МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему: «Віртуалізація комп'ютерної мережі
для модернізації та оптимізації роботи LAN кафедри ІТ»

за спеціальністю 122 «Комп'ютерні науки»,
освітньо-професійна програма «Інформаційні технології проектування»

Виконавець роботи: студент групи ІТ-81-9 Шевченко Данило Олександрович

Кваліфікаційна робота бакалавра
захищена на засіданні ЕК
з оцінкою _____ «__» _____2022 р.

Науковий керівник _____ к.т.н., доц., Антипенко В. П.
(підпис) (науковий ступінь, вчене звання, прізвище та ініціали)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів
без відповідних посилань.

Студент _____
(підпис)

Суми-2022

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра інформаційних технологій
Спеціальність 122 «Комп'ютерні науки»
Освітньо-професійна програма «Інформаційні технології проектування»

ЗАТВЕРДЖУЮ
Зав. кафедри ІТ

_____ В. В. Шендрик
«__» _____ 2022 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА СТУДЕНТУ

Шевченко Данило Олександрович

1 Тема роботи *Віртуалізація комп'ютерної мережі для модернізації та оптимізації роботи LAN кафедри ІТ*

керівник роботи *Антипенко Вікторія Петрівна, к.т.н., доцент*,

затверджені наказом по університету від « 27 » квітня 2022 р. №0301_VI

2 Строк подання студентом роботи « 14 » червня 2022 р.

3 Вхідні дані до роботи технічне завдання на розробку проєкту для віртуалізації комп'ютерної мережі для модернізації та оптимізації LAN кафедри ІТ

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) аналіз предметної області, моделювання мережі, віртуалізація комп'ютерної мережі для модернізації та оптимізації LAN кафедри ІТ

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) актуальність роботи, постановка задачі, аналіз аналогів, засоби реалізації, структурно-функціональне моделювання, діаграма варіантів використання, віртуалізація мережі, інтеграція з сервісами Azure, демонстрація роботи мережі

6. Консультанти розділів роботи:

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7.Дата видачі завдання_____6 жовтня 2021_____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Планування робіт	До 06.05.2022	
2	Написання технічного завдання	До 12.05.2022	
3	Аналіз предметної області	До 16.05.2022	
4	Проектування мережі	До 23.05.2022	
5	Віртуалізація мережі	До 29.05.2022	
6	Інтеграція з сервісами Azure	До 07.06.2022	
7	Оформлення пояснювальної записки	До 14.06.2022	
8	Підготовка до захисту роботи	До 20.06.2022	

Студент _____ Шевченко Д.О.
(підпис)

Керівник роботи _____ к.т.н., доц. Антипенко В.П.
(підпис)

РЕФЕРАТ

Тема кваліфікаційної роботи бакалавра «Віртуалізація комп’ютерної мережі для модернізації та оптимізації роботи LAN кафедри ІТ»

Пояснювальна записка складається зі вступу, трьох розділів, висновків, списку використаних джерел із 31 найменування, п’яти додатків. Загальний обсяг пояснювальної записки складає 97 сторінок, у тому числі 72 сторінок основного тексту, 3 сторінки списку використаних джерел, 22 сторінки додатків.

Кваліфікаційну роботу бакалавра присвячено віртуалізації комп’ютерної мережі для оптимізації роботи LAN кафедри ІТ.

У першому розділі досліджено актуальність даного проекту. Також проведено аналіз існуючих технологій створення мереж. Виділено їх переваги та недоліки. Виконано опис новітніх технологій побудови мереж. Проведений аналіз недоліків існуючої мережі. Після чого було сформульовано мету та задачі проекту, визначено засоби реалізації проекту.

У другому розділі виконано структурно-функціональне моделювання. Було визначено варіанти використання мережі. У результаті створено контекстну діаграму IDEF0, її декомпозицію та діаграму варіантів використання.

У третьому розділі було створено та змодульовано хмарну мережеву інфраструктуру. Також реалізована інтеграція з окремим сервісами платформи Azure. Продемонстровано результат даного проекту. Роботу мережі протестовано.

Практичне значення даного проекту полягає в оптимізації роботи локальної обчислювальної мережі кафедри ІТ за рахунок її віртуалізації та модернізації шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій.

Ключові слова: ВІРТУАЛІЗАЦІЯ, LAN, СЕРВЕР, МЕРЕЖА, MICROSOFT AZURE, WINDOWS SERVER, ХМАРНІ ТЕХНОЛОГІЇ.

ЗМІСТ

ВСТУП

На сьогоднішній день неможливо уявити роботу підприємства без використання цифрових технологій. Однією з таких інформаційних структур є локальна обчислювальна мережа. Вона допомагає зв’язати наявні служби разом, прискорює обіг даних та об’єднує всі робочі станції та периферійні пристрої.

Активне поширення локальних мереж почалося приблизно у 1980-их роках і триває й надалі. Із того часу вони пройшли багато ступенів розвитку. На даний час сформовані деякі представлення щодо їх проектування. Наприклад, були виділені важливі властивості мереж, окремі набори ір-адрес та сформовані як їх основні топології, так і FDDI, Ethernet та Token Ring [1].

Для підтримки мережі в оптимальному стані, її відповідності сучасним вимогам, потрібно своєчасно оновлювати структуру, сервіси та технічну базу. Якщо не приділяти цьому увагу, вона швидко застаріє й не зможе ефективно функціонувати. Проблема модернізації полягає в тому, щоб спроектувати мережу, яка б відповідала всім представленим вимогам. Також необхідно виділяти найбільш необхідні з них. При цьому необхідним є звернення уваги на бюджетні та технічні можливості.

Реалізація даного проекту допоможе підвищити продуктивність роботи мережі. Зокрема збільшиться її пропускна здатність. Також зменшиться затримка її роботи, втрати даних та мережеві помилки. Взагалі дана модернізація принесе ряд переваг. Після неї зросте швидкість роботи мережі, її безпека та безпека користувачів, а також контроль адміністратора над системою.

Отже, метою даного проекту є оптимізація роботи локальної обчислювальної мережі кафедри ІТ за рахунок її віртуалізації. Модернізацію можна здійснити шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій.

Для досягнення поставленої мети необхідно виконати наступні задачі:

– дослідити актуальність роботи та її предметну область;

– проаналізувати можливі способи реалізації серверу;

– визначення недоліки існуючої топології та встановити нові вимоги до мережі;

– визначити оптимальні методи для модернізації локальної мережі;

– розробити схеми та практичні моделі нової мережі;

– виконати віртуалізацію мережі;

– протестувати роботу мережі, можливість віддаленого підключення, функціонування всіх сервісів.

Результати роботи були апробовані на науково-практичній конференції ІМА-2022 у Сумському державному університеті [2].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд останніх досліджень і публікацій

Локальна обчислювальна мережа (Local Area Network – LAN) – це об’єднання робочих станцій та периферійних пристроїв на невеликій відстані. Вони з’єднуються між собою за допомогою швидкісних ліній зв’язку. Це дозволяє їм спільно використовувати програмні та апаратні ресурси. Зазвичай LAN створюється в межах однієї організації. Такі мережі також можуть називатися корпоративними системами. Найпростішим прикладом LAN є два комп’ютери, які з’єднані між собою кабелем. Приклад складнішої її варіації – це декілька клієнтів підключених до сервера, що представляє собою більш потужний комп’ютер. У таких мережах із робочих станції можна отримати доступ до інформації, яка знаходиться як на сервері, так і на інших комп’ютерах. Робочі станції призначені для того, щоб на них працювали користувачі, а сервери – для обслуговування робочих станцій. Сервери використовують для об’єднання й розподілу ресурсів LAN між робочими станціями. Як сервер може використовуватися один досить потужний комп’ютер. До нього можна додати ще декілька комп’ютерів, які будуть виступати як резервні.

Раніше один виділений сервер використовували для окремого сервісу, як, наприклад, сервер електронної пошти чи веб-сервер. Розвиток технологій віртуалізації надає можливість на одній робочій станції виділяти окремі ресурси. Це дозволило запускати на серверах декілька операційних систем із реалізацією різних сервісів [3].

У сучасних реаліях є можливість використати послугу по оренді хмарного серверу замість використання фізичного. Це буде вигідніше фінансово та дозволить не виконувати спеціальне технічне обслуговування, що буде роботи відповідний провайдер. Тому вона є досить актуальною сьогодні. Ця послуга базується на застосуванні хмарних технологій. Тобто користувач може використовувати виділені

йому ресурси компанією-провайдером. Це дозволить знизити затрати на експлуатацію, тому що всі виплати на електроенергію та технічне обслуговування бере на себе надавач послуг, та підвищити надійність та відмовостійкість мережі, так як в дата центрах є великий запас резервної потужності [4].

Додавання серверу до LAN надає можливість виділити деякий централізований пункт управління системою. Це звісно не означатиме повний контроль над всіма пристроями в мережі, але підвищить зручність адміністрування деякими сервісами.

Тому, для відповідності сучасним вимогам є актуальним проводити своєчасну модернізацію мережі. Це допоможе підвищити як зручність її управління для адміністратора, так і рівень безпеки, та дозволить впровадити нові сервіси.

На сьогоднішній день існує багато компаній, які займаються хмарними технологіями. Останні почали свій розвиток у 2006 році. Тоді команда Amazon Web Services (AWS) запустила власні сервіси Amazon Simple Queuing Service та Amazon Simple Storage Service. Після цього вони впроваджували інноваційні технології з віртуальними мережами. У 2010 році компанія Microsoft представила свою платформу, подібну до AWS, під назвою Azure. Через деякий час теж саме зробили і в Google, з їх Google Cloud Platform. Ці три платформи є основними постачальниками послуг на ринку хмарних технологій і предоставляють великий спектр сервісів, від баз даних до сервісів додатків, інструментарія DevOps та сервісів штучного інтелекту. У цій роботі буде використовуватися платформа та сервіси Microsoft Azure [5].

У сучасності Azure – це об’єднання концепцій моделі як платформи (PaaS) та інфраструктури як сервісу (IaaS). Є можливість використання як сторонніх сервісів, так і компанії Microsoft, в якості моделі програмного забезпечення як сервісу (SaaS). IaaS є основною категорією хмарних служб. У цій схемі користувач орендує інфраструктуру (сервери, віртуальні машини, мережі тощо) у хмарного провайдера. За допомогою всього вищеперерахованого можна реалізувати гібридну хмару. Вона буде поєднувати в собі локальну інфраструктуру та хмару, забезпечуючи спільний доступ до даних та програм. Azure дає такі інструменти для реалізації проєкту, як віртуальний робочий стіл, можливість реалізації Windows Server, інструменти

управління ресурсами для оптимізації та автоматизації роботи, також можливість інтеграції із окремими сервісами, що додає більшої гнучкості [6].

1.2 Аналіз існуючих продуктів-аналогів

Для оцінки поточної мережі потрібно виділити ключові фактори для порівняння. Вони можуть відрізнятися в залежності від призначення LAN. Для мережі кафедри інформаційних технологій (ІТ) було виділено ряд факторів, які потребують модернізації. Це безпека мережі та користувачів, реалізація окремих сервісів, управління груповими політиками, віддалений доступ до інформації та можливість віддаленої роботи.

Безпека користувачів та мережі полягає в таких можливостях, як створення окремого аккаунту для кожного клієнта, обмеження прав доступу до системи, розбиття користувачів на окремі групи. Створення унікального профілю дає можливість виділити для нього деяку частину дискового простору, в якому можна буде зберігати власні робочі файли, до яких доступ матиме лише він та учасники групи з правами адміністратора. Обмеження прав доступу дозволить забезпечити безпеку операційної системи (ОС). Це буде можливим, оскільки клієнтам будуть доступними тільки ті файли, які обиратиме адміністратор при налаштуванні. Розбиття користувачів на окремі групи дозволяє керувати політиками доступу у відповідності до створеної групи, а не індивідуально для кожного. Це достатньо збільшує продуктивність роботи та зручність адміністрування, що відбувається у менеджері управління групами (рис. 1.1) [7].

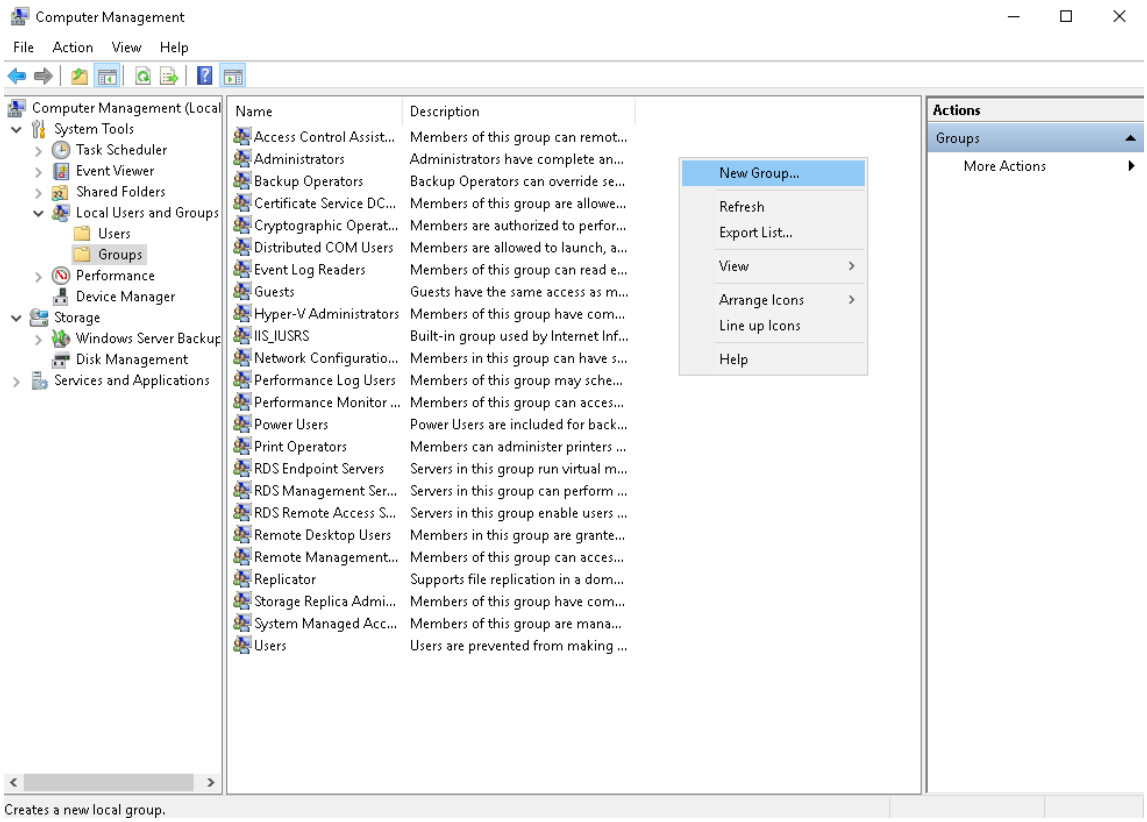

Рисунок 1.1 – Менеджер управління групами користувачів в ОС Windows Server

Можливість встановлювати різні сервіси, під сервісами мається на увазі ролі сервера, це програмне забезпечення за допомогою якого сервер може виконувати певні функції (рис. 1.2). До таких ролей, наприклад, відносяться: dhcp-сервер, dns-сервер, веб-сервер та FTP-сервер.

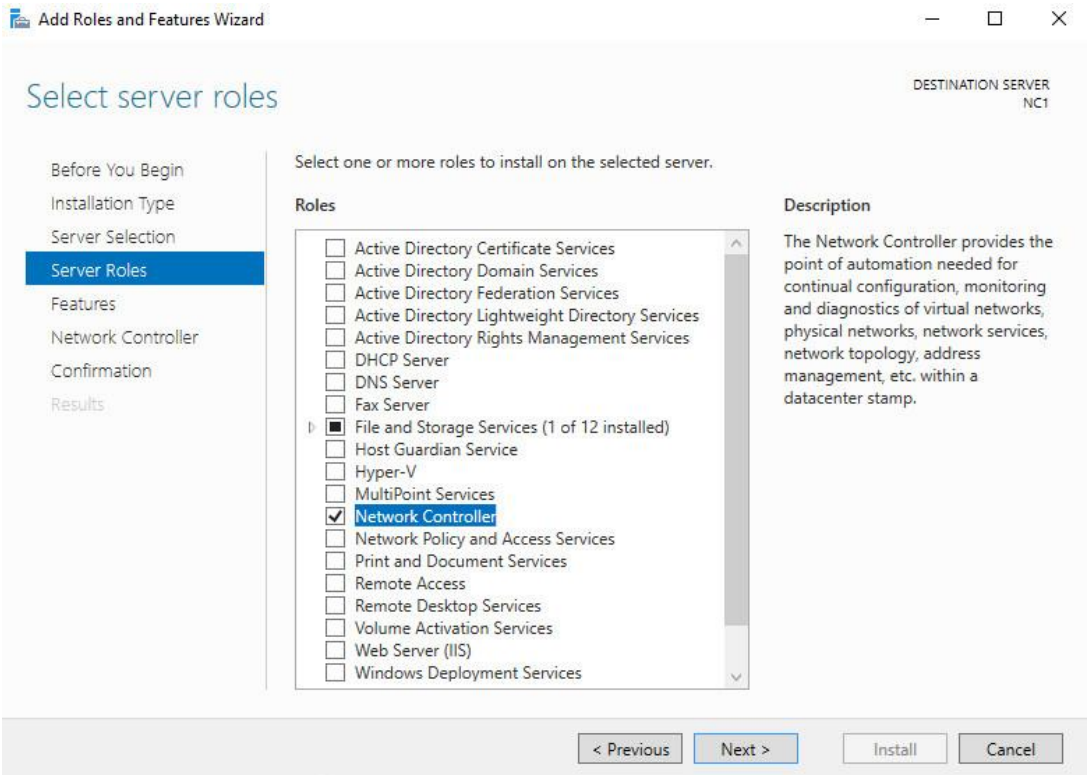

Рисунок 1.2 – Менеджер управління ролями серверу
в ОС Windows Server

Віддалений доступ до інформації та можливість роботи реалізується за рахунок ролі серверу, яка відповідає за служби віддалених робочих столів та віддаленого доступу. Наприклад, в операційних системах сімейства Windows Server використовується служби терміналів Remote Desktop Services (RDS) [8]. Підключення до робочої станції відбувається за допомогою протоколу Remote Desktop Protocol (RDP) [9]. Це дає змогу користувачу підключитися до серверу та працювати, використовуючи його апаратні та програмні ресурси. При чому для використання віддаленого робочого столу клієнтом, не обов’язково використовувати стаціонарний комп’ютер. Можна застосувати так званий апаратний тонкий клієнт (рис. 1.3). Це спеціальні пристрої, які мають мінімальну апаратну конфігурацію та невеликий розмір. На них встановлена спеціалізована операційна система. Їх головна задача – це зв’язок із термінальним сервером [10].

Рисунок 1.3 – Приклад тонкого клієнта

Групові політики – це інструмент адміністрування, який дозволяє отримати централізоване керування налаштуваннями на клієнтських станціях та серверах, працюючих у домені (це сервер, що контролює певну область комп’ютерної мережі) [11]. В операційних системах сімейства Windows Server такий інструмент працює на архітектурі Active Directory (рис. 1.4). У Unix-подібних системах використовується пакет програмного забезпечення Samba [12]. Групові політики мають два компонента – серверний та клієнтський. Перший використовується для управління адміністративними налаштуваннями, як, наприклад, налаштування безпеки, шаблонів, встановлення програмного забезпечення. Клієнтський компонент відповідає за налаштування політик, які відносяться до клієнтських робочих станцій. Active Directory можна використовувати, наприклад, для таких задач, як налаштування принтерів та доступу до каталогів та програм, установлення та оновлення програмного забезпечення тощо [13].

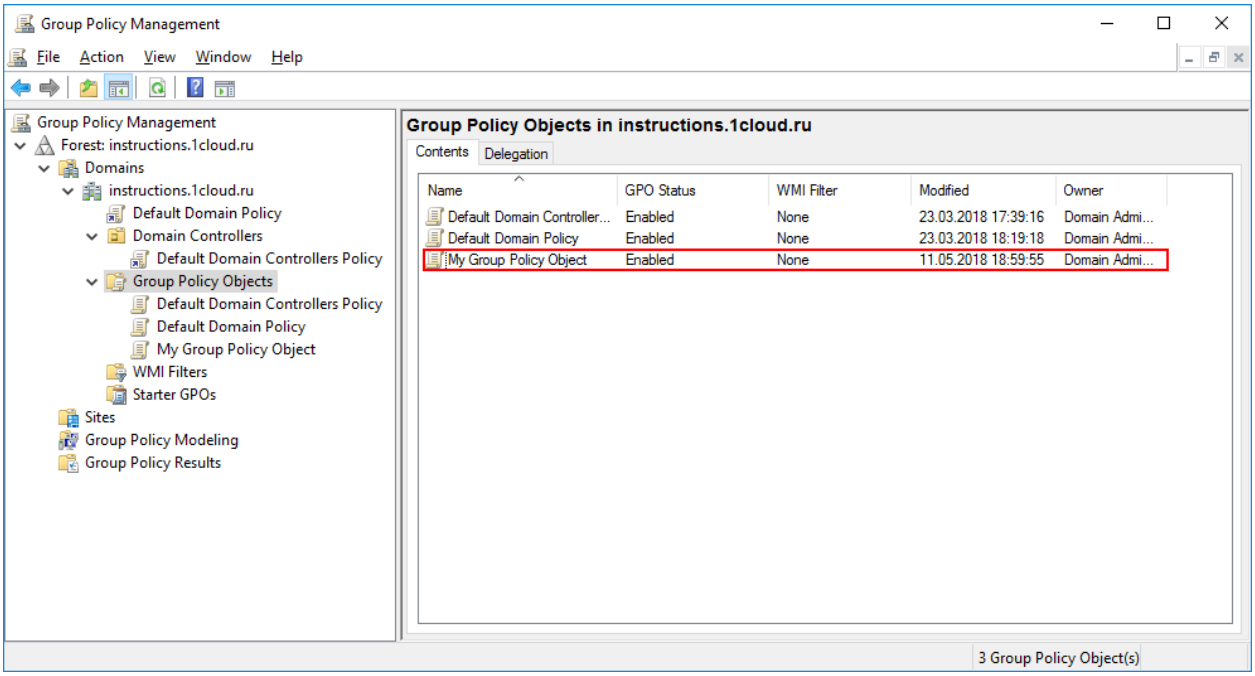

Рисунок 1.4 – Менеджер управління груповими політиками Active Directory

Після аналізу існуючої мережі кафедри IT і її характеристик з потенціально новою, було визначено ряд їх переваги та недоліки. Його результати представлені в таблиці 1.1.

Таблиця 1.1 – Порівняльна таблиця характеристик двох LAN

Параметр порівняння	Актуальна мережа	Нове рішення
Окремий аккаунт для кожного користувача	-	+
Заборона доступу до файлів	+	+
Заборона доступу до перегляду директорій	-	+
Віддалений доступ до системи	-	+
Управління серверними груповими політиками	-	+
Управління клієнтськими груповими політиками	+	+
Можливість встановлення ролей серверу	-	+
Простота в обслуговуванні	+	-

Були проаналізовані головні недоліки існуючої мережі. Дивлячись на це, можемо їх усунути та модернізувати LAN кафедри IT із оглядом на сучасні вимоги, застосовуючи технологію хмарних сервісів.

Для модернізації комп'ютерної мережі було вирішено створити сервер, використовуючи сервіс хмарних технологій. Це дозволить виділити деякий централізований пункт управління. У свою чергу, дана можливість збільшить контроль над мережею. Також використання хмарних технологій дозволить реалізувати нові функції, які визначені у вимогах.

Використання платформи Azure дає можливість для інтеграції звичного методу розгортання серверу з окремим сервісами. На приклад резервне копіювання можна повністю перекласти на сторону хмари, воно буде здійснюватися зовнішніми інструментами. Також є можливість замість додавання нових дисків коли закінчується пам'ять створити спеціальну мережеву директорію. Або ж в доповнення до серверу можна створити окремі віртуальні машини, що візьмуть на себе запуск специфічних застосунків.

Звичайно створити сервер можна фізично. Він буде розташовуватися на території кафедри та потребувати спеціальних умов зберігання. Даний сервер потребує регулярного технічного обслуговування, що буде виконуватися спеціалістом. Усі експлуатаційні витрати, які стосується електроенергії, адміністрування, апаратного оновлення лягають на плечі штатної команди [14].

При використанні ж хмарного сервісу дані будуть розміщені у стороннього постачальника послуг. Він бере на себе всі обов'язки по технічному обслуговуванню. Це потребує орендної плати раз на місяць. Для управління надається обліковий запис, який відкриває доступ до служб. Це відбувається через мережу Інтернет за допомогою веб-браузера або спеціального програмного додатку [14].

Однією з найбільших переваг хмарних рішень є відсутність початкових фінансових вкладень. Досить часто такі витрати виходять менше, ніж сума, яку б витратили на покупку фізичного обладнання. Для точного рахування вартості, зазвичай компанії надають спеціальний калькулятор для обрахування ціни. Економія

на ресурсах залежить від об’єму інфраструктури; для невеликих мереж вона буде вигідніша.

