: 131413 Назва: Система доступу до інформаційних ресурсів університету Додано в БД: 2024-06-18 Автора: Баран А.А, Керівники: Мостовий С.В, Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	72597	640	3432 (5%)	26 (4%)

### Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

Ім'я користувача:  
Кафедра кібербезпеки

Дата перевірки:  
18.06.2024 22:26:59 EEST

Дата звіту:  
18.06.2024 22:31:09 EEST

ID перевірки:  
1016373394

Тип перевірки:  
Doc vs Internet + Library

ID користувача:  
100008300

Назва документа: Баран А.А. На плагіат

Кількість сторінок: 74 Кількість слів: 10335 Кількість символів: 81697 Розмір файлу: 5.29 MB ID файлу: 1016180885

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

## 15.4% Схожість

Найбільша схожість: 3.56% з Інтернет-джерелом ([https://msn.khnu.km.ua/mod/page/view.php?id=10201&lang=es\\_es](https://msn.khnu.km.ua/mod/page/view.php?id=10201&lang=es_es))

14.9% Джерела з Інтернету

548

Сторінка 76

0.75% Джерела з Бібліотеки

53

Сторінка 78

## 0% Цитат

Вилучення цитат вимкнено

Вилучення списку бібліографічних посилань вимкнено

## 0% Вилучень

Немає вилучених джерел

## Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Підозріле форматування

29  
сторінок

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ  
КАФЕДРИ КІБЕРБЕЗПЕКИ  
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система доступу до інформаційних ресурсів університету

Автор: Баран Андрій Андрійович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Мостовий Сергій Володимирович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 84,6%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (<https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf>, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи



Сергій МОСТОВИЙ

Завідувач кафедри кібербезпеки



Юрій КЛЮЧ

**РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ**  
освітнього ступеня «бакалавр»

Дипломник Баран Андрій Андрійович  
Тема Система доступу до інформаційних ресурсів університету  
Спеціальність 123 – Комп'ютерна інженерія

**Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:**

кількість листів креслень 2; кількість сторінок записки 86

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та розгорнуто систему доступу до інформаційних ресурсів університету, що дозволяє проводити централізоване управління всіма ресурсами та користувачами системи,

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети. У першому розділі проведено огляд та аналіз сучасних технологій доступу до інформаційних ресурсів організацій, виконана постановка задачі. В другому розділі виконано аналіз інформаційних ресурсів університету та політик безпеки, спроектовано логічну структуру домену. В третьому розділі виконано розгортання та впровадження системи, а також виконано її тестування.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Практична цінність результатів дослідження полягає в обґрунтуванні вибору засобів для проєктування та розгортання систем доступу до інформаційних ресурсів організацій

5. Негативні сторони роботи В роботі відсутній деталізований опис вибору засобів для розгортання системи, а також недостатньо висвітлено питання групових політик безпеки домену.

---

---

---

---

---

---

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

---

---

---

---

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

---

---

---

---

8. Інші зауваження \_\_\_\_\_

---

---

---

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».


РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) \_\_\_\_\_  
Бойко Юлій Миколайович, професор кафедри ТМІТ, доктор, технічних наук, професор

---

---

---

« 19 » \_\_\_\_\_ 06 \_\_\_\_\_ 2024р.

 \_\_\_\_\_ (підпис)