Тому, зважаючи на вищевказані переваги і недоліки, було вирішено провести модернізацію існуючої мережі кафедри ІТ за рахунок використання хмарних технологій.

1.3 Постановка задачі

Метою даного проекту є оптимізація роботи локальної обчислювальної мережі кафедри ІТ за рахунок її віртуалізації, модернізація шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій.

Основні вимоги до проекту є наступні:

– підвищити рівень безпеки в мережі для користувачів за рахунок створення індивідуальних профілів;

– підвищити рівень безпеки мережі за рахунок розмежування прав доступу користувачів;

– додати можливість введення в роботу різних сервісів, інтегрувавши інфраструктуру з Azure;

– додати можливість управління груповими політиками, реалізуючи Windows Server;

– збільшити діапазон можливостей управління мережею для адміністратора, через додавання централізованого пункту управління;

– збільшити відмовостійкість за рахунок перекладння роботи по обслуговуванню мережі на хмарного провайдера;

– покращити можливість для масштабування мережі за рахунок використання хмарної інфраструктури;

– реалізувати можливість доступу до файлів та можливість продовжувати роботу в виділеній операційній системі з віддаленого вузла, реалізувавши сервіси віддаленої роботи.

Для реалізації поставленої мети потрібно вирішити такі задачі:

– дослідити актуальність роботи та її предметну область;

– проаналізувати можливі способи реалізації серверу;

– визначення недоліки існуючої топології та встановити нові вимоги до мережі;

– визначити оптимальні методи для модернізації локальної мережі;

– розробити схеми та практичні моделі нової мережі;

– виконати віртуалізацію мережі;

– протестувати роботу мережі, можливість віддаленого підключення, функціонування всіх сервісів.

Проект розроблюється з оглядом на використання його результатів на кафедрі IT студентам, викладачами та робочим персоналом.

Технічне завдання на розробку продукту у повному обсязі наведено у Додатку А.

Для практична реалізації даного проекту було обрано платформу хмарних обчислень Azure, будуть використані сервіси створення мережевої інфраструктури та віртуальних машин для реалізації Windows Server. До серверу будуть інтегровані окремі сервіси Azure, як наприклад гнучка хмарна інфраструктура віртуальних робочих столів (AVD), для створення сесій віддаленого управління окремими застосунками [15].

2 МОДЕЛЮВАННЯ МЕРЕЖІ

2.1 Структурно-функціональне моделювання

Моделювання складається з етапів, які пов’язані між собою. Цей процес починається з абстрактної концептуальної схеми. Після неї створюються логічна та фізична моделі.

IDEF (Integrated Definition) – це графічна методологія моделювання процесів. Вона використовується для впровадження систем та інженерного програмного забезпечення. Ці методи використовуються в функціональному моделюванні даних, об’єктно-орієнтованому аналізі й отриманні знань [16].

Для нових систем, IDEF0 може використовуватися для визначення вимог і характеристик функцій. А потім розробки реалізації, яка відповідає вимогам і виконує призначені функції. Для існуючих систем, IDEF0 може використовуватися для аналізу функцій, що виконуються системою та реєстрації механізмів (засобів), за допомогою яких вони виконуються [17].

Результатом застосування IDEF0 до тієї чи іншої системи є модель, яка складається з ієрархічного ряду діаграм із супровідним пояснювальним текстом, що мають перехресні посилання один на одного [17].

Для контекстної діаграми були визначено такі дані:

– Вхідні дані: запити користувачів;

– Вихідні дані: безперебійна робота в мережі;

– Управління: права доступу, дані для авторизації;

– Механізми: Microsoft Azure, Microsoft Active Directory, Server Manager, Remote Desktop Protocol. При створенні даної моделі використовувався веб-додаток «draw.io». На рисунку 2.1 зображена контекстна діаграма роботи LAN мережі.

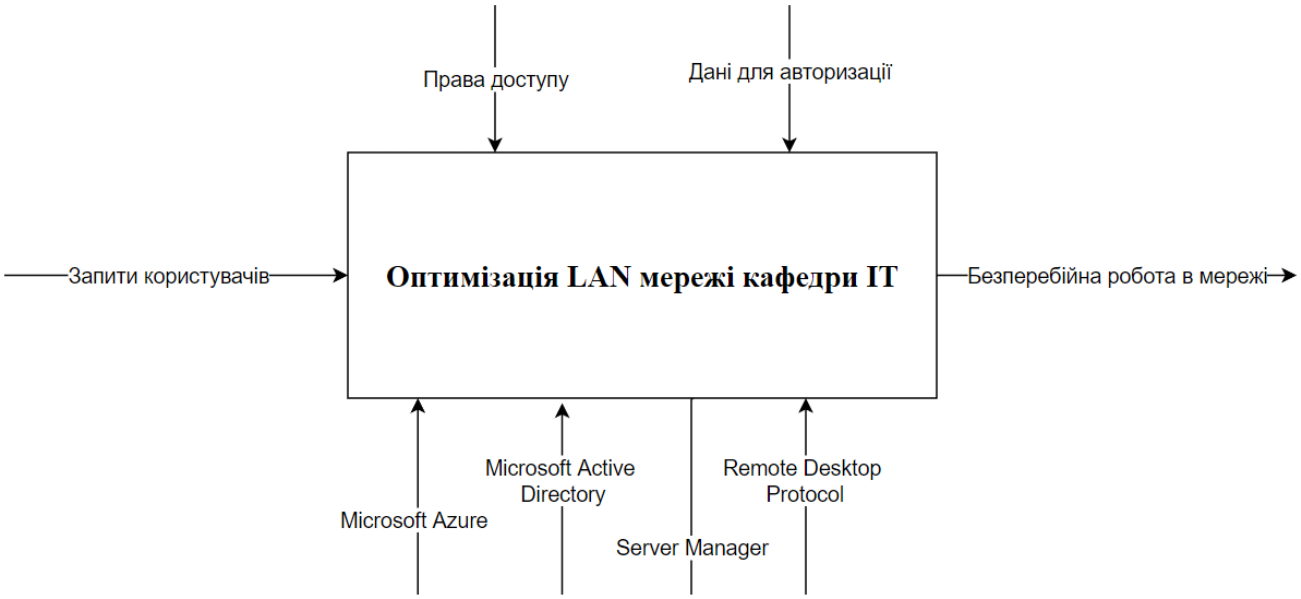

Рисунок 2.1 – Контекстна діаграма IDEF0

Побудована контекстна діаграма представляє декомпозицією нульового рівня. Вона дає можливість отримати загальне представлення про роботу створюваної системи. Для більш детального її опису було здійснено декомпозицію першого рівня, яка представлена на рисунках 2.2-2.5.

Декомпозиція була проведена з огляду на можливості різних користувачів.

Діаграма роботи мережі з точки зору студентів представлена такими підпроцесами:

- авторизація;
- розмежування прав доступу;
- виділена ділянка пам’яті для власних файлів;
- перегляд навчальних матеріалів.

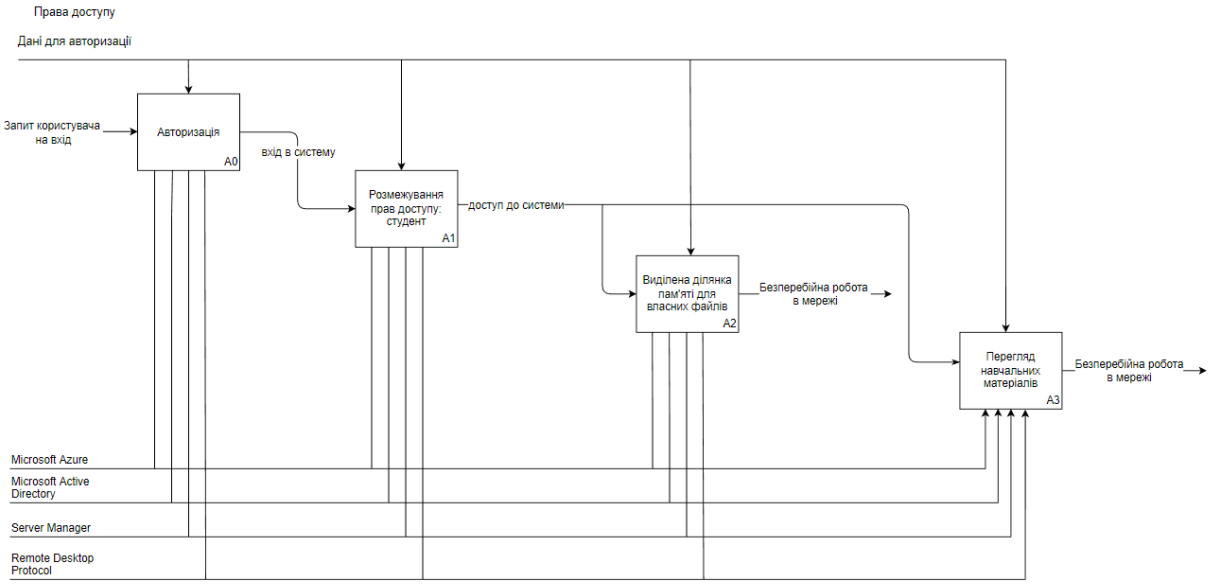

Рисунок 2.2 – Діаграма декомпозиції роботи студента

Діаграма роботи мережі з точки зору викладачів представлена такими підпроцесами:

- авторизація;
- розмежування прав доступу;
- виділена ділянка пам’яті для власних файлів;
- перегляд та редагування навчальних матеріалів.

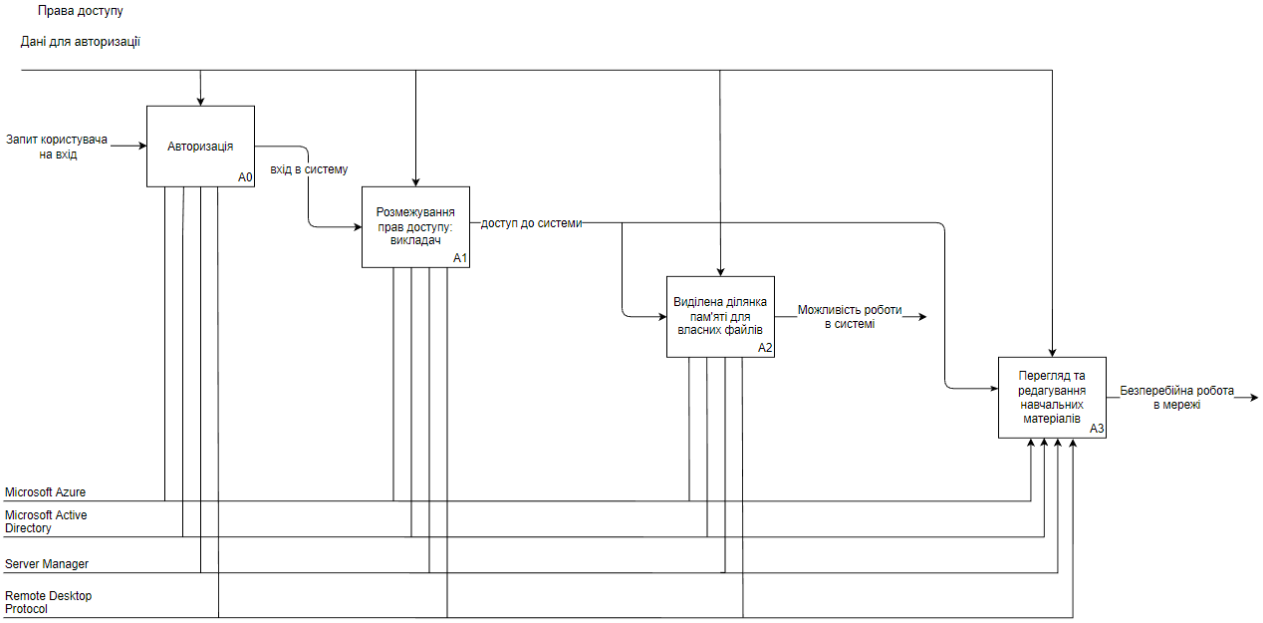

Рисунок 2.3 – Діаграма декомпозиції роботи викладача

Діаграма роботи мережі з точки зору адміністратора представлена такими підпроцесами:

- авторизація;
- розмежування прав доступу;
- доступ до всіх ділянок пам’яті;
- встановлення, видалення та оновлення програмного забезпечення (ПЗ);
- перегляд та редагування всіх файлів в системі.

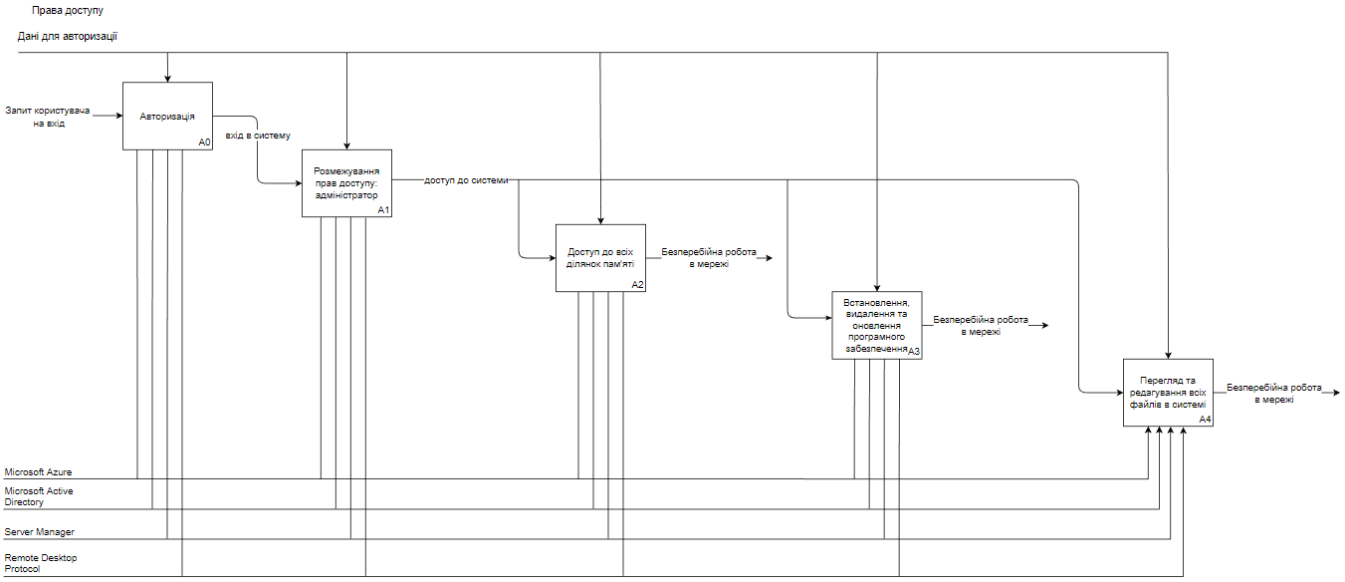

Рисунок 2.4 – Діаграма декомпозиції роботи адміністратора

Діаграма роботи мережі з точки зору головного адміністратора представлена такими підпроцесами:

- авторизація;
- розмежування прав доступу;
- доступ до всіх ділянок пам’яті;
- встановлення, видалення та оновлення ПЗ;
- перегляд та редагування всіх файлів в системі;
- управління налаштуваннями серверу.

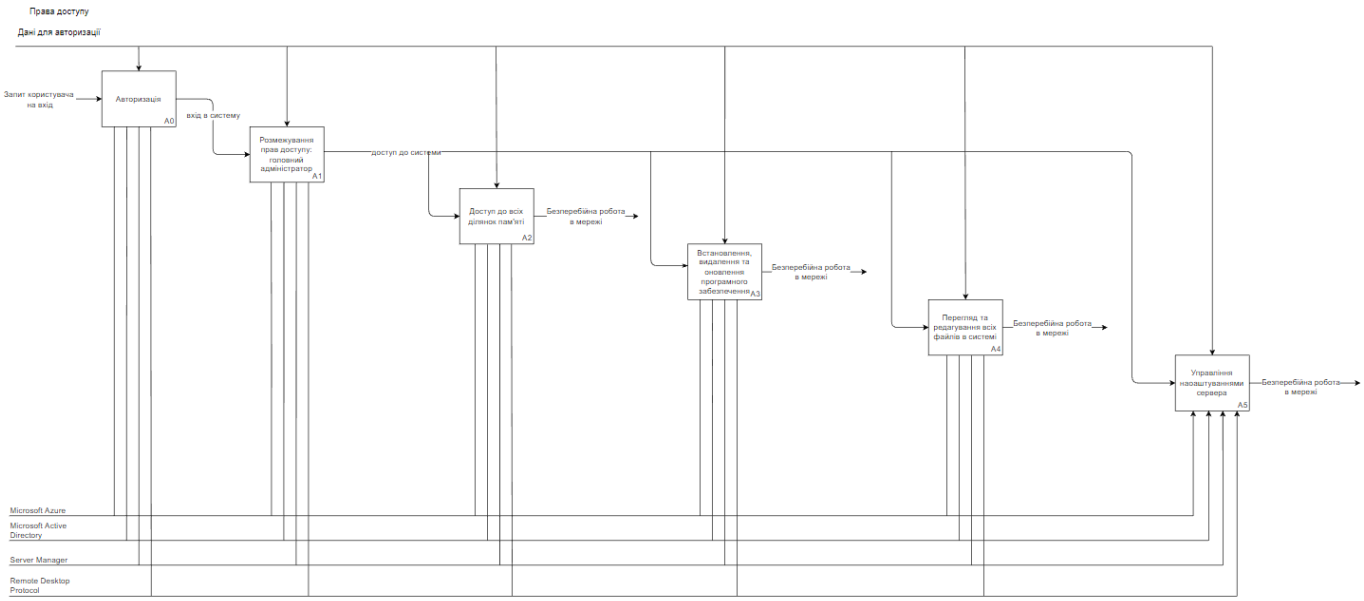

Рисунок 2.5 – Діаграма декомпозиції роботи головного адміністратора

Інформація про вхідні та вихідні дані діаграм представлена в таблиці 3.1.

Таблиця 2.1 – Вхідні та вихідні дані

Стрілка/ Підпроцес	**Вхідні дані**	**Управління**	**Механізми**	**Вихідні дані**
Авторизація	Запити користувача на вхід	Права доступу, Дані для авторизації	Microsoft Azure, Microsoft Active Directory, Server Manager, Remote Desktop Protocol	Вхід в систему
Розмежування прав доступу;	Вхід в систему			Доступ до системи
Виділена ділянка пам’яті для власних файлів;	Доступ до системи			Безперебійна робота в мережі
Перегляд навчальних матеріалів, редагування навчальних матеріалів				
Доступ до всіх ділянок пам’яті				

Продовження таблиці 2.1 – Вхідні та вихідні дані

Встановлення, видалення та оновлення ПЗ;	Доступ до системи	Права доступу, Дані для авторизації	Microsoft Azure, Microsoft Active Directory, Server Manager, Remote Desktop Protocol	Безперебійна робота в мережі
Перегляд та редагування всіх файлів в системі.				
Управління налаштуваннями серверу.				

2.2 Моделювання варіантів використання

Для досягнення цілей функціонування спочатку будується модель у формі діаграми варіантів використання (use-case diagram), яка описує функціональне призначення системи [18]. Діаграма варіантів використання є вихідною концептуальною моделлю системи в процесі її проектування та розробки.

При реалізації діаграми було виділено декілька акторів: студент, викладач, адміністратор та головний адміністратор. Були сформовані наступні варіанти використання:

- перегляд навчальних матеріалів;
- редагування навчальних матеріалів;
- робота з виділеною ділянкою пам’яті;
- перегляд та редагування всіх файлів в системі;
- доступ до всіх ділянок пам’яті;

– встановлення, видалення та оновлення ПЗ;

– управління налаштуваннями серверу.

Діаграма варіантів використання в нотації UML представлена на рисунку 2.6.

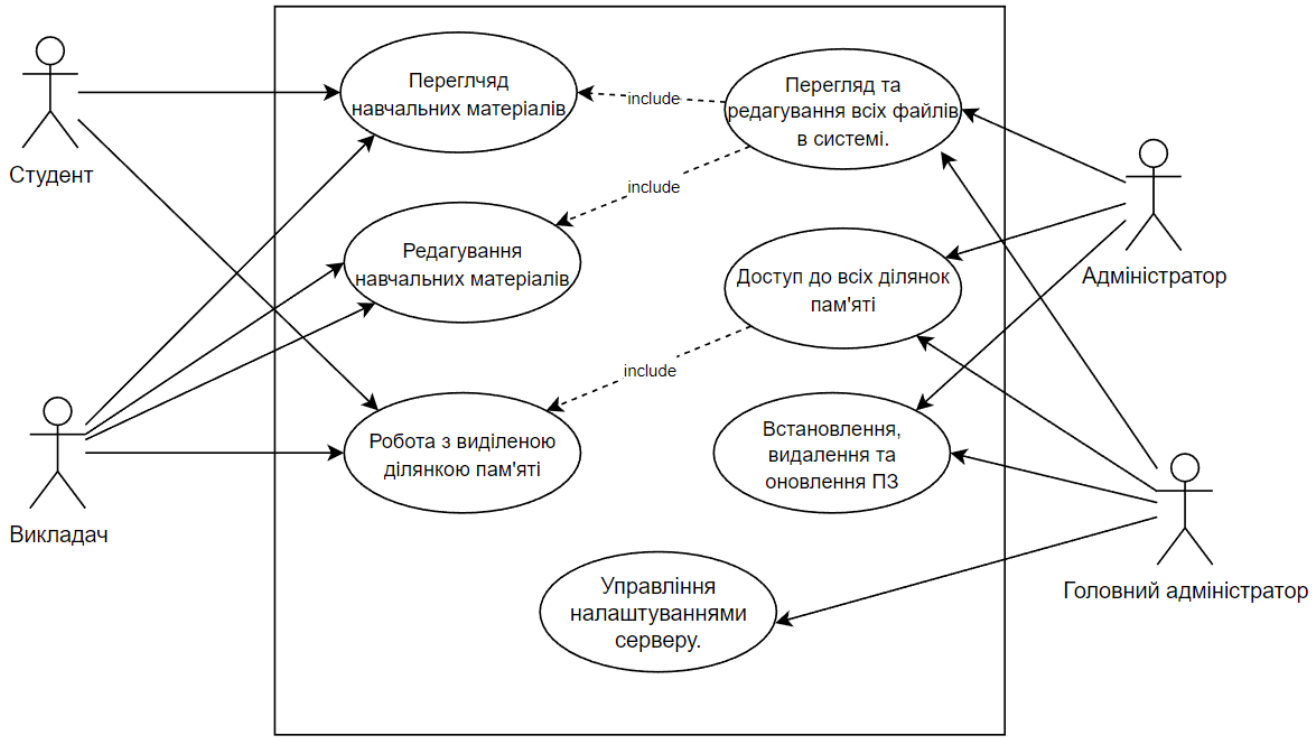

Рисунок 2.6 – Діаграма варіантів використання

3 ВІРТУАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ МОДЕРНІЗАЦІЇ ТА ОПТИМІЗАЦІЇ РОБОТИ LAN КАФЕДРИ ІТ

3.1 Віртуалізація на основі Windows Server

На даний момент існуюча мережа повністю організована як on-premise інфраструктура. Це означає, що вся вона розміщена в кампусі університету й адмініструється локально. А це спонукало до її модернізації. Для цього було вирішено перенести центр адміністрування у хмару. Проєкт вирішено реалізовувати, використовуючи Microsoft Azure. Ця хмарна платформа надає значну кількість сервісів для вирішення поставлених задач.

Як основний елемент мережі була створена віртуальна машина (Virtual Machine – VM), на яку встановлено серверну ОС. Вона по суті представляє звичну реалізацію зі знайомими інструментами.

Для початку було створено ресурсну групу. Це контейнер, в якому розміщені всі зв'язані між собою сервіси, які виділені для певної цілі, як, наприклад, віртуальний шлюз (рис. 3.1) [19]. При його створенні потрібно було обрати підписку та регіон, в якому потенційно зберігатимуться дані. Також зазначається назва контейнеру.

Наступний крок – це створення виділеної віртуальної мережі. Мовою оригіналу – Virtual Network (VNet). Вона потрібна, щоб попередньо виділені ресурси в межах групи могли обмінюватися даними між собою. За принципом дії VNet досить схожа на традиційну LAN. Вона є основою для приватної мережі Azure. Це дає змогу пристроям, таким як віртуальні машини, безпечно встановлювати з'єднання між собою, Інтернетом та LAN [20].

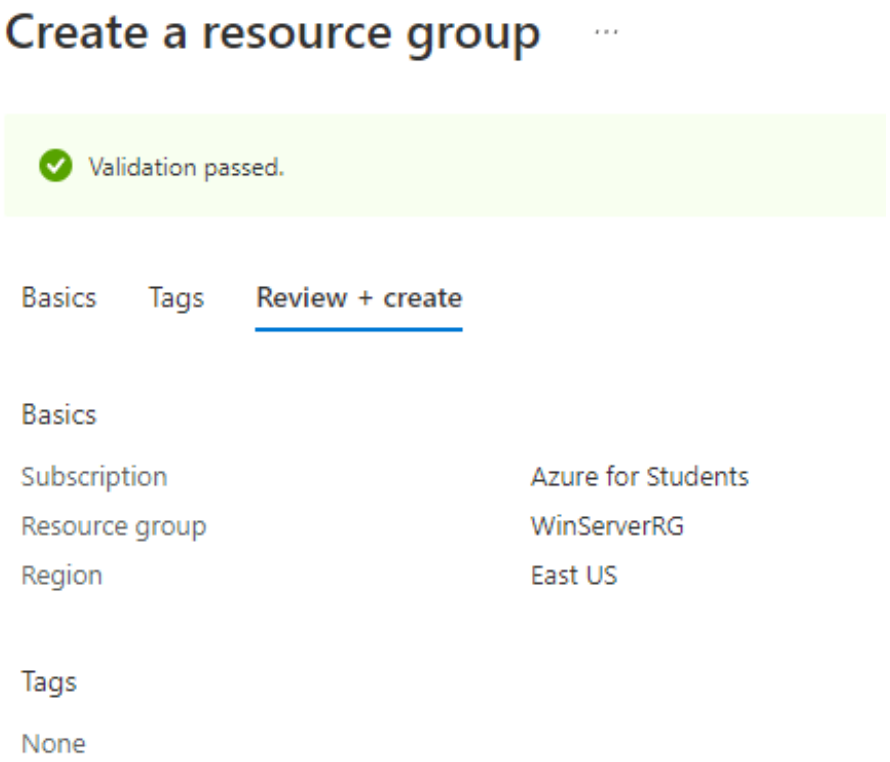

Рисунок 3.1 – Створення ресурсної групи

Тут, як і у випадку з ресурсною групою, обрано підписку, назву та регіон розміщення. У розділі адресації обрано ip-діапазон та виділено маски підмереж. Також зазначено, які параметри безпеки будуть встановлені (рис. 3.2).

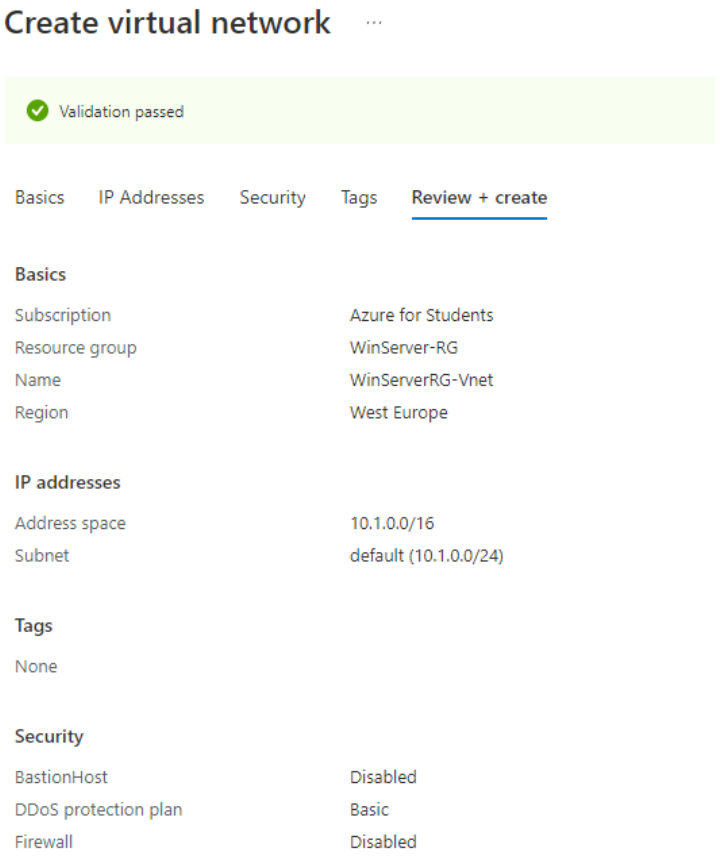

Рисунок 3.2 – Створення віртуальної мережі

Наступним кроком є створення VM. Слід зазначити, що тут вибір регіону це не те ж саме, що регіон, який був обраний під час створення ресурсної групи. Компанія Microsoft має спеціальну веб-сторінку, де можна подивитись затримку від локації користувача до найближчих датацентрів. У рекомендаціях зазначено, що для нормальної роботи вона має бути не більше 150 мс, але для повністю безперебійної роботи – менше 100 мс.

Далі було обрано образ, який буде встановлено. На порталі доступні тисячі образів, від операційних систем до окремих застосунків, також можна завантажити свої образи. Наступним був обраний вид віртуальної машини, що відображає апаратні характеристики. Списки можуть змінюватись відносно обраного регіону (рис. 3.3) [21].

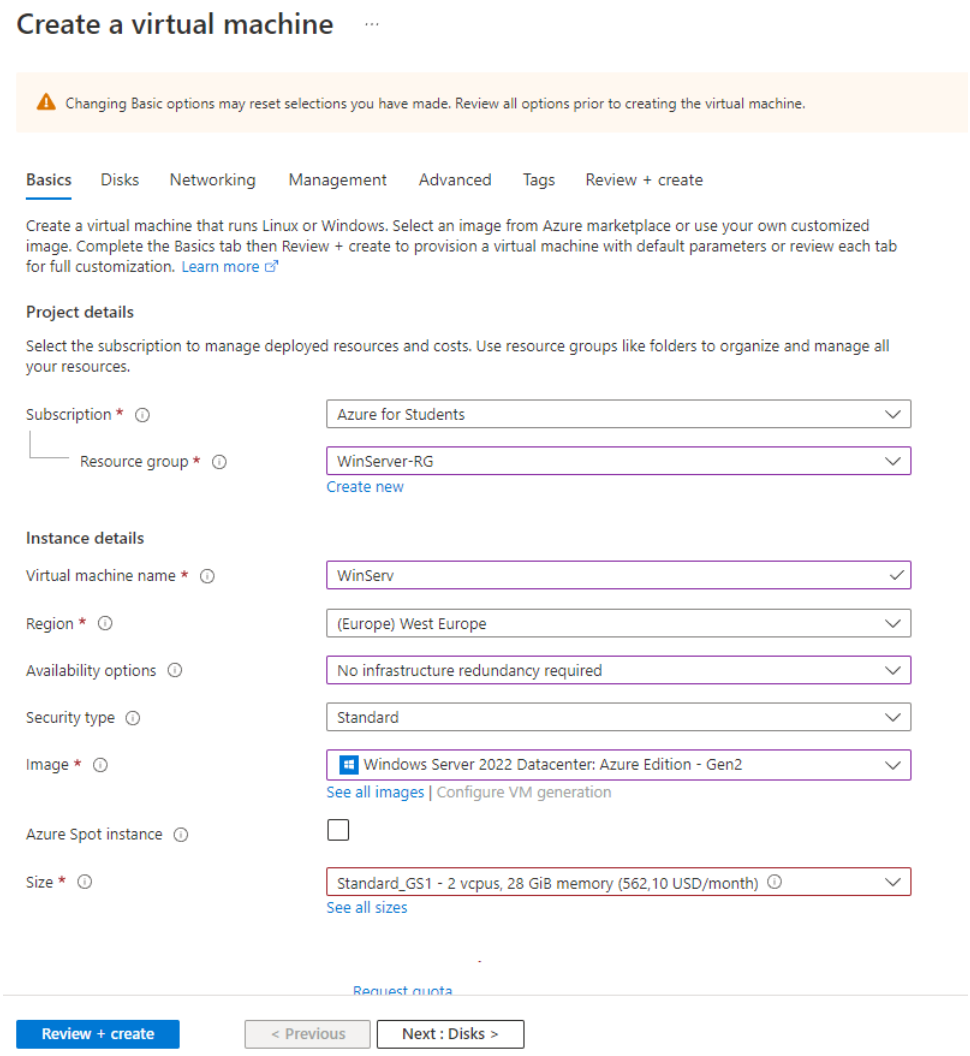

Рисунок 3.3 – Створення віртуальної машини

Віртуальну машину було підключено до раніше створеної мережі. Тут же задано вид захисту та зазначено відкриті порти. Обраний RDP порт потрібен для підключення до віртуальної машинин та її налаштування (рис. 3.4).

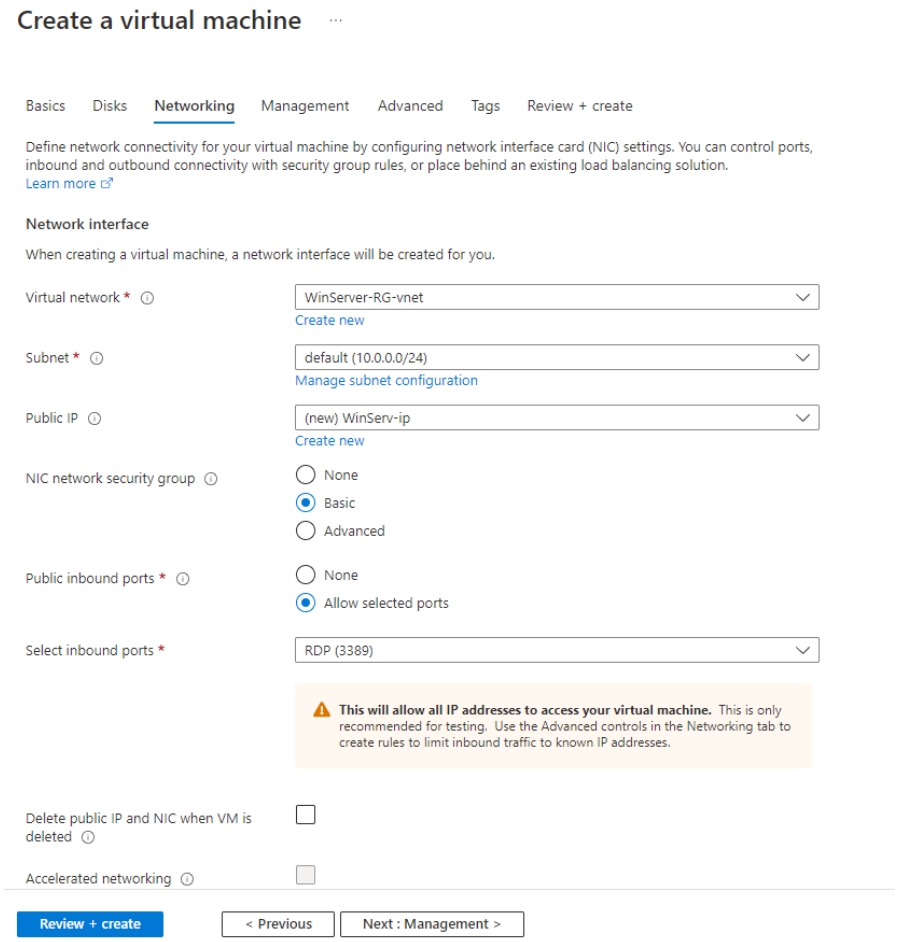

Рисунок 3.4 – Вибір віртуальної мережі

На рисунку 3.5 можна побачити уже створену віртуальну машину та панель управління нею. Тут зазначені основні характеристики й звідси здійснюється керування. Azure дозволяє змінити апаратні характеристики машини, якщо виникне така потреба, додати ще один диск, налаштувати резервне копіювання, а також відслідковувати стан роботи через меню моніторингу.

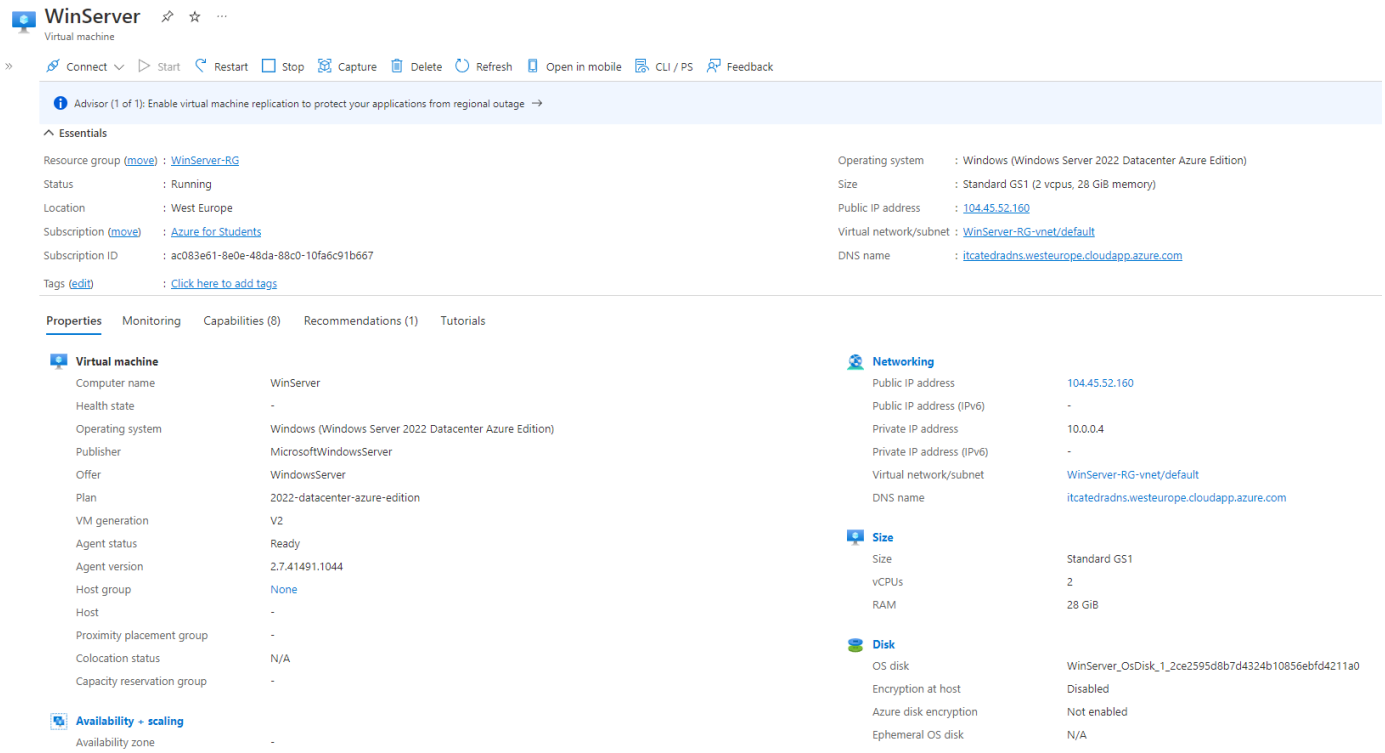

Рисунок 3.5 – Створена віртуальна машина

Після завершення всіх дій із віртуальними ресурсам час перейти до налаштування самого Windows Server. При першому запуску автоматично запуститься сервер менеджер. Ця утиліта допомагає керувати системою та встановленими ролями й функціями. У вікні відображено повідомлення, яке можна назвати коротким планом налаштування (рис. 3.6). Для початку було зроблено стандартний набір дій: встановлено правильний часовий пояс, задано статичну ip-адресу, змінено ім’я системи.

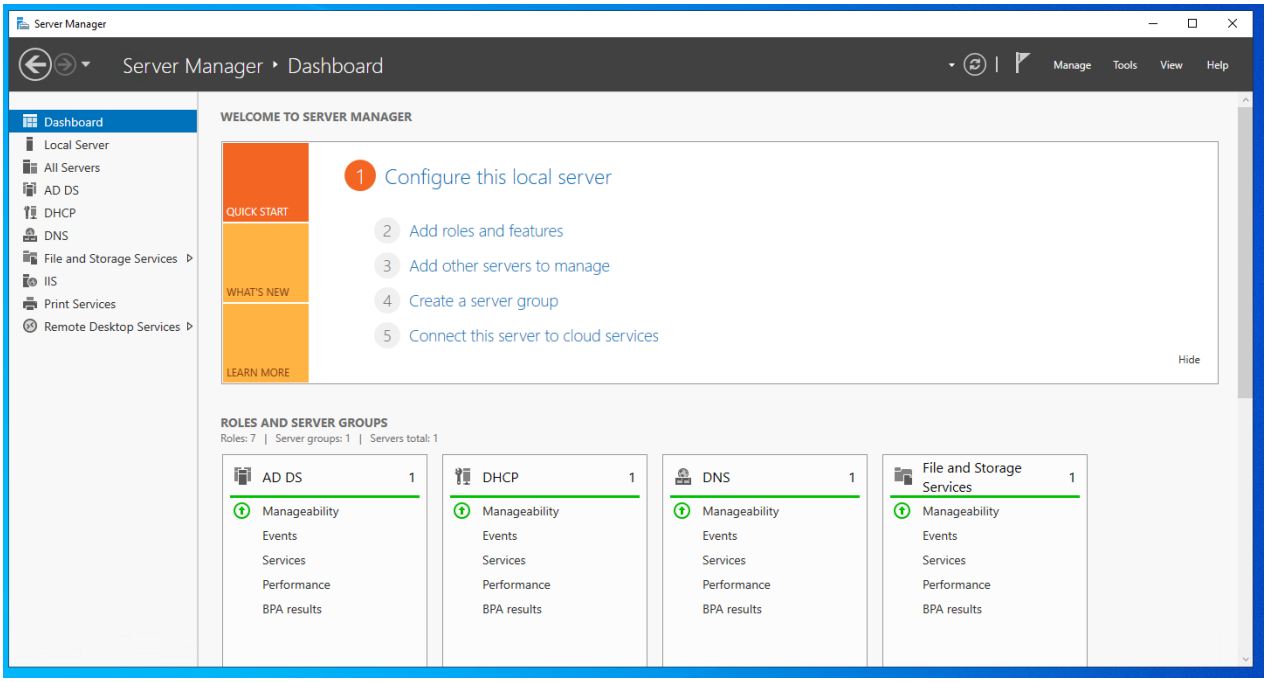

Рисунок 3.6 – Утиліта Server Manager

Далі час перейти до встановлення ролей і компонентів. Найважливішим із широкого списку є служба Active Directory (AD). Вона надає методи для управління й зберігання даних каталогів, можливість зберігати інформацію про профілі, їх імена, номера телефонів, електронні адреси, тощо. AD дозволяє користувачам мати унікальні аккаунти, і переглядати інформацію один про одного за потреби.

Active Directory є ієрархічною структурою, ліс та домен є її основою. Перші представляють об'єднання всіх об'єктів. Один ліс може містити декілька дерев зв'язаних між собою. Вони, в свою чергу, можуть складатися з декількох доменів, де кожен з них має контролер. Також наявним є унікальне ім'я в середині структури. Домени об'єднують в собі організаційні підрозділи. Мовою оригіналу –Organizational Unit (OU). Вони створюють ієрархію в середині домену й можуть містити як і інші OU, так і користувачів. Це розподілення призводить до більшого контролю над реплікацією даних і зменшує навантаження на мережу, тому що дані не копіюються там де не потрібно [22]. Спрощена структурна схема роботи сервісу Active Directory показана на рисунку 3.7.

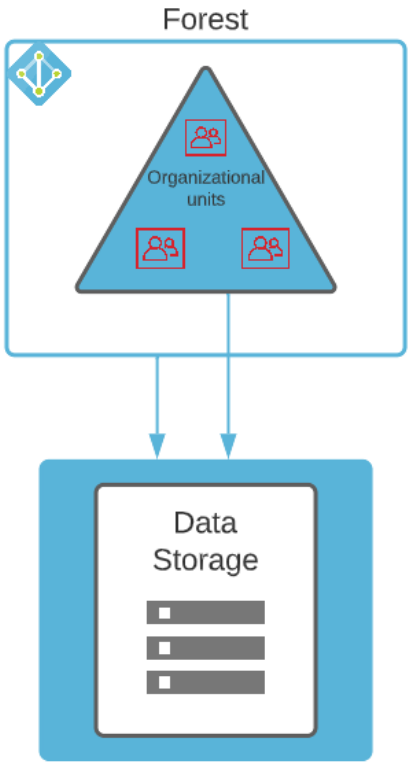

Рисунок 3.7 – Структура служби Active Directory

Під час встановлення було створено новий ліс з кореневим доменом itcatedra.com (рис. 3.8).

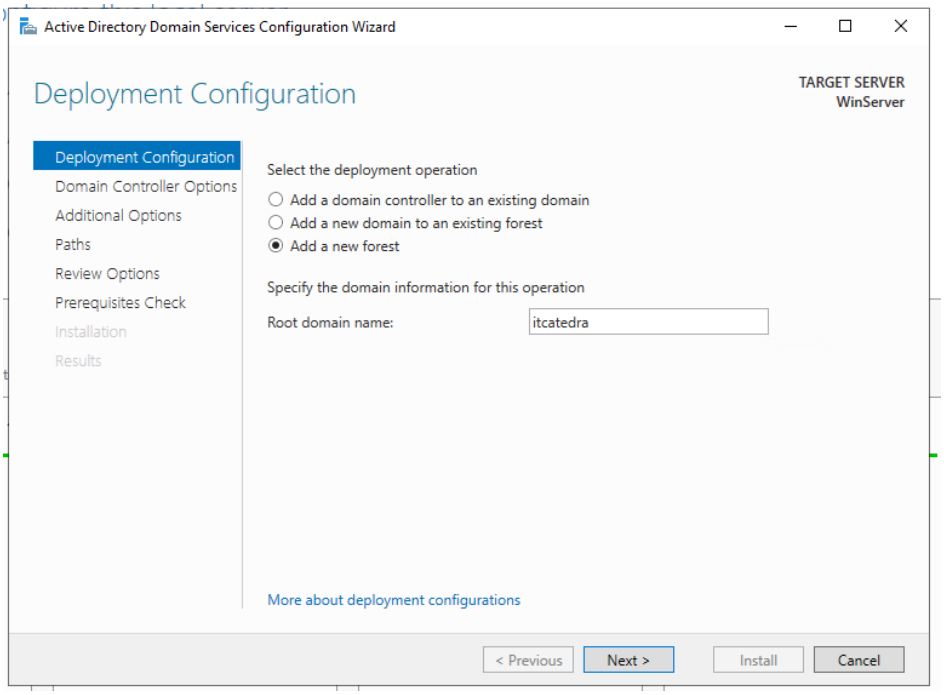

Рисунок 3.8 – Створення нового доменного лісу

Разом із службою AD була встановлена роль DNS серверу (рис. 3.9).

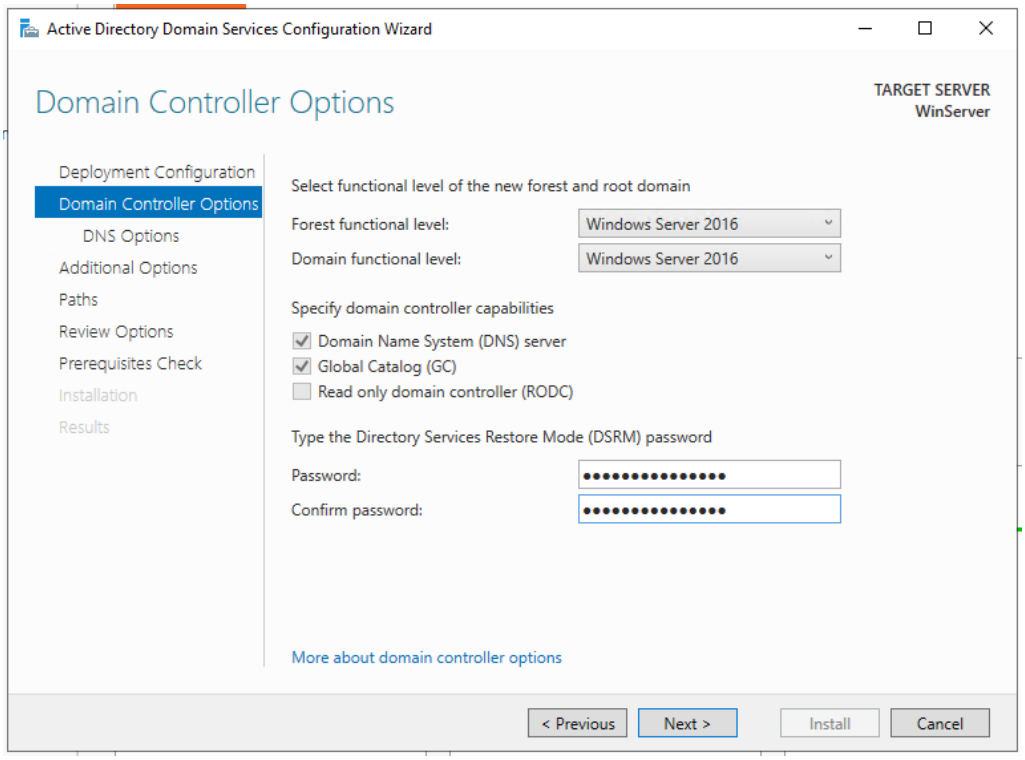

Рисунок 3.9 – Налаштування контролеру домену

Після перезавантаження видно, що комп’ютер знаходиться у новому домені (рис. 3.10).

Рисунок 3.10 – Домен сервера

Для управліннями профілями використовується інструмент AD Users and Computers. Через нього відбувається створення нових організаційних підрозділів, окремих облікових записів та груп користувачів. Були створені нові OU для студентів та викладачів (рис. 3.11). При великій кількості користувачів їх потрібно об’єднувати в групи для більш простішого розподілення прав доступу.

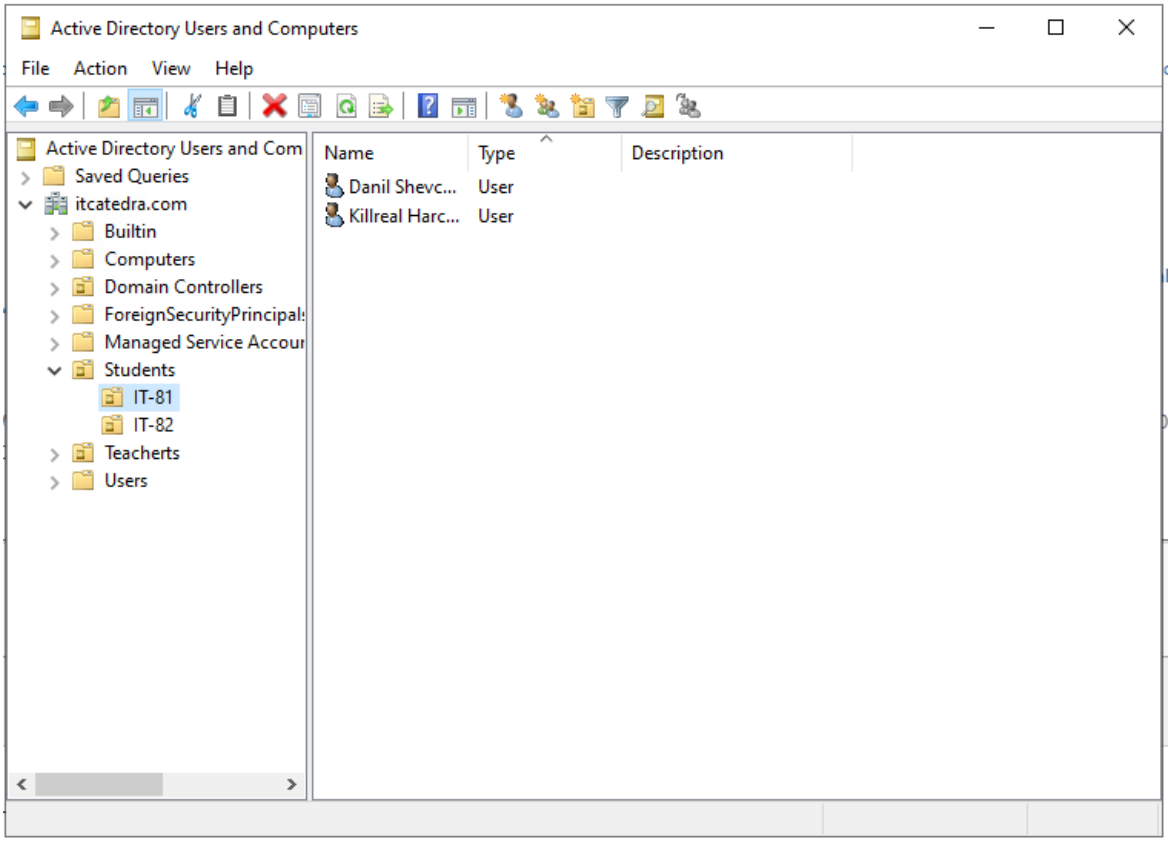

Рисунок 3.11 – Менеджер управління профілями користувачів та комп’ютерів

Наступним кроком було налаштування групових політик для користувачів. Це робиться за допомогою інструменту Group Policy Management. Даний інструмент дозволяє ефективно застосовувати засоби по контролю за безпекою мережі та системи. Групові політики призначаються до окремих OU і можуть включати управління як користувачем, так і окремим комп’ютером [23]. Було заборонено встановлення програм із носіїв, і будь-який інсталяційний файл має запускатися з правами адміністратора (рис. 3.12).

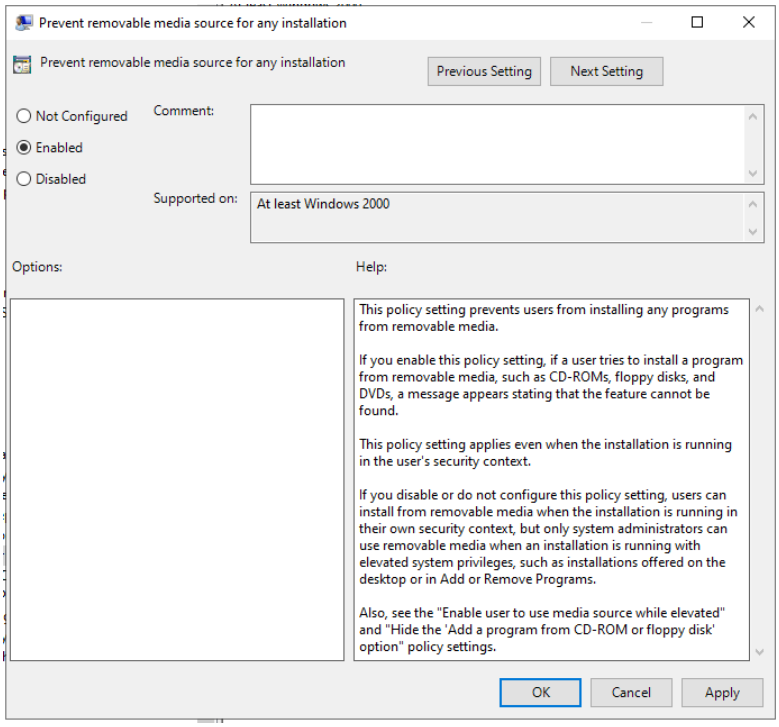

Рисунок 3.12 – Встановлення параметру групової політики

Папки користувачів будуть розташовані на окремому диску. Через групові політики обраний том був схований від відображення. Створення папки реалізовано через спеціальну функцію GPO. Директорія повинна створюватися автоматично при вході користувача в систему (рис. 3.13).

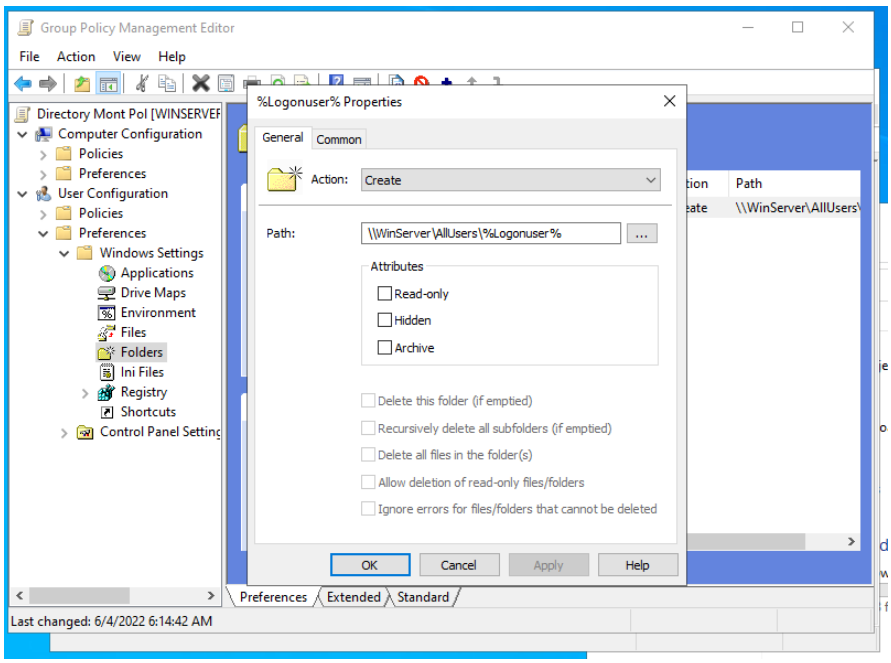

Рисунок 3.13 – Створення директорії для користувачів

Також за допомогою GPO можна директорію змонтувати як окремий віртуальний диск. Процедура схожа зі створенням папки й буде виконуватися при вході користувача в систему (рис. 3.14).

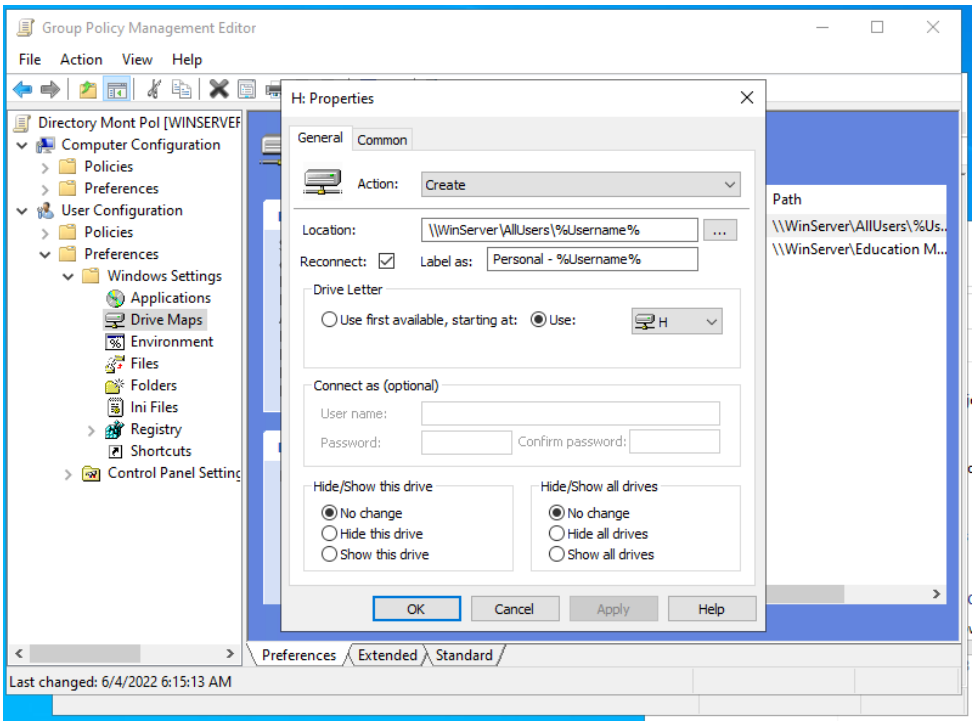

Рисунок 3.14 – Монтування мережевого диску

У результаті змонтовані диски відображаються як показано на рисунку 3.15.

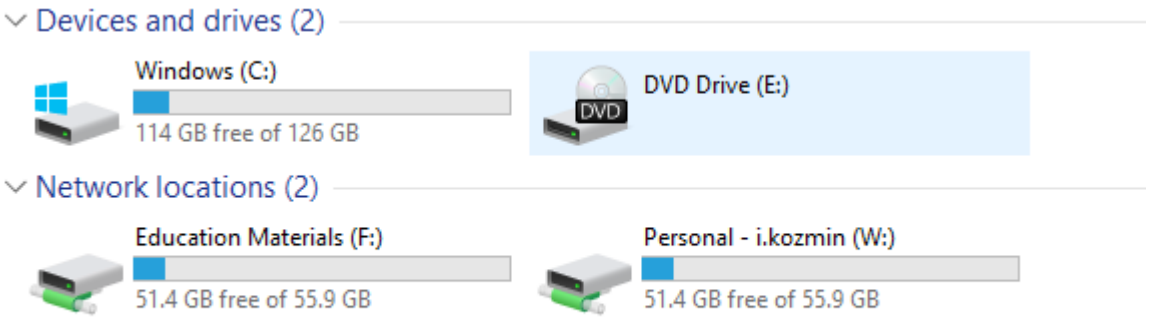

Рисунок 3.15 – Змонтовані мережеві диски

Також до диску було призначено спеціальні квоти. Це можна зробити через GPO, або ж через налаштування на томах NTFS. У меню властивостей тома є можливість обмежити кількість пам’яті, що доступна користувачу [24]. Квоти будуть працювати для нових користувачів (рис. 3.16).

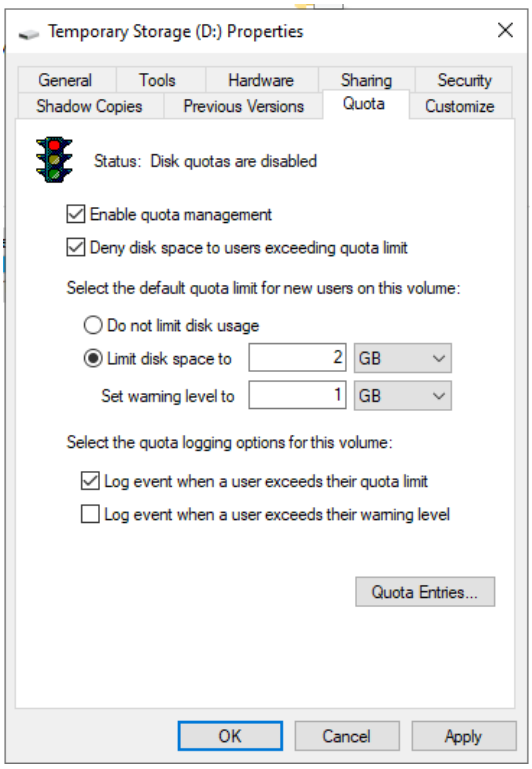

Рисунок 3.16 – Встановлення дискових квот

Профілі, які вже зареєстровані за замовчуванням не мають встановленого ліміту. Через таблицю записів є можливість встановлення квоти для кожного окремого користувача (рис. 3.17-3.18).

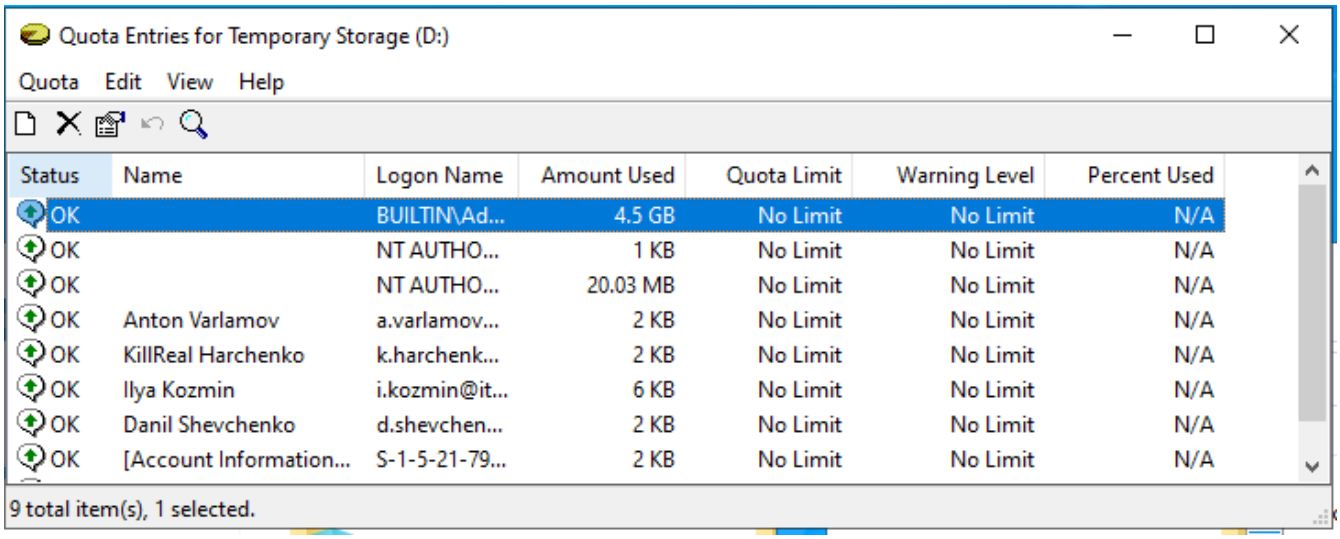

Рисунок 3.17 – Список індивідуальних квот

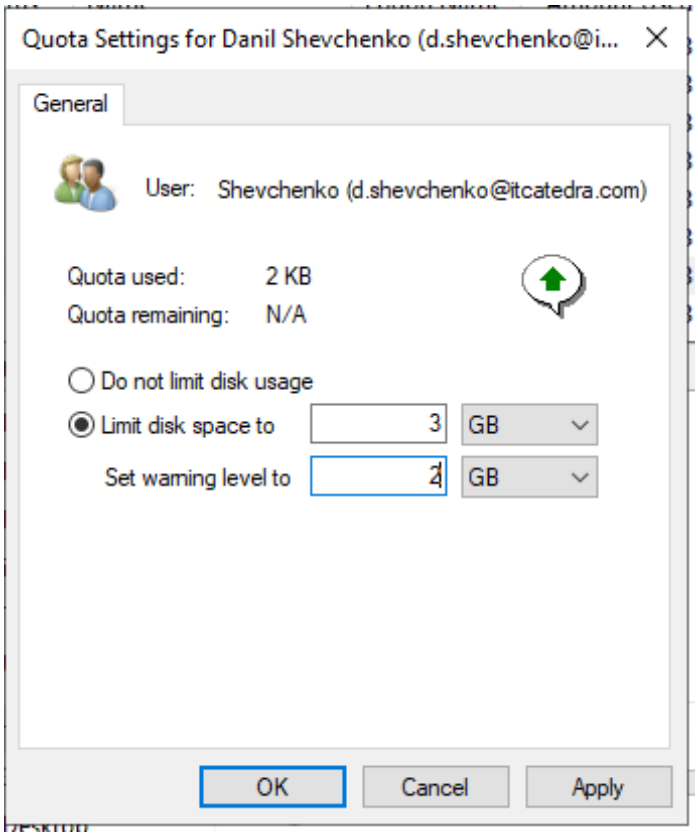

Рисунок 3.18 – Встановлення індивідуальної квоти для користувача

Також для надання спільного доступу до директорій чи файлів є спеціальний інструмент File and Storage Services, де можна обрати диск або вказати шлях до папки, якій потрібно призначити цю властивість (рис. 3.19).

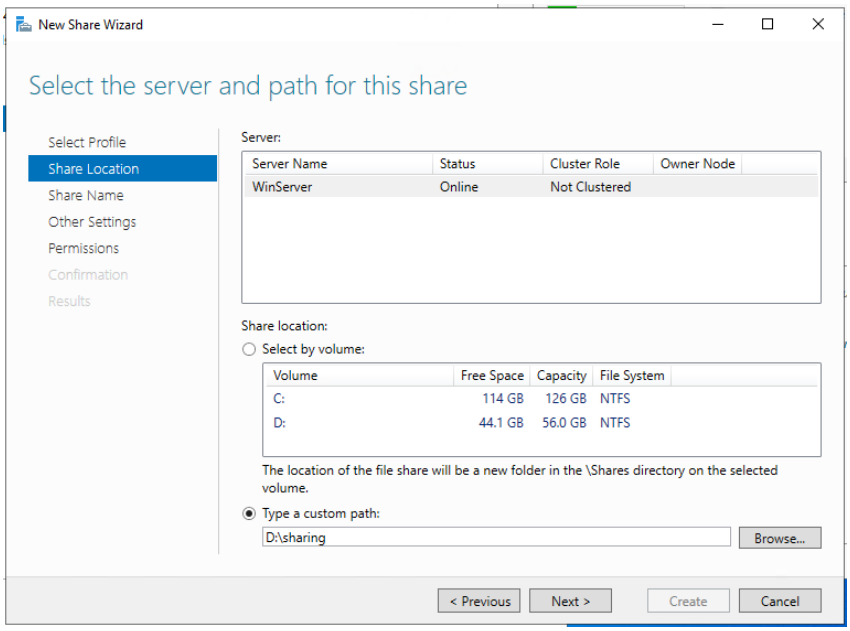

Рисунок 3.19 – Налаштування спільного доступу до директорії

У майстрі створення потрібно зазначити права доступу для облікових записів (рис. 3.20).

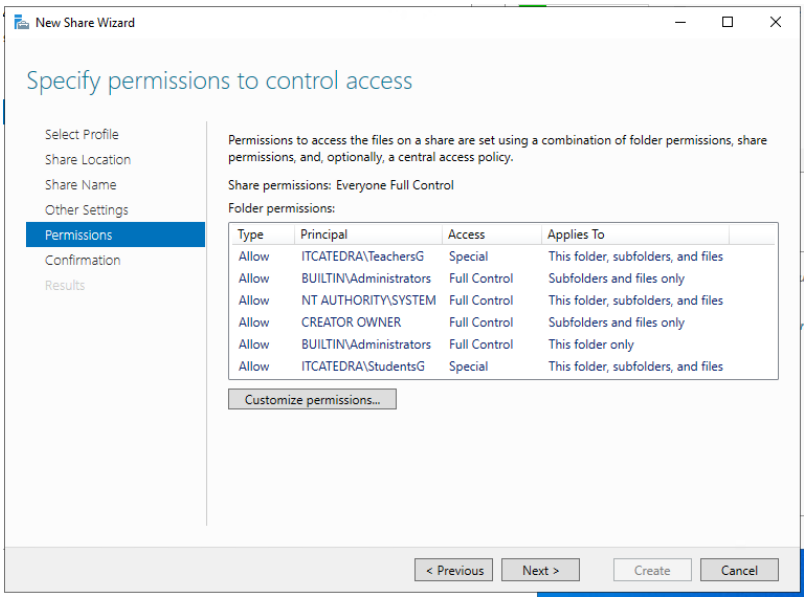

Рисунок 3.20 – Призначення прав доступу

Тепер для повноцінної роботи користувачів в системі, потрібно встановити сервіси віддаленого доступу.

Спочатку було обрано роль RDS і потрібні функції для роботи віддаленого доступу (рис. 3.21-3.22).

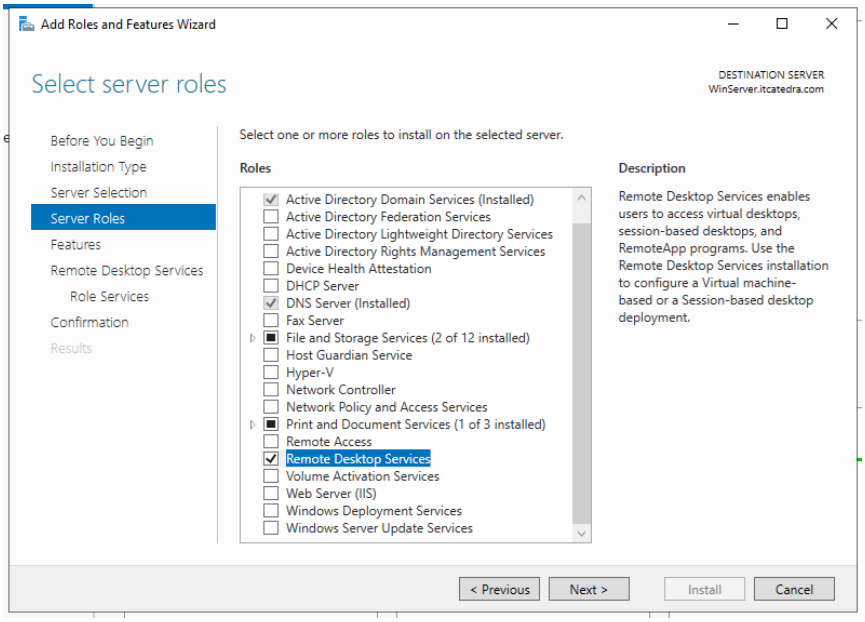

Рисунок 3.21 – Встановлення ролі RDS

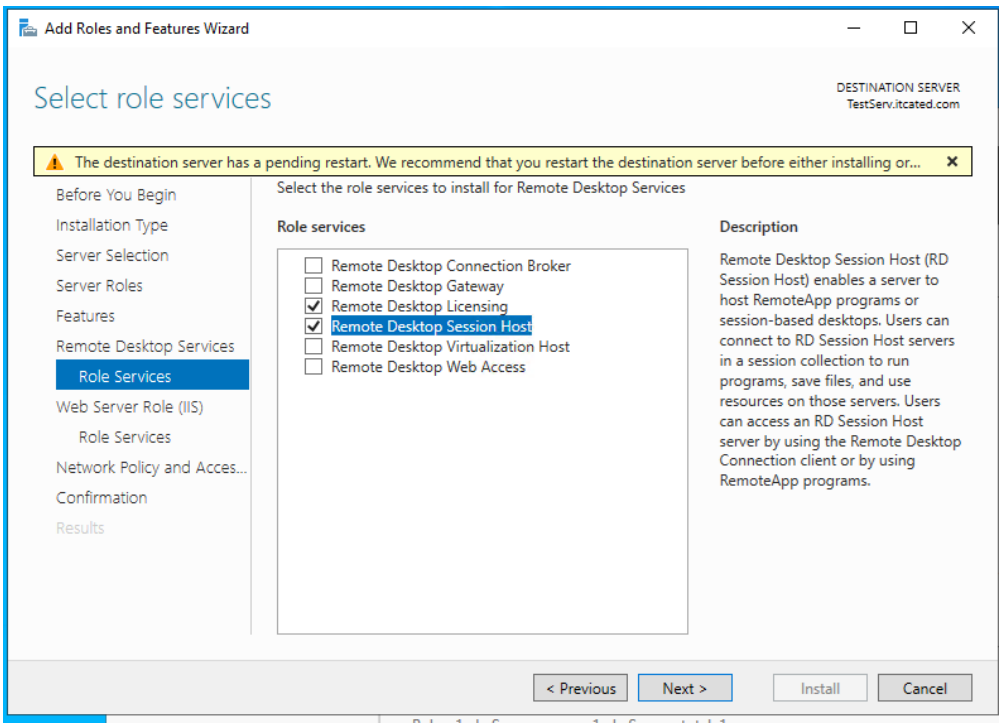

Рисунок 3.22 – Продовження встановлення ролі RDS

Після додавання ролі, встановлено сервіси віддаленого доступу, які в нових версіях Windows Server винесені в окремий пункт в майстрі вибору ролей (рис. 3.23).

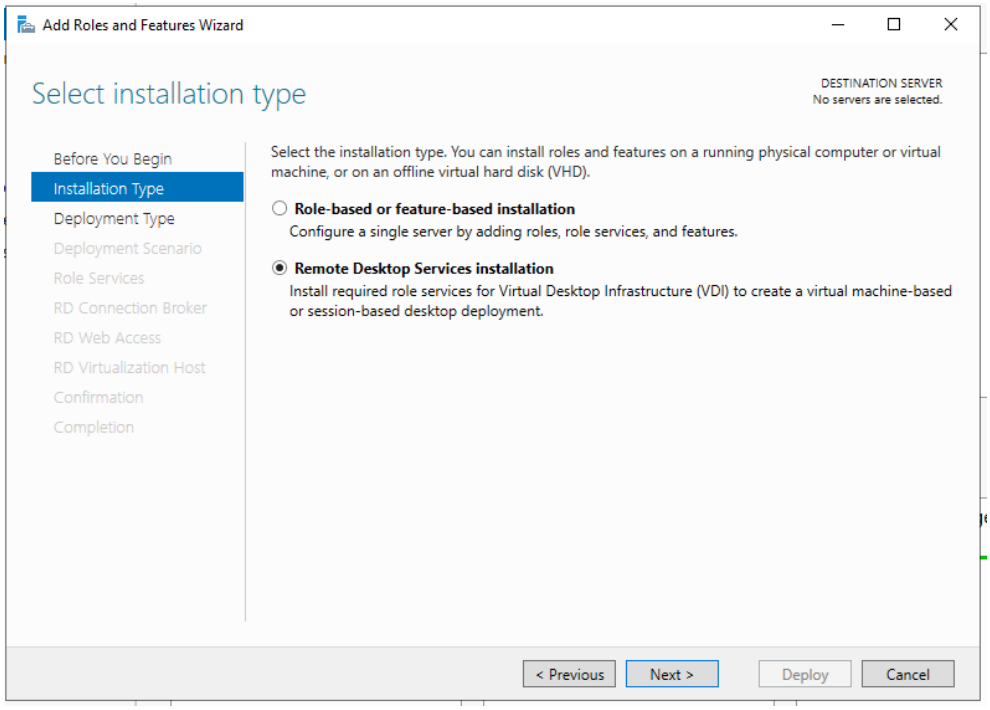

Рисунок 3.23 – Встановлення сервісів віддаленого доступу

У майстрі потрібно обрати сценарій розгортання віддалених робочих столів (рис. 3.24). Останні на основі сеансів будуються як одне централізоване віртуальне середовище, що розміщується на сервері. До нього підключаються користувачі через клієнт або веб-додаток. Сервер створює сеанс робочого столу для кожного облікового запису. Останній повинен мати доступ до одного віртуального середовища. Підключення працює на одному хостовому сервері, а користувачі мають доступ до спільної файлової системи.

Інфраструктура на основі віртуальних робочих столів створює окремий простір для кожного профілю, запускаючи їх на окремих VM. Це дає користувачам повністю ізольовані один від одного VM, кожен стіл має свою файлову систему та розподіл ресурсів.

У цьому варіанті реалізації віддаленого доступу був обраний варіант на основі сеансів.

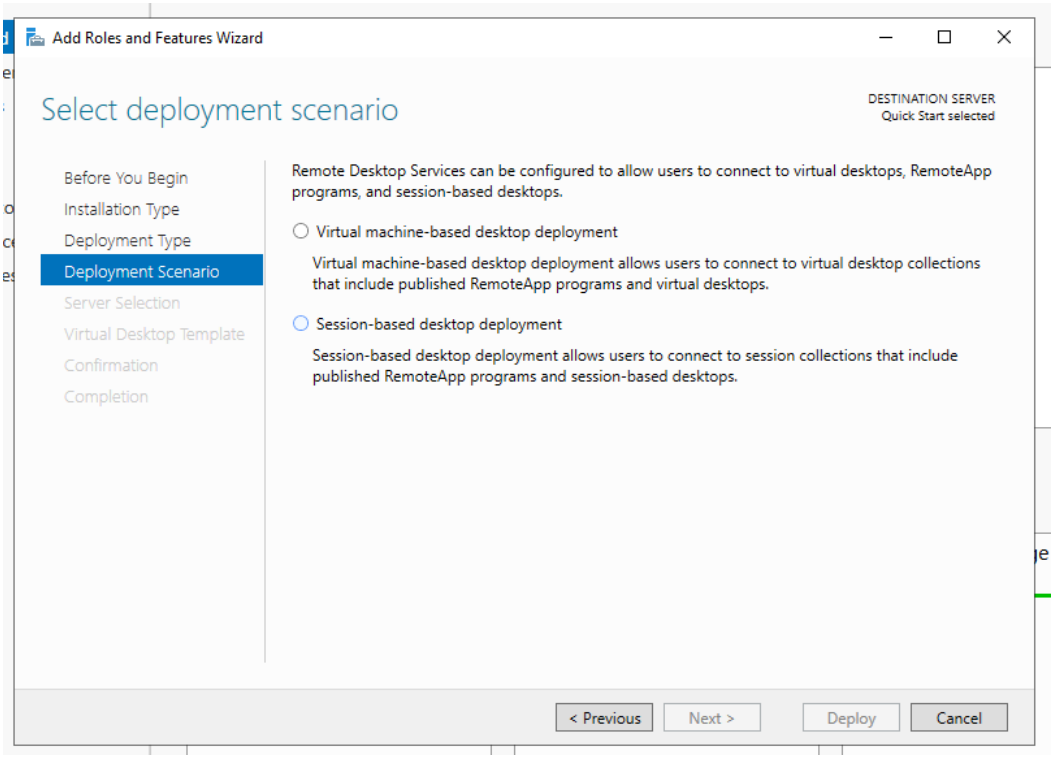

Рисунок 3.24 – Вибір сценарію розгортання RDS

Після встановлення всіх сервісів користувачі можуть підключатися до віддаленого робочого столу за протоколом RDP.

На цьому можна завершити першочергові налаштування системи. Подальші зміни в політиках треба вносити, виходячи з міркувань і формування вимог під час повноцінної експлуатації мережі.

Тепер проблема полягає в тому, щоб ввести локальну інфраструктуру в новостворений доменний ліс itcatedra.com. Оскільки по суті це дві різні географічно розділені мережі, було вирішено створити між ними VPN тунель. Останній шифрує трафік на одному кінці та відправляє його в іншу через загальнодоступний канал Інтернеті, де він розшифровується та направляється до місця призначення.

Було реалізовано варіант Site-To-Site VPN, це створює зашифроване з’єднання між двома VPN-шлюзами. Організовано постійний зв’язок між двома мережами, які будуть обмінюватися інформацією та ресурсами як в єдиному просторі [25]. Для організації тунелю зазвичай використовується спеціальне обладнання, як, наприклад, мережеві екрани та маршрутизатори компанії Cisco [26]. Схема роботи Site-To-Site VPN представлена на рисунку 3.26.

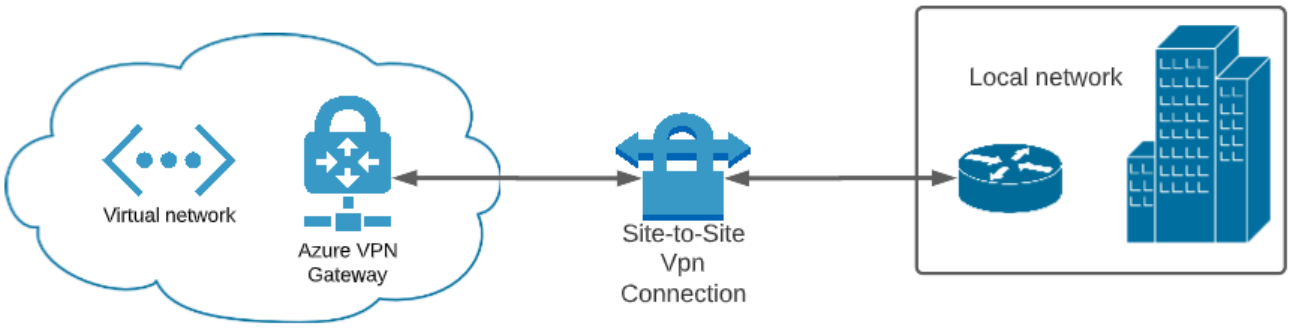

Рисунок 3.26 – Схема Site-To-Site VPN

На платформі Azure для створення з’єднання типу Site-To-Site VPN потрібно створити та налаштувати наступні ресурси:

– Virtual Network – віртуальна мережа; є основою для створення приватної мережі в Azure;

– Virtual Network Gateway – VPN-шлюз, який складається з декількох віртуальних машин, що розгортаються до певної підмережі; він містить в собі таблиці маршрутизації та запускає спеціальні служби шлюзу;

– Public IP Address – публічна адреса, по якій відбувається звернення до шлюзу;

– Local Network Gateway – спеціальний об’єкт, який представляє дані локальної мережі;

– Connection – спеціальний об’єкт, який виконує безпосереднє з’єднання між двома шлюзами.

Для підключення використовується вже раніше створена віртуальна мережа з діапазоном ip-адрес 10.0.0.0/16. Останній не повинен співпадати з тим, що використовується в on-premise мережі (рис. 3.27).

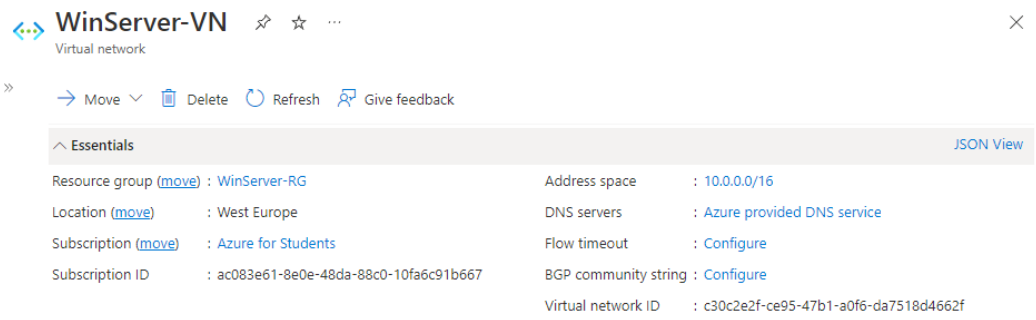

Рисунок 3.27– Віртуальна мережа

Для створення VPN-шлюзу був використаний спеціальний елемент. Потрібно вказати тип шлюзу. Також необхідно зазначити певну Vnet, де він буде використовуватися. Шлюз може бути лише один на мережу, але можна створити декілька з’єднань, що будуть направлені на нього В адресному просторі виділено окрему підмережу. Тут же зазначена публічна адреса, є можливість використати вже наявну, але була створена нова спеціально для шлюзу (рис. 3.28).

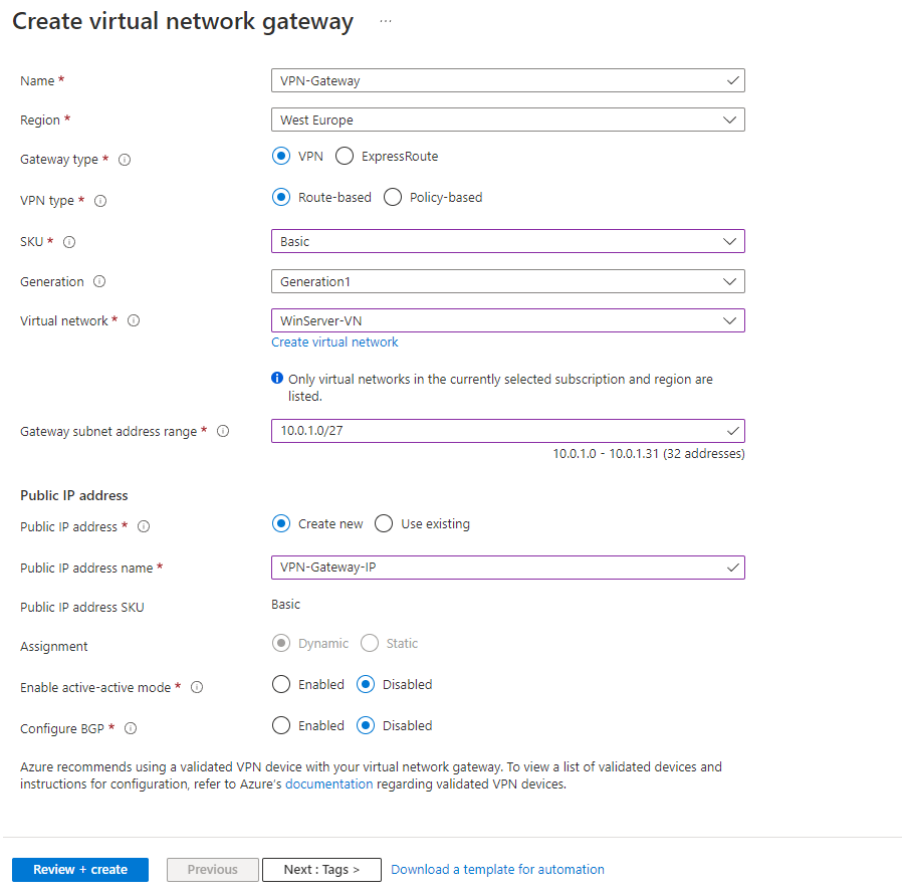

Рисунок 3.28 – Створення віртуального шлюзу

При додаванні об’єкту локального шлюзу вказана публічну адресу on-premise мережі. Для прикладу в проєкті вона зазначена як 1.2.3.4. Також указано простір ip-адрес та маску, яка використовується в локальній підмережі (рис. 3.29).

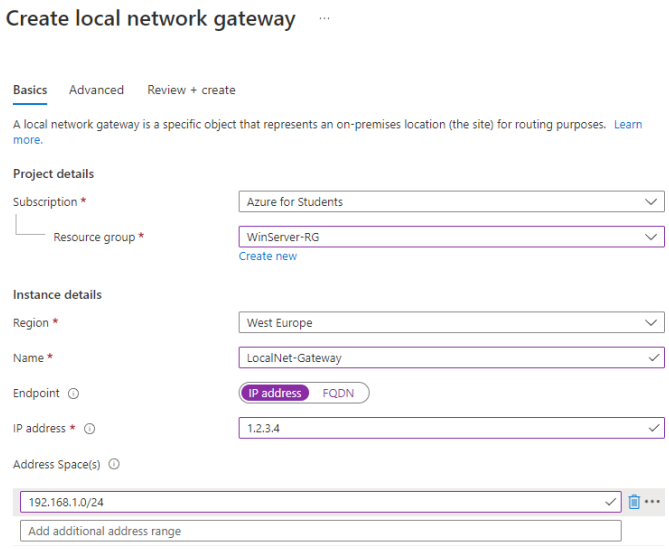

Рисунок 3.29 – Створення локального шлюзу

При створенні елементу з’єднання було вказано його тип, обрано шлюзи й віртуальну мережу. Також зазначено PSK ключ, він використовується для шифрування підключень (рис. 3.30). Однаковий ключ має бути вказаний як у віртуальному шлюзі, так і в шлюзі локальної мережі. Його може надавати локальний пристрій, або ж можна створити в Azure і потім застосувати його до on-premise шлюзу.

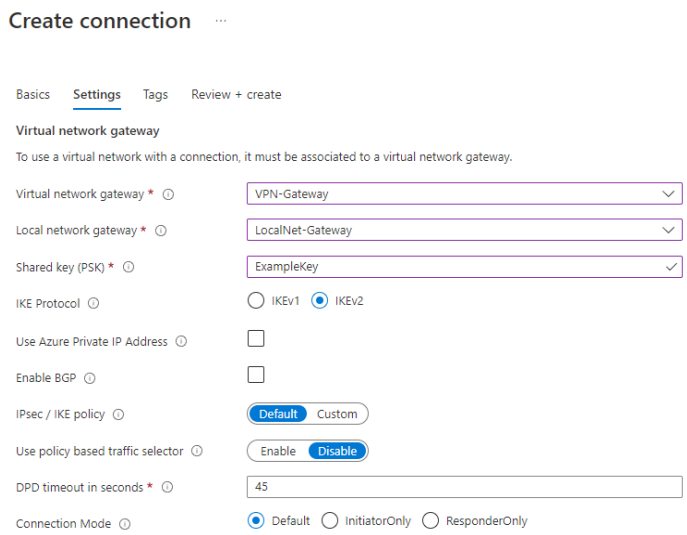

Рисунок 3.30 – Створення з’єднання між шлюзами

Наступним кроком є налаштування локального пристрою для створення VPN підключення. У роботі показано скрипт для систем Cisco IOS версії 15 і вище, як, наприклад, Cisco ISR 2911.

Параметри мережі є такими:

– Ім’я з’єднання: ITCatedra-S2S-Connection;

– Ім’я VPN шлюза: VPN-Gateway;

– Публічна ip-адреса: 13.80.74.71;

– Адресний простір віртуальної мережі: 10.0.0.0, префікс:10.0.0.0, мережева маска :255.255.0.0;

– Ім’я локального шлюза: LocalNet-Gateway;

– On-premises VPN IP: 1.2.3.4;

– Адресний простір локальної мережі: 192.168.1.0, префікс:192.168.1.0, мережева маска: 255.255.255.0;

– PSK ключ: ExampleKey.

Для налаштування систем CiscoIOS був створений спеціальний скрипт, він являє собою набір команд для конфігурації пристрою. Лістинг скрипта для налаштування для систем CiscoIOS надано в Додатку Г.

На цьому конфігурацію шлюзу завершено. Тепер потрібно включити парк машин в домен і можна вважати, що система налаштована й почати перевірку функціональності.

3.2 Інтеграція з сервісами Azure

Портал Azure дозволяє інтегрувати деякі сервіси з серверним рішенням, що підвищить гнучкість мережі. Із сервером будуть інтегровані: Azure Backup, Storage accounts, Azure Active Directory (AAD) та Azure Virtual Desktop (AVD).

Резервне копіювання даних є важливим. Його можна б було виконати засобами операційної системи, але в цьому проєкті воно зроблене через портал Azure. Для цього існує сервіс Backup Center, який дозволяє робити копії віртуальних машин, окремих дисків, баз даних та папок спільного доступу. Стратегія, яка пропонується для забезпечення відмостійкості системи та можливого відновлення після аварійних ситуацій, полягає в тому, щоб створити реплікацію інфраструктури до іншого регіону Azure. Усю ресурсну групу, тобто віртуальні машини, диски, папки спільного доступу, віртуальні мережі тощо, буде скопійовано до нової ресурсної групи, яка базується в датацентрі, який розташований іншій частині світу [27]. Схему роботи такої стратегії показано на рисунку 3.25.

Для резервного копіювання був використаний інструмент Site Recovery. Під час створення задачі потрібно вказати в якому регіоні базується ресурсна група. Потім обрати нову групу, що розташована в іншому місці світу, в яку буде здійснено копіювання ресурсів. У кінці необхідно зазначити тип копії, час її створення та машину, до якої це застосовано (рис. 3.26-3.27).

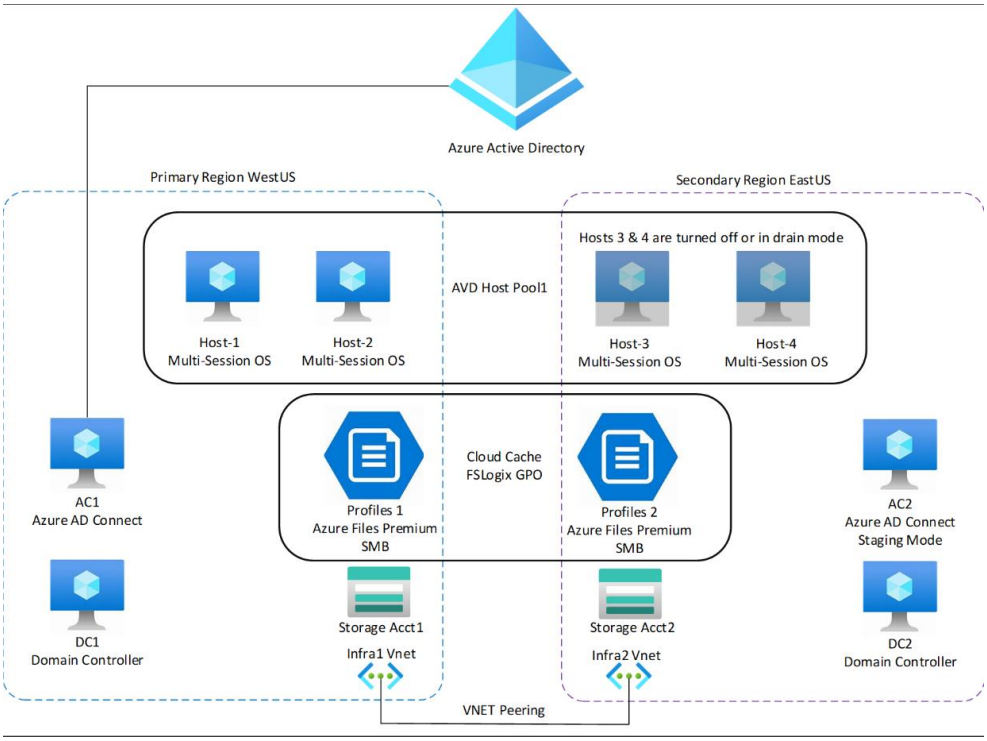

Рисунок 3.25 – Схема роботи стратегії реплікації

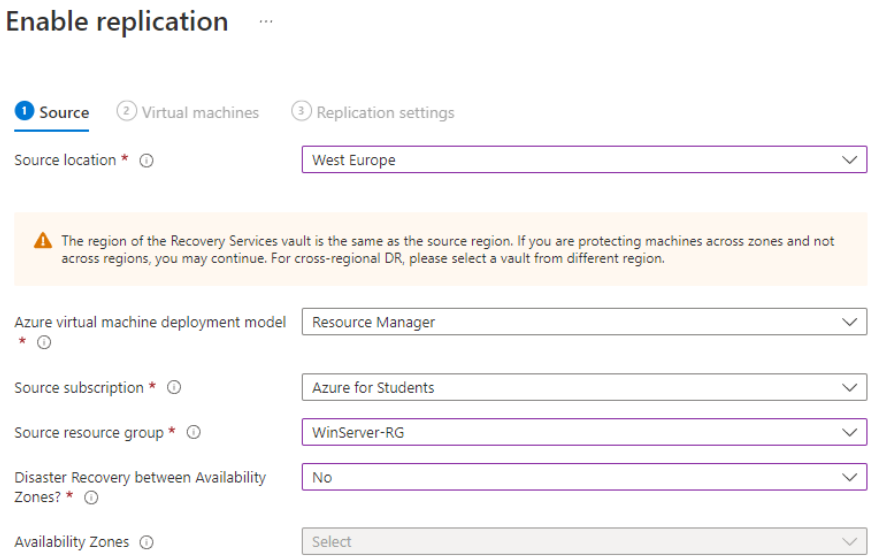

Рисунок 3.26 – Створення реплікації для пулу машин

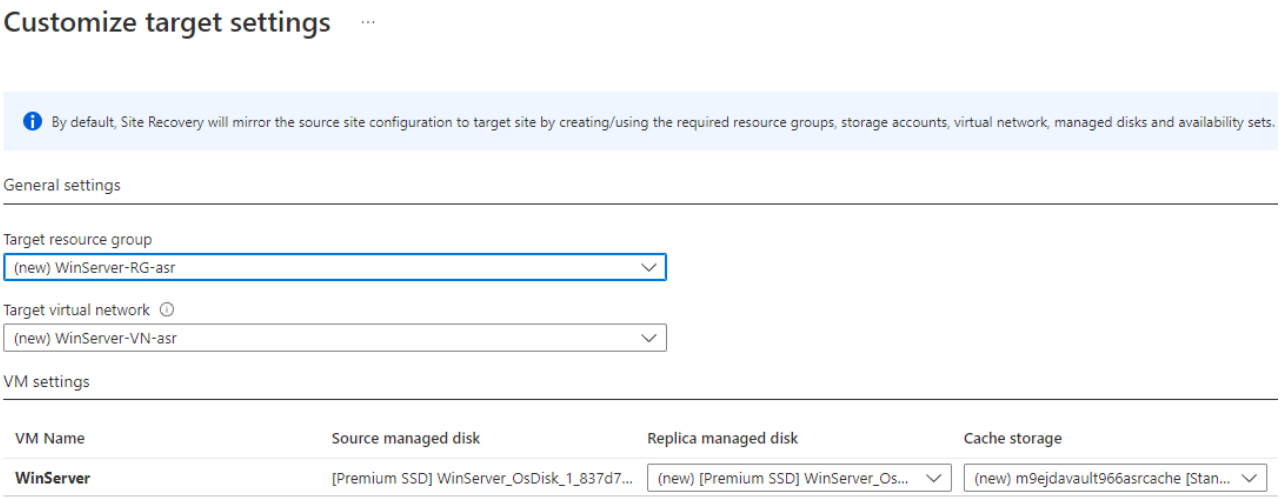

Рисунок 3.27 – Налаштування ресурсів реплакації

Наступним кроком є синхронізація Active Directory з Azure Active Directory (AAD) – це хмарна служба ідентифікації та керування доступом користувачів до різноманітних сервісів Azure та Office365. Синхронізація робиться за допомогою спеціальної утиліти, яка встановлюється на Windows Server [28]. На рисунку 3.28 показані користувачі, які зареєстровані в домені AAD до синхронізації.

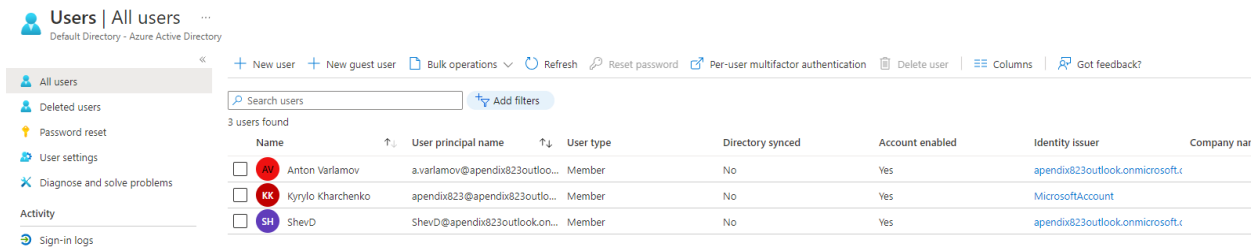

Рисунок 3.28 – Користувачі AAD до синхронізації

Після запуску утиліти AD Connect потрібно вказати профіль AAD з правами глобального адміністратора та вказати його пароль. Потім обрати ліс, який буде синхронізуватися з хмарою. Усі інші параметри залишити за замовчуванням (рис. 3.29-3.30).

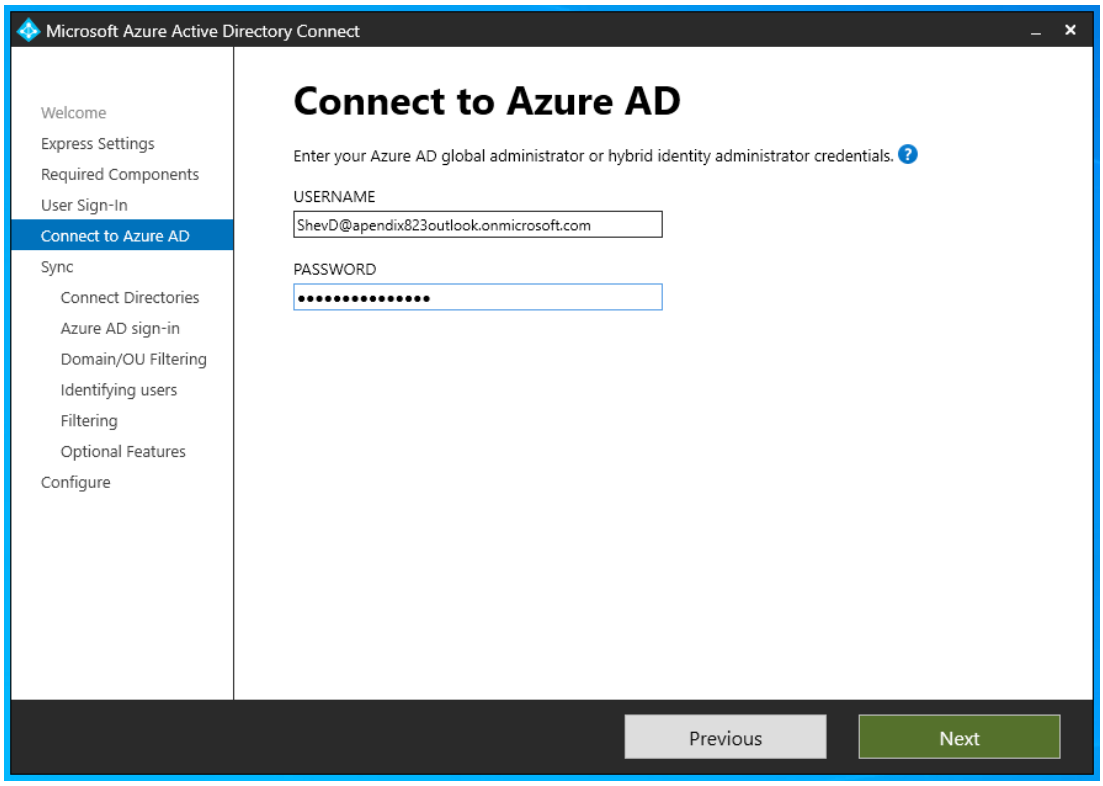

Рисунок 3.29 – AD Connect авторизація

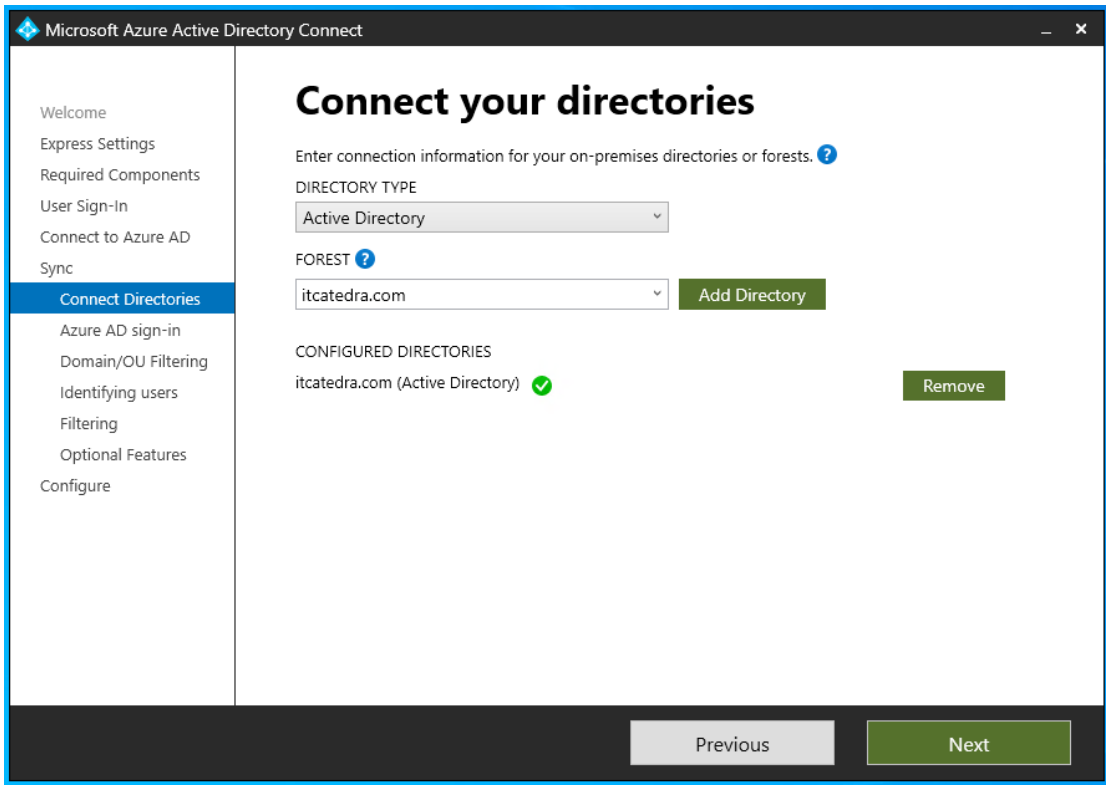

Рисунок 3.30 – AD Connect вибір лісу

Після синхронізації до AAD були додані нові користувачі та групи користувачів. Тепер ці профілі можна використовувати для авторизації в сервісах Azure (рис. 3.31).

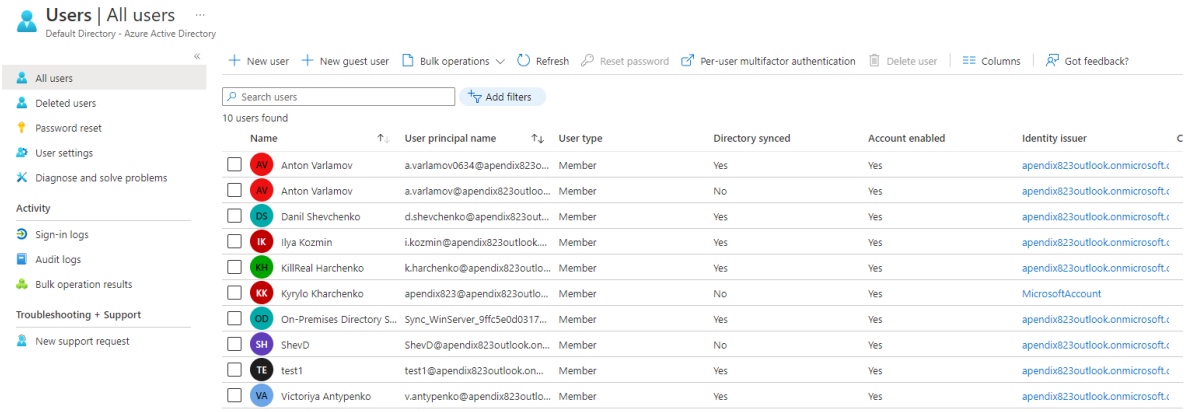

Рисунок 3.31 – Користувачі AAD після синхронізації

Наступним сервісом є Storage accounts. Він дозволяє створювати виділені директорії, які можуть бути підключені до машини у вигляді мережевого диску. Для серверу була створена директорія зі спільним доступом (рис. 3.32). Для включення її у файлову систему віртуальних машин потрібно виконати скрипт, який буде монтувати директорію як окремий мережевий диск [29].

Лістинг скрипта для монтування директорії надано в Додатку Д.

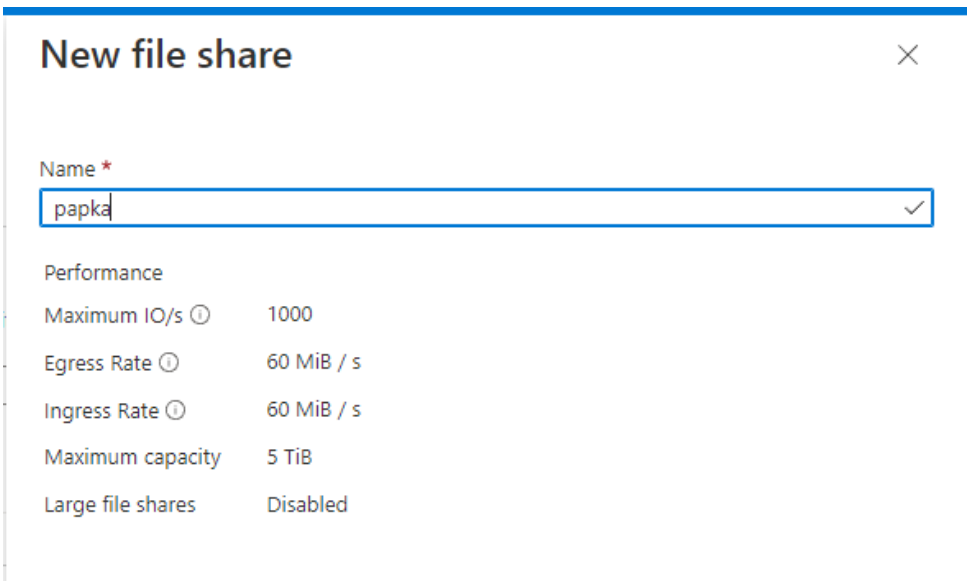

Рисунок 3.32 – Створення директорії для спільного доступу

Наступним для інтеграції є сервіс Azure Virtual Desktop. Його застосовують для віртуалізації робочого стола та виділених програм. Azure Virtual Desktop повністю працює в хмарі. Він забезпечує багатосеансовий доступ до робочого столу, але при тому залишає персональне робоче середовище. Сервіс дозволяє розгорнути як середовище робочого столу, так і окремі програми, які будуть запускатися на тих же машинах. Ця технологія доволі нова. Її анонс відбувся у 2018 році, а в публічний доступ сервіс потрапив у 2019. Тому варто мати на увазі, що зараз все ще йде період активного розвитку й компанія Microsoft продовжує впровадження нових інструментів управління, як, наприклад, рішення FSLogix та інтеграція з сервісами VMware та Citrix. У мережі даний сервіс використовується саме для запуску виділених застосунків. Це може бути корисно, коли апаратної потужності віртуальної машини, на якій базується Windows Server, не вистачить для запуску того чи іншого сценарію. У такому випадку на базі AVD можна буде додати більш підходящу під задачі машину й на ній виконати специфічну роботу [30].

Для функціонування сервісу AVD потрібна розгорнута інфраструктура в Azure. Базова версія AAD за замовчуванням створюється для користувачів платформи.

Далі було розгорнуто Azure Active Directory Domain Services (AADDS). Це сервіс доменів, який надає служби управління, та можливість обробки протоколів LDAP та Kerberos/NTLM, які використовувалися в локальних рішеннях і не були інтегровані в AAD. Для роботи AVD потрібно синхронізувати даний сервіс з AAD, щоб був зв’язок із доменом служб AADDS. Можна сказати ця служба виступає аналогом контролеру домена. Схематично принцип роботи сервісу показано на рисунку 3.33. Розгортаючи AADDS, його треба синхронізувати з AAD, а потім вже, конфігуруючи VDI, налаштовувати систему.

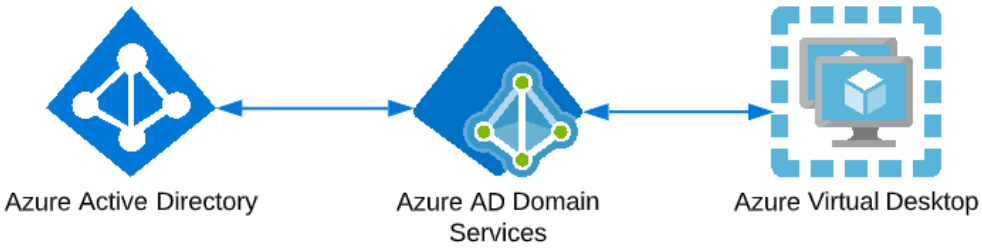

Рисунок 3.33 – Схема взаємодії AVD та AAD

Якщо ж є власна AD, то схема отримує доповнення, які показані на рисунку 3.34. Тобто локальна AD через спеціальний інструмент AD Connect синхронізується з хмарною.

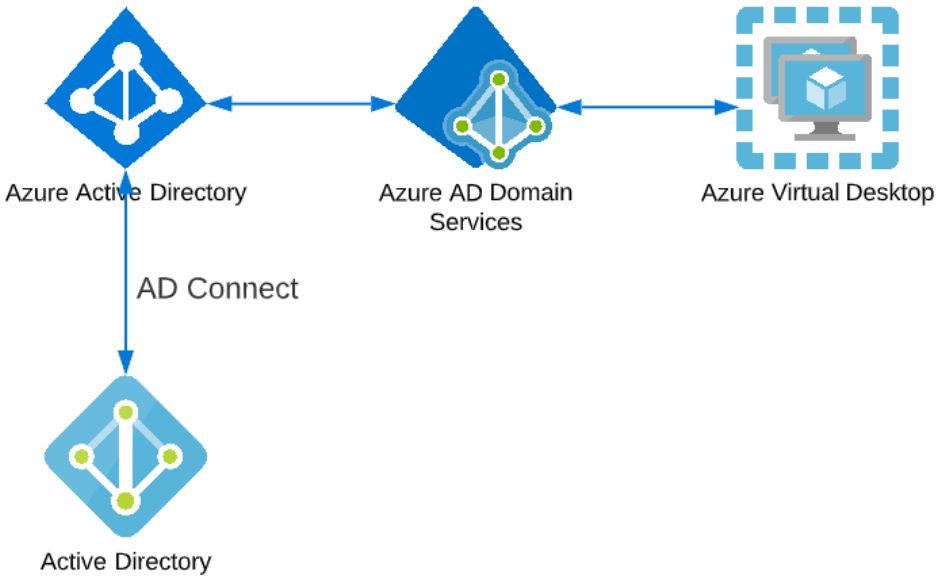

Рисунок 3.34 – Схема взаємодії AVD з локальною AD

Створення сервісу AVD схоже на інші. Було вказано ресурсну групу, тип AD яка буде використовуватися, зазначено VNet, до якої будуть відноситися створені VM, обрано образ ОС та апаратні характеристики.

Важливим параметром можна виділити тип створених хотів. Це саме та перевага, яку надає AVD. Можна обрати personal і тоді на одного користувача буде виділятися одне середовище, а отже, й одна VM. Також є варіант pooled. Він дозволяє

одночасне підключення до віртуальної машини декількох облікових записів. Тут також можна вказати й кількість одночасних сесій, але кожен користувач зберігає своє унікальне робоче оточення (рис. 3.35).

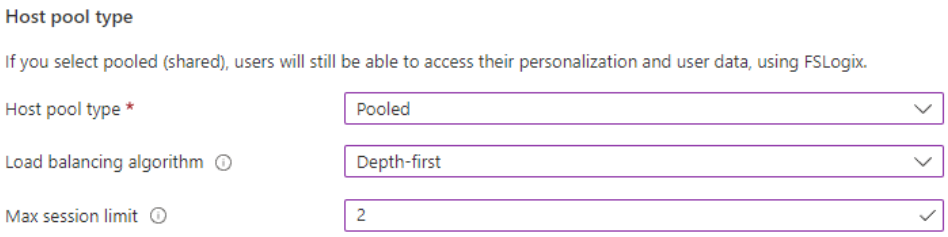

Рисунок 3.35 – Створення пулу віртуальних машин AVD

Створення профілів відбувається через службу AAD, але для коректної авторизації новоствореним обліковим записам потрібно в панелі управління ресурсною групою надати спеціальні ролі Virtual Machine Administrator Login та Virtual Machine User Login. Без цих ролей користувач зможе зайти в панель керування доступними йому сеансами, але під час з'єднання з віртуальною машиною отримає відмову у доступі. Також профілі були додані в меню Assignments у панелі управління групами застосунків сервісу AVD (рис. 3.36).

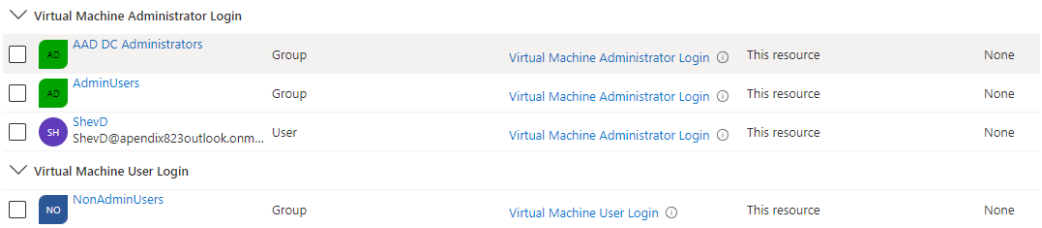

Рисунок 3.36 – Призначені ролі користувачів

За замовчуванням у AVD створюється одна така, в ній знаходиться сесія віддаленого робочого столу. Можна додати ще одну групу, в яку помістити окремі програми встановлені у середовищі, як приклад браузер або текстовий редактор (рис. 3.37). Тут же є можливість не просто обирати з наявних програм, але й встановити MSIX пакет, який треба створити та додати до спеціального розділу у меню Host

pools. Та слід мати на увазі, що зараз для нормального розгортання й управління пакетами MSIX потрібно на кожну машину встановити пакет інструментів FSLogix.

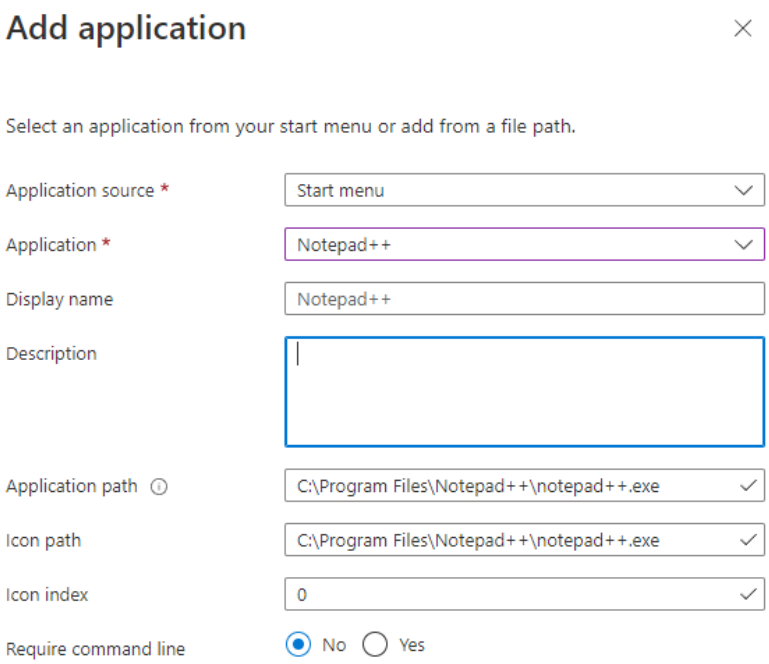

Рисунок 3.37 – Створення сеансу для окремого застосунку

Також для створеної групи хостів зроблений план масштабування, в якому зазначено розклад та умови, за яких буде відбуватися автоматичне розгортання віртуальних машин. У розкладі потрібно вказати час старту, пікового навантаження та завершення роботи, у спеціальних умовах при якому відсотку від спільного ресурсу потрібно підключати нові машини (рис. 3.38-3.40).

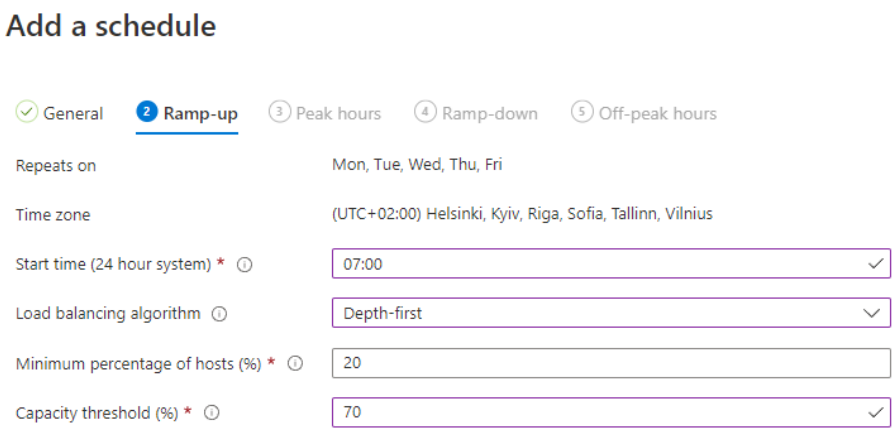

Рисунок 3.38 – Налаштування включення машин

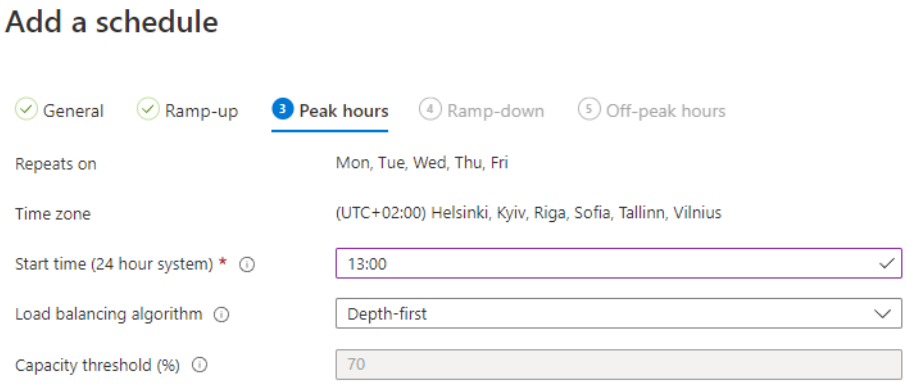

Рисунок 3.39 – Налаштування роботи в час пікового навантаження

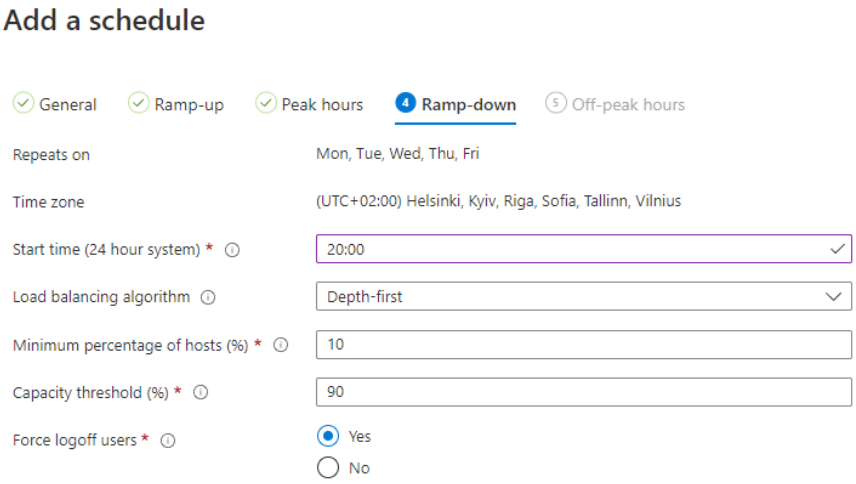

Рисунок 3.40 – Налаштування вимкнення машин

3.3 Демонстрація роботи мережі на основі Windows Server

Для підключення до віддаленого робочого столу користувачу треба скористуватися застосунком, який дозволить підключення через протокол RDP. У системі Windows такий встановлений за замовчуванням. Користувач повинен указати публічну IP адресу серверу й дані від власного профілю (рис. 3.41).

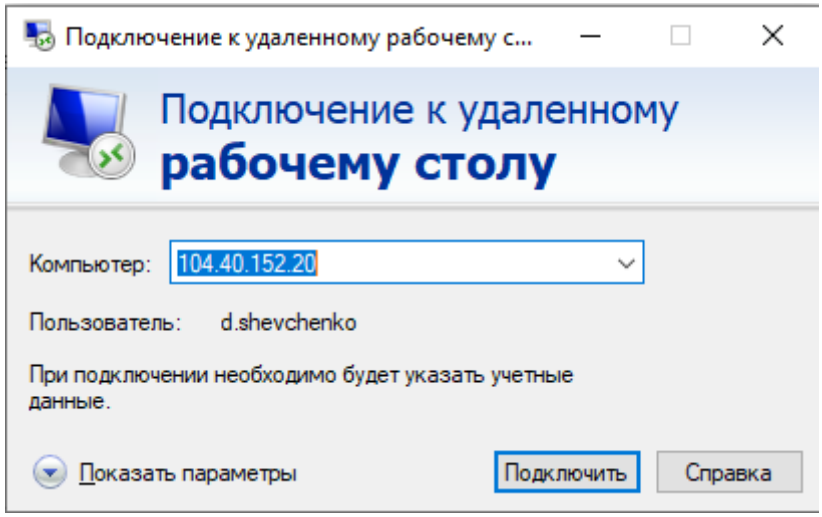

Рисунок 3.41 – Підключення за протоколом RDP

Після входу в систему, юзеру є доступним звичний робочий стіл. Є можливість запускати встановлені програми через ярлики, які адміністратор може винести на робочий стіл. Також користуватися доступними йому директоріями й у цілому працювати так само, як і за локальним комп'ютером. На рисунках 3.42 і 3.43 можна відмітити, що користувач знаходиться в домені itcatedra.com, який було створено на віртуальному сервері.

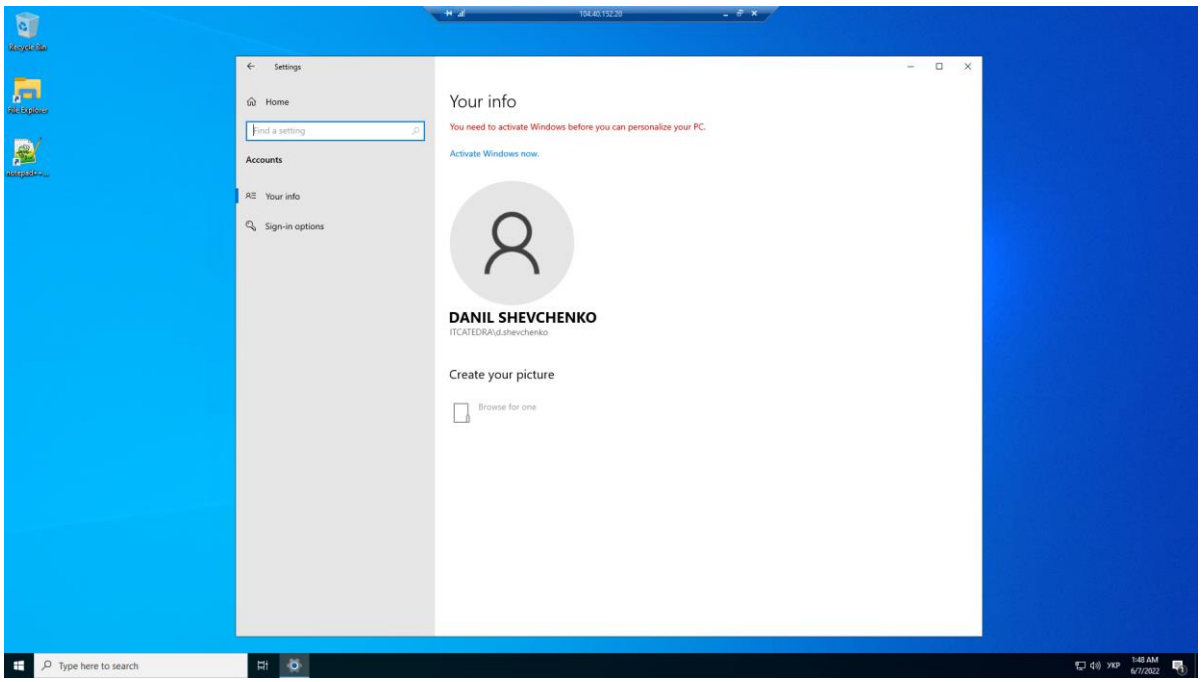

Рисунок 3.42 – Робочий стіл користувача

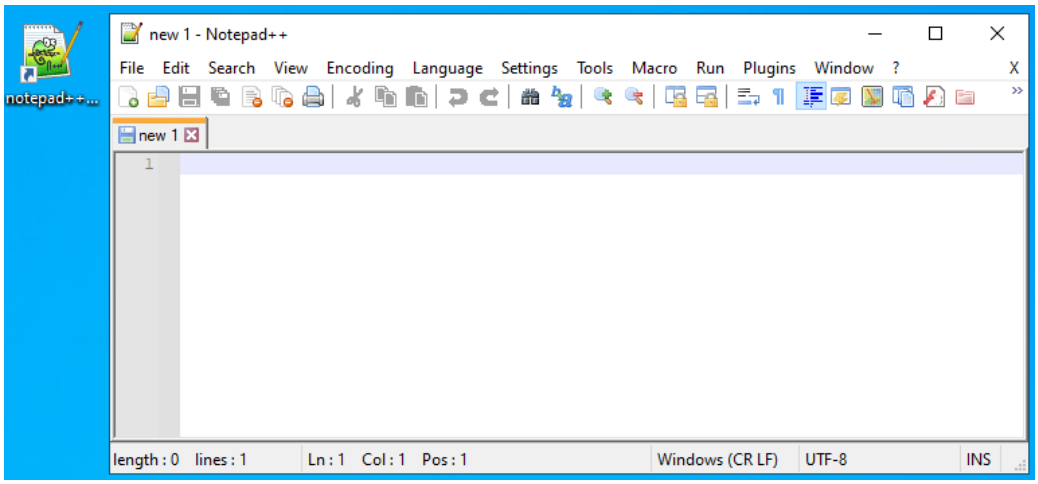

Рисунок 3.43 – Запущена програма

У файловому менеджері розташовані доступні й видимі для користувача диски та змонтовані папки. Директорія Personal створюється автоматично для кожного облікового запису й не обмежує його в правах. У ній він може зберігати власні файли. Shader Folder спільна для всіх і також не накладає обмежень на запис чи зміну файлів. У директорії Education Materials для користувачів із рівнем доступу студента встановлений дозвіл лише на перегляд, читання та виконання файлів. Профілі, які відносяться до групи викладачів, мають дозвіл на створення, видалення та редагування файлів та директорій (рис. 3.44-3.46).

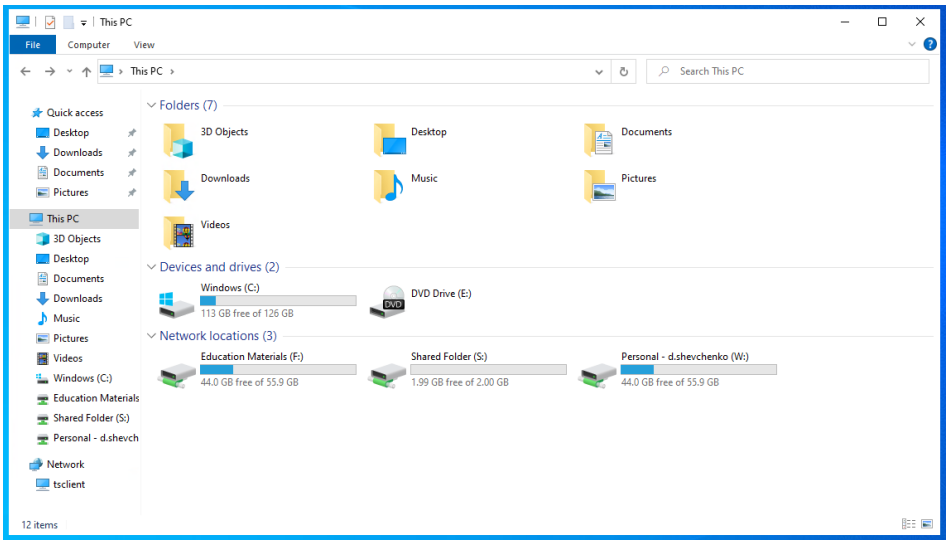

Рисунок 3.44 – Файловий менеджер

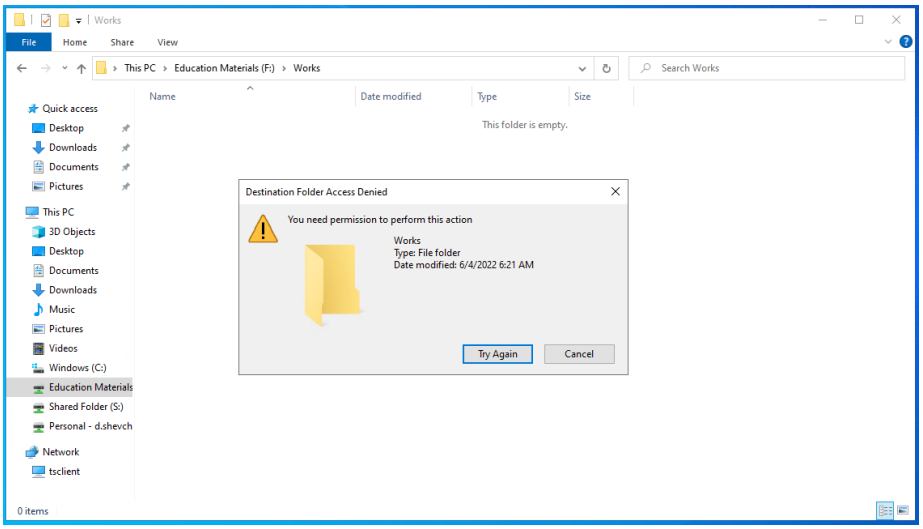

Рисунок 3.45 – Заборона на створення файлів та директорій для студента

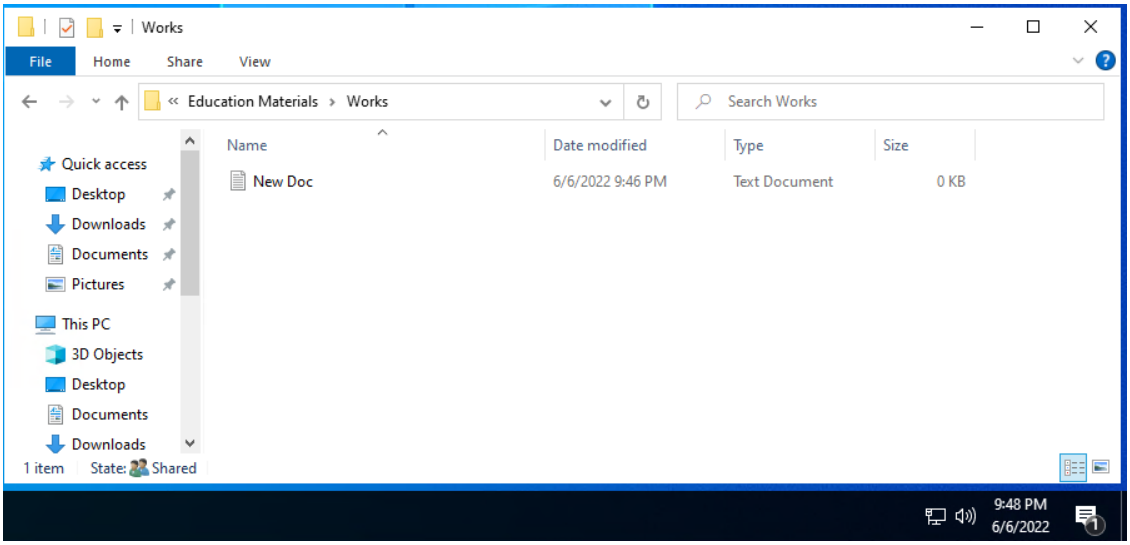

Рисунок 3.46 – Створений файл під профілем викладача

Як студентам, так і викладачам заборонено встановлювати будь-які програми. До цього також відносяться й фізичні носії з виконуваними файлами, або ж на яких може бути встановлений образ з автоматичним запуском (рис. 3.47). Також заборонено виклик команди «Виконати», яка може бути запущена комбінацією win+R (рис. 3.48).

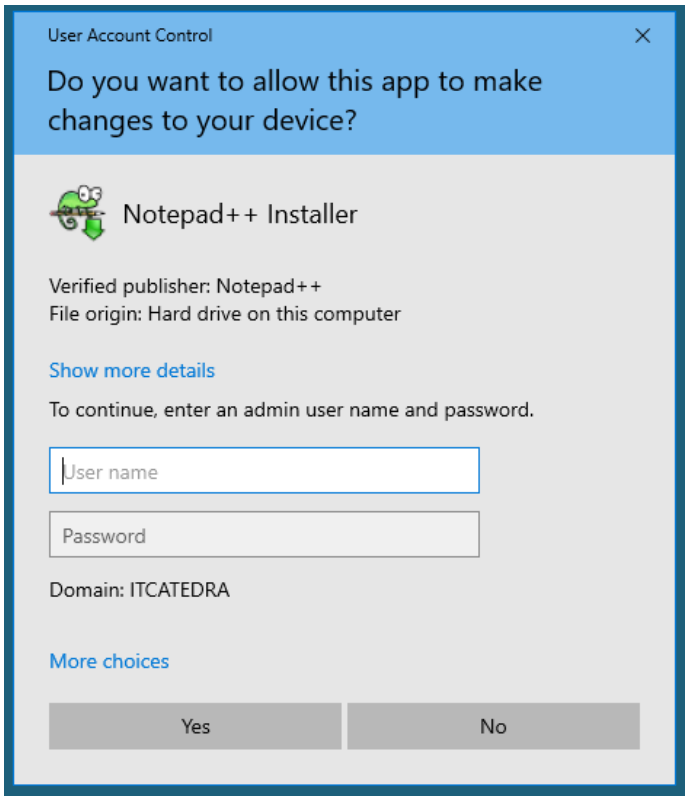

Рисунок 3.47 – Заборона на встановлення застосунків

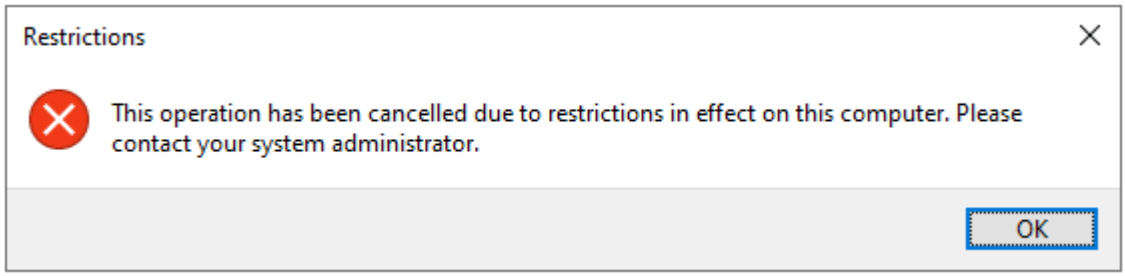

Рисунок 3.48 – Заборона команди «Виконати»

Після авторизації у якості адміністратора, користувач побачить менеджер із інформацією про локальний сервер. Цей інструмент дозволяє централізовано контролювати роботу виконуваних ролей. Тут відображений статус роботи встановлених сервісів. Також можуть бути доступними повідомлення про деякі збої в роботі. Через цю утиліту відбувається встановлення нових ролей або ж видалення вже наявних (рис. 3.49).

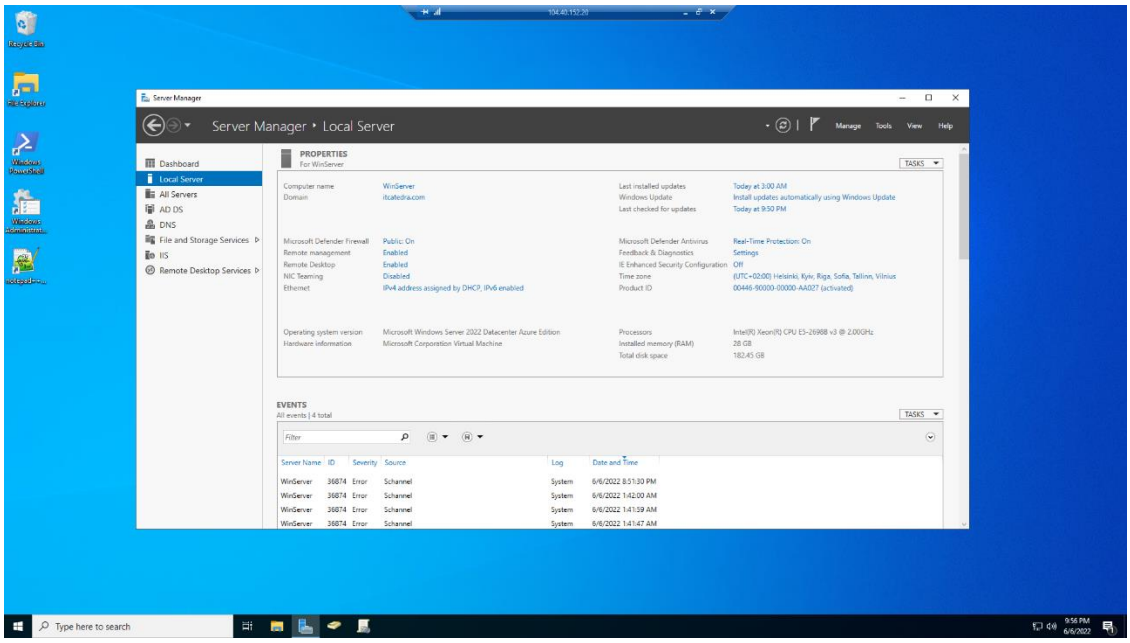

Рисунок 3.49 – Робочий стіл адміністратора

Також у даній утиліті можна переглянути всі папки та диски з загальним доступом, призначити або відкоригувати їх квоти або ж перейти до меню NTFS дозволів для управління файловою системою (рис. 3.50). Саме через меню редагування прав доступу адміністратор має визначити, що саме, група користувачів зможе робити з директоріями та вкладеними в них файлами (рис. 3.51).

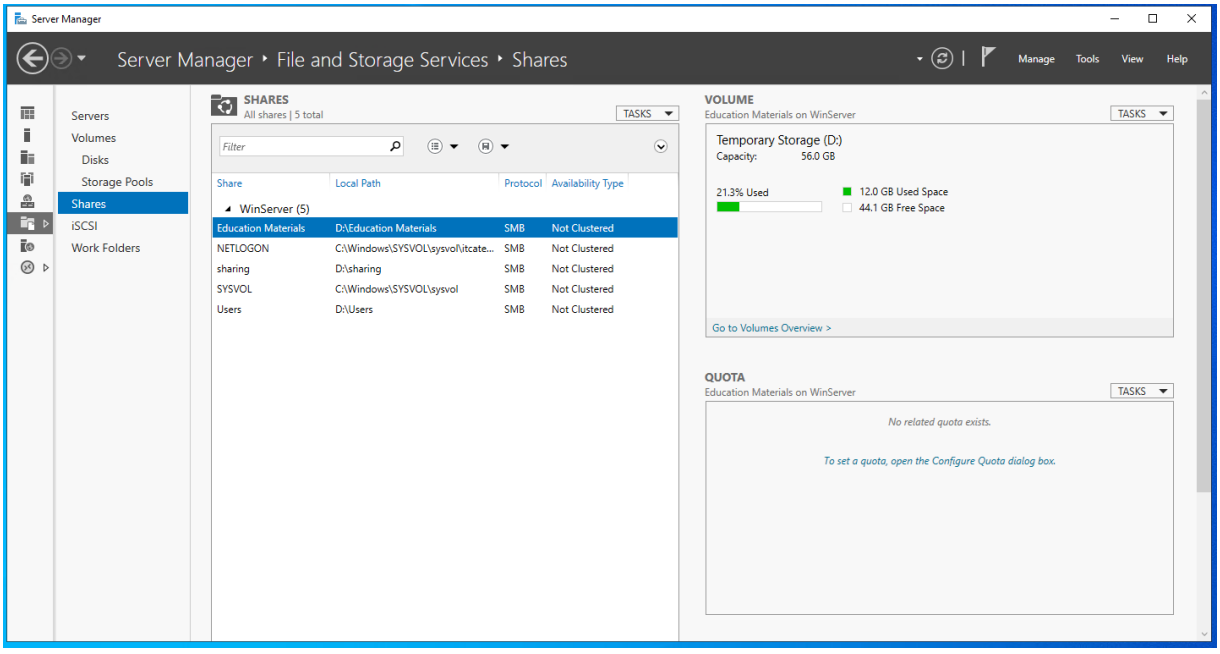

Рисунок 3.50 – Менеджер управління ресурсами зі спільним доступом

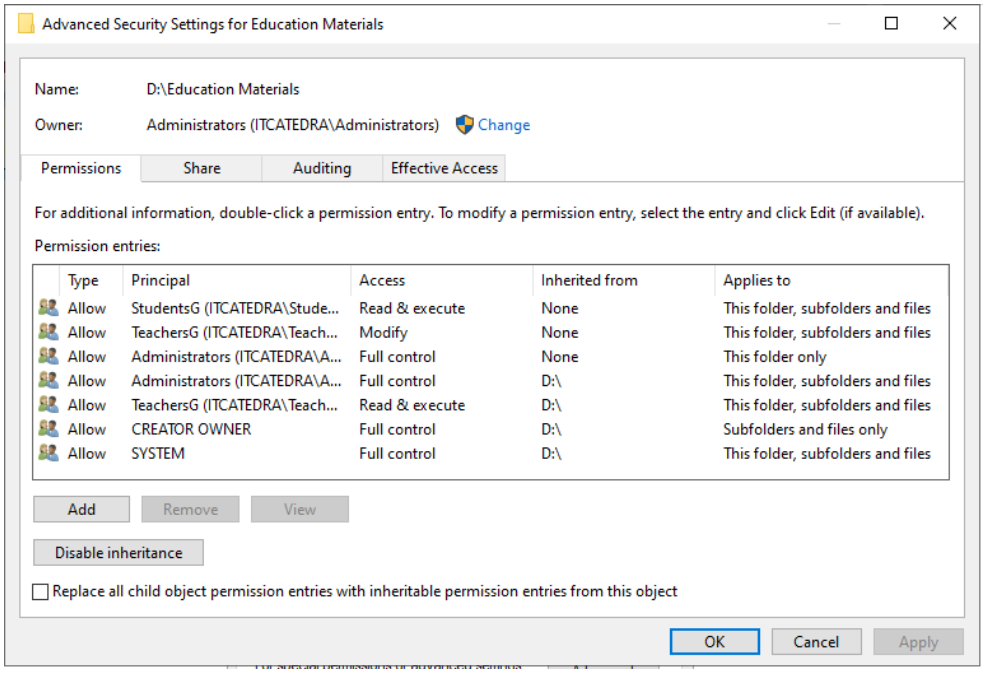

Рисунок 3.51 – Менеджер управління правами доступу

У домені були створені 4 профілі для студентів та 1 для викладача. Усі вони розподілені по окремим OU та є членами груп для простішого застосування дозволів файлової системи та ін. (рис. 3.52). Також для кожного користувача, який хоча б один раз увійшов в систему, була створена окрема директорія (рис. 3.53).

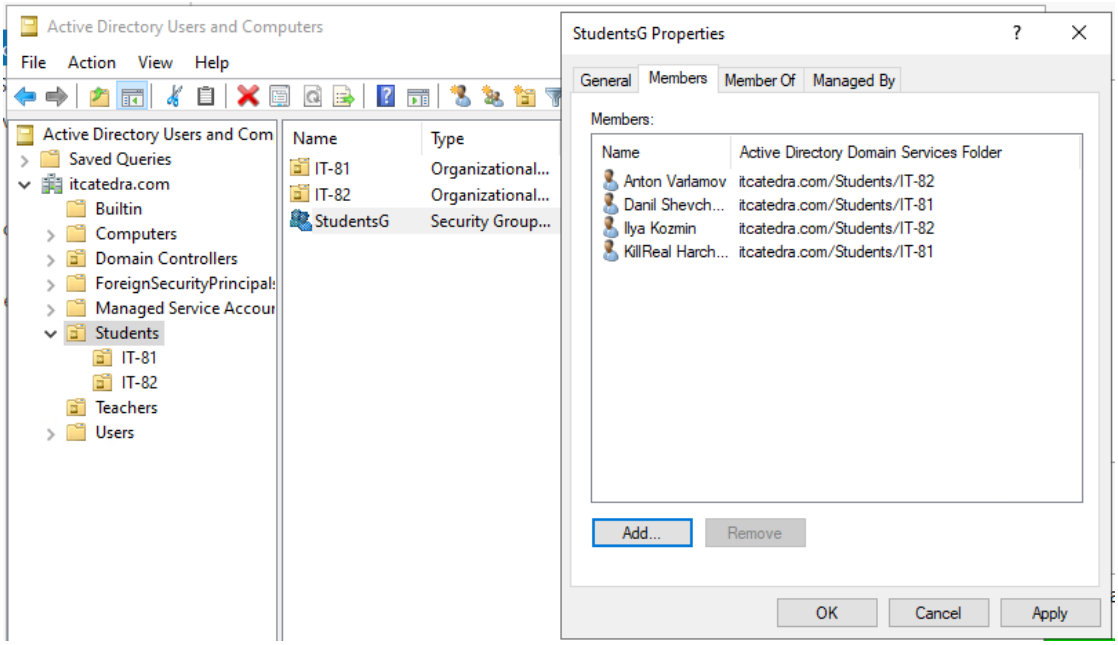

Рисунок 3.52 – Створені профілі користувачів

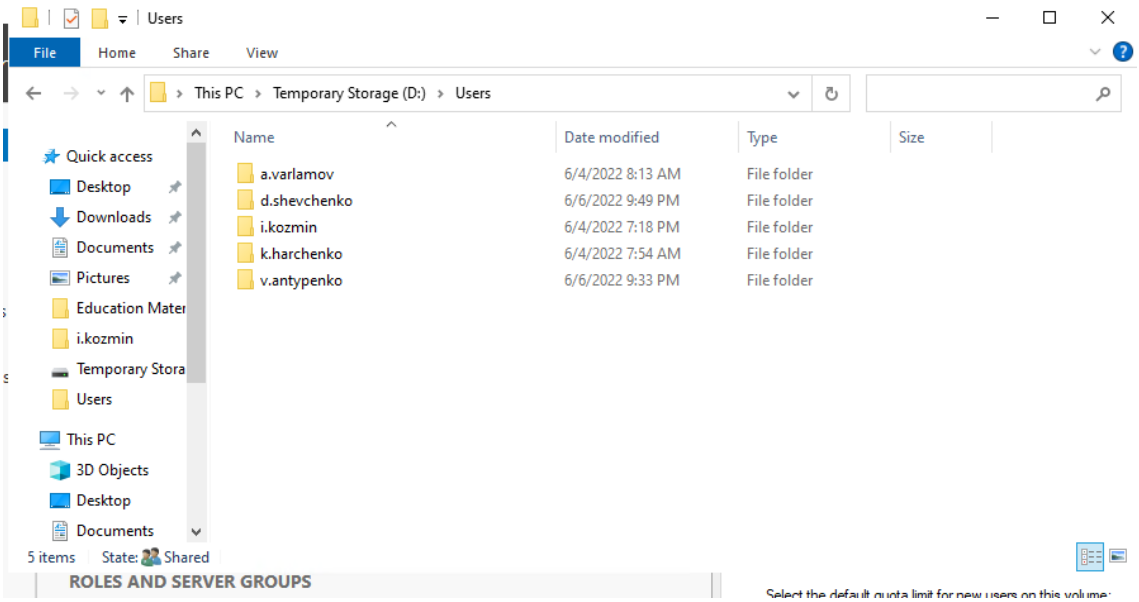

Рисунок 3.53 – Створені індивідуальні директорії

Для студентів та викладачів були створені дві окремі групові політики, які обмежують деякі їх можливості (рис. 3.54-3.55).

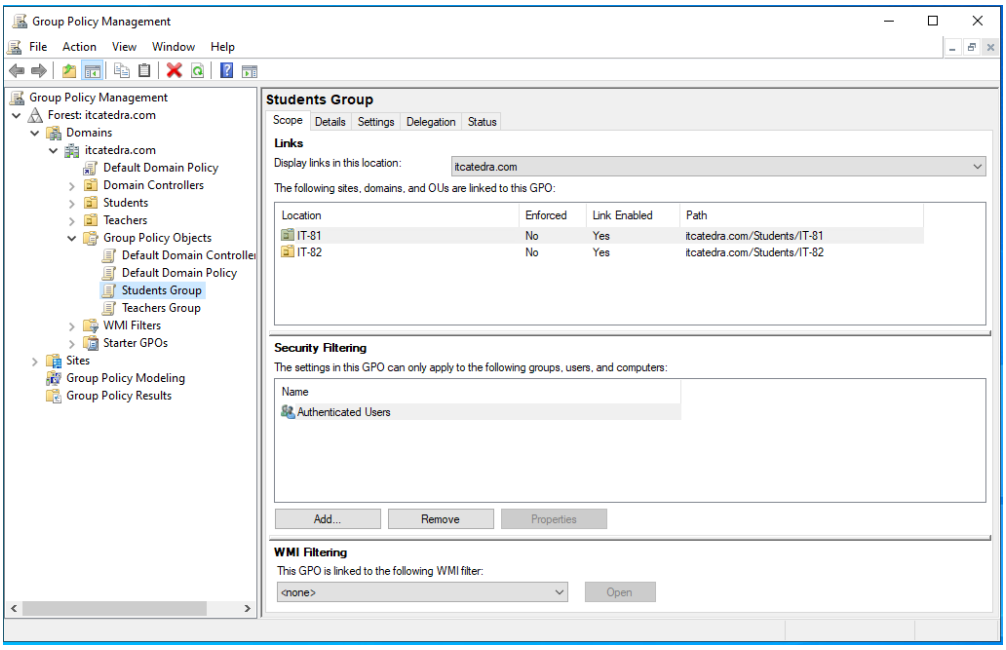

Рисунок 3.54 – Менеджер управління груповими політиками

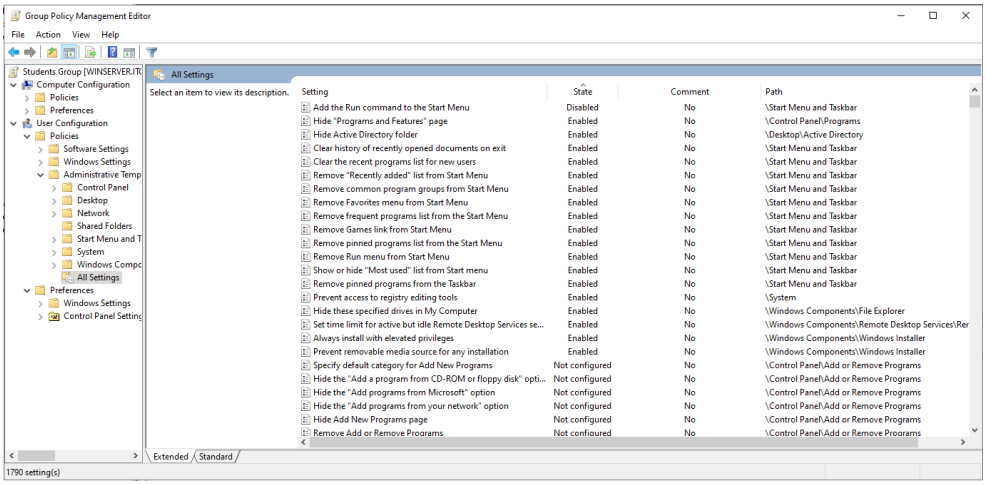

Рисунок 3.55 – Змінені політики

Для імітації тунелю Site-to-Site VPN було створену ще одну VNet з VM під управлінням операційної системи Windows 11. Налаштування підключення між двома віртуальними машинами майже нічим не відрізняється від Site-to-Site, просто в типі підключення потрібно обрати VNet-to-VNet (рис. 3.56).

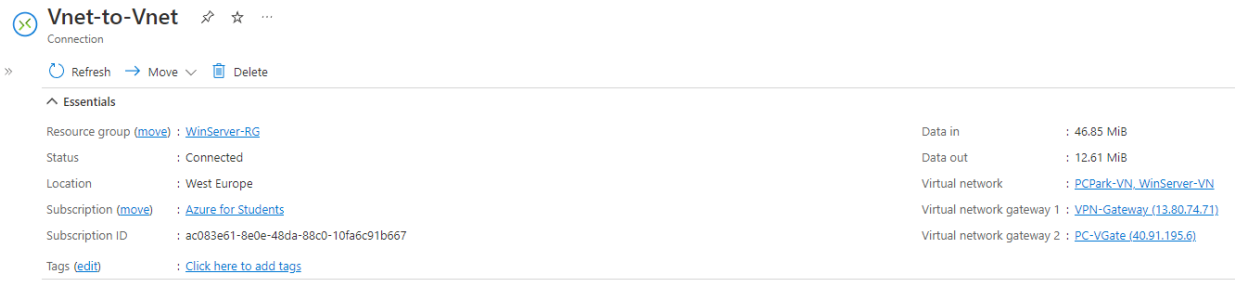

Рисунок 3.56 – Мережа для з’єднання VNet-to-VNet

Для вводу комп’ютера в домен потрібно зайти у властивості системи та знайти пункт вибору домену або робочої групи (рис. 3.57). У строфі вводу потрібно вказати адресу домену, а саме itcatedra.com, і після цього повинно стати доступним меню запиту даних адміністратора домену. Якщо логін та пароль були введені вірно, комп’ютер буде додано в домен (рис. 3.58). Може виникнути помилка через те, що DNS сервер, до якого звертається комп’ютер, не містить запису про таке доменне ім’я. Для вирішення даної проблеми достатньо вказати адресу серверу, так як на ньому налаштована роль DNS й він сам видає інформацію про власні налаштування.

Уведений в домен комп’ютер буде керуватися контролером із серверу й отримає автоматичні налаштування та політики для тих користувачів, які авторизуються за своїми профілями.

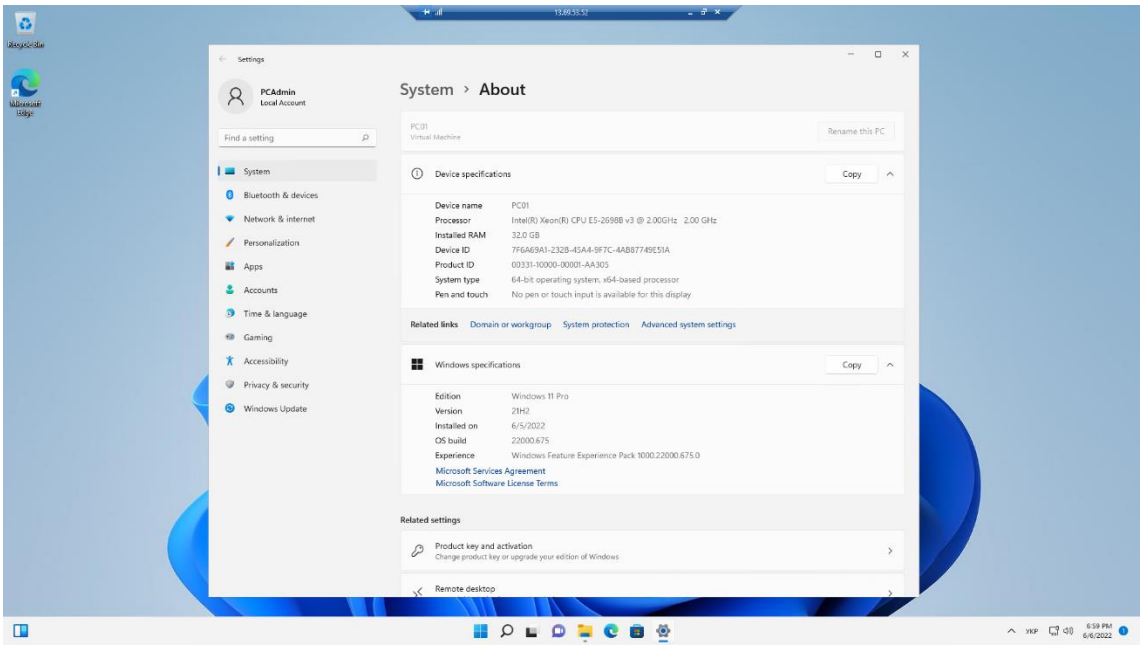

Рисунок 3.57 – Комп’ютер підключений до локальної групи

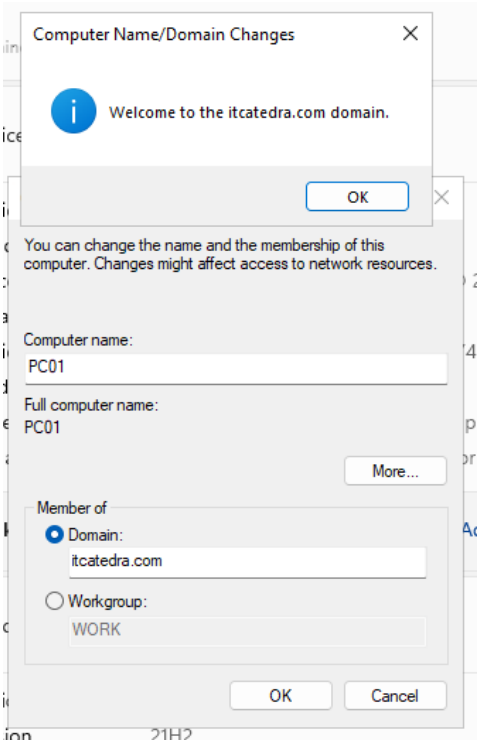

Рисунок 3.58 – Ввід комп’ютера в домен

Для підключення користувача до AVD звичайної утиліти RDP вже не достатньо. Для цього потрібна спеціальна програма або ж можна скористатися веб-інтерфейсом [31]. У застосунку з випадаючого меню потрібно обрати пункт, підписатися й вказати дані профілю, який був створений в AAD. Якщо все було введено правильно на панелі стане доступний користувачу набір підключень (рис. 3.59).

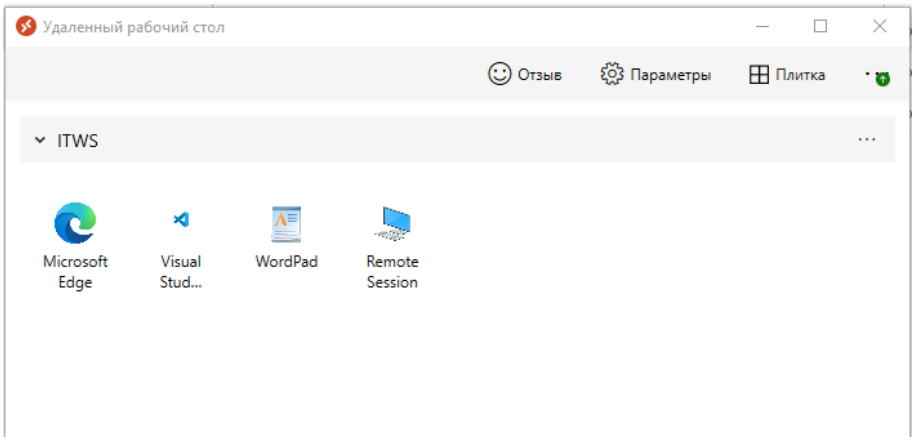

Рисунок 3.59 – Клієнт для підключення до AVD

Якщо обрати виділену програму, то вона запуститься в окремому вікні і буде своїм видом нагадувати аналог, який міг би бути запущений локально. Але застосунок має зв’язок із віртуальною файловою системою та мережею. Тому створений текстовий файл можна зберегти як на локальному диску, так і на віртуальних файлових сховищах (рис. 3.60-3.61).

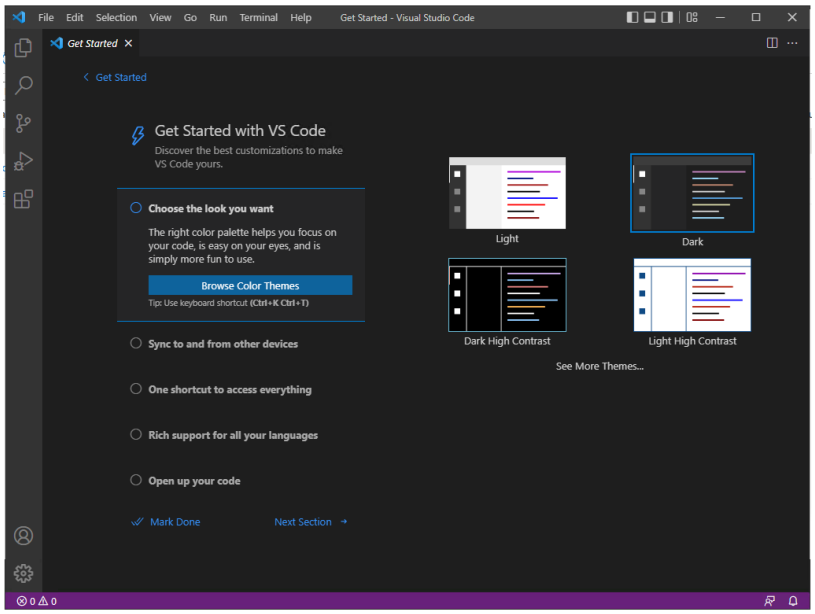

Рисунок 3.60 – Віртуальна сесія виділеної програми

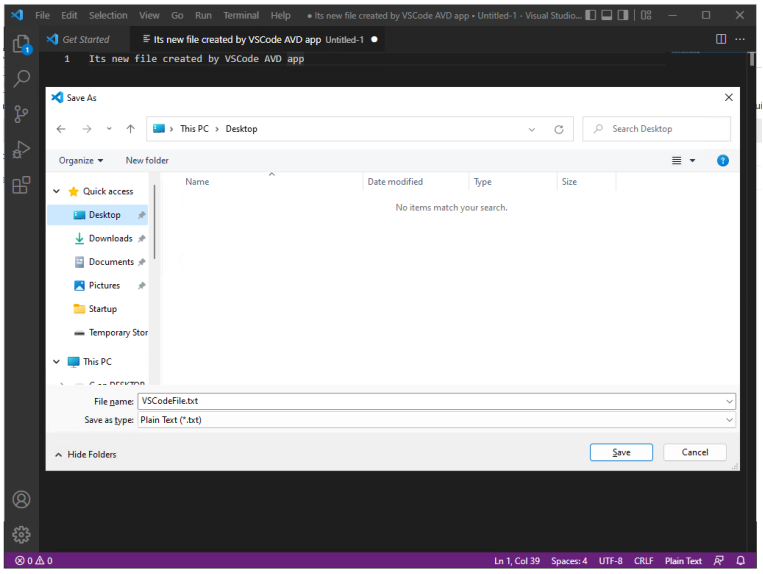

Рисунок 3.61 – Збереження файлу на віртуальний диск

Створення нових профілів відбувається на платформі Azure через сервіс AAD. Але по суті сам процес відрізняється від того, що було на сервері, хіба що візуально. Тут так само треба вказати ім’я, прізвище, логін для входу та пароль, який користувач буде зобов’язаний змінити після першого входу (рис. 3.62).

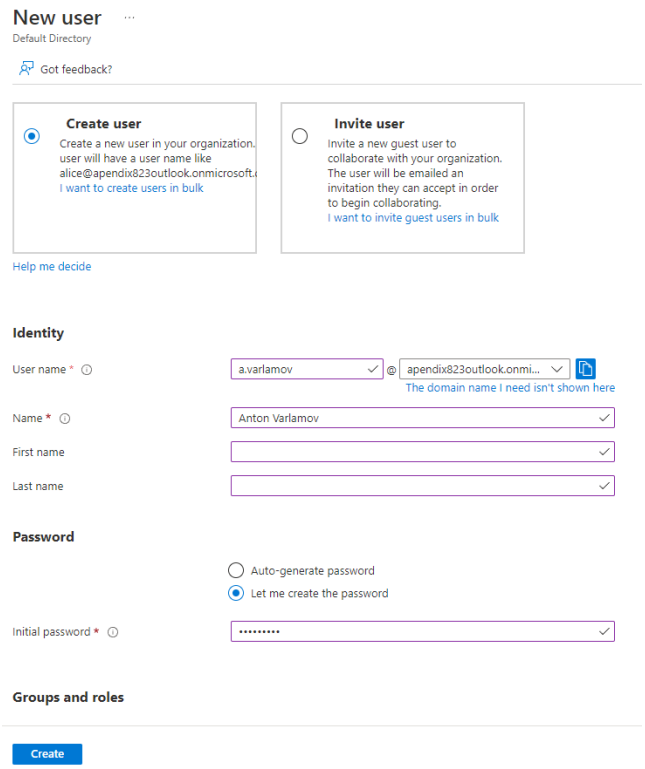

Рисунок 3.62 – Меню створення нового користувача

Після під’єднання нового користувача йому доступне тільки з’єднання з робочим столом, додати віртуальний запуск застосунків можна у панелі управління AVD (рис. 3.63).

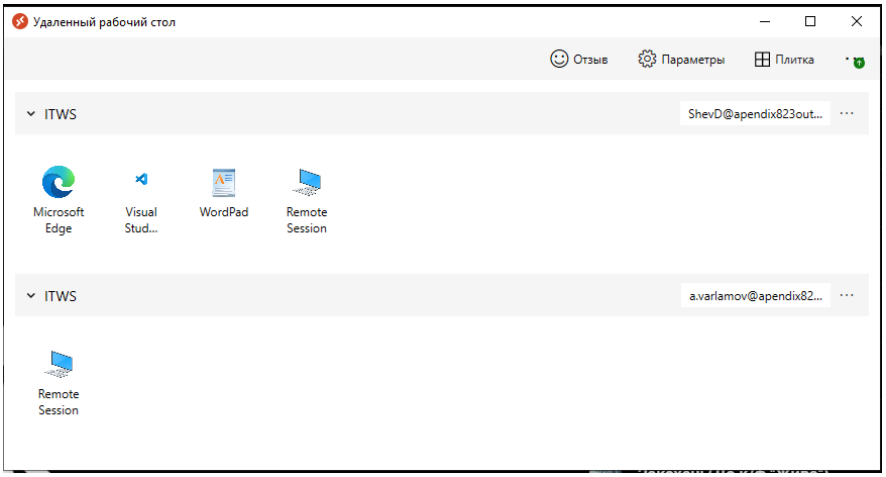

Рисунок 3.63 – Підпис нового профілю
до клієнта віддалених підключень

Усі облікові записи поділені на дві групи: адміністратори та звичайні користувачі. Також є окрема специфічна група контролеру домену. У ресурсній групі цим профілям призначені відповідні ролі для авторизації до віртуальних машин (рис. 3.64).

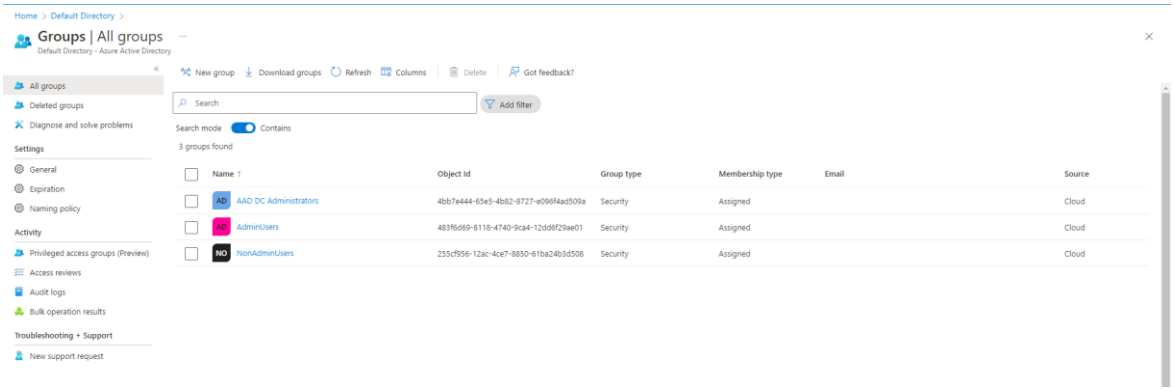

Рисунок 3.64 – Групи користувачів

Меню адміністрування сервісу AVD надає можливості для відстеження за станом пулу віртуальних машин, активних сесій, дозволяє відстежити користувача та VM, із якою він підключився. Тут же створюються нові пули віртуальних машин, якщо виникне потреба розширення інфраструктури. Через підменю Application groups додаються дозволи для запуску окремих застосунків або їх же додавання окремим користувачам (рис. 3.65-3.66).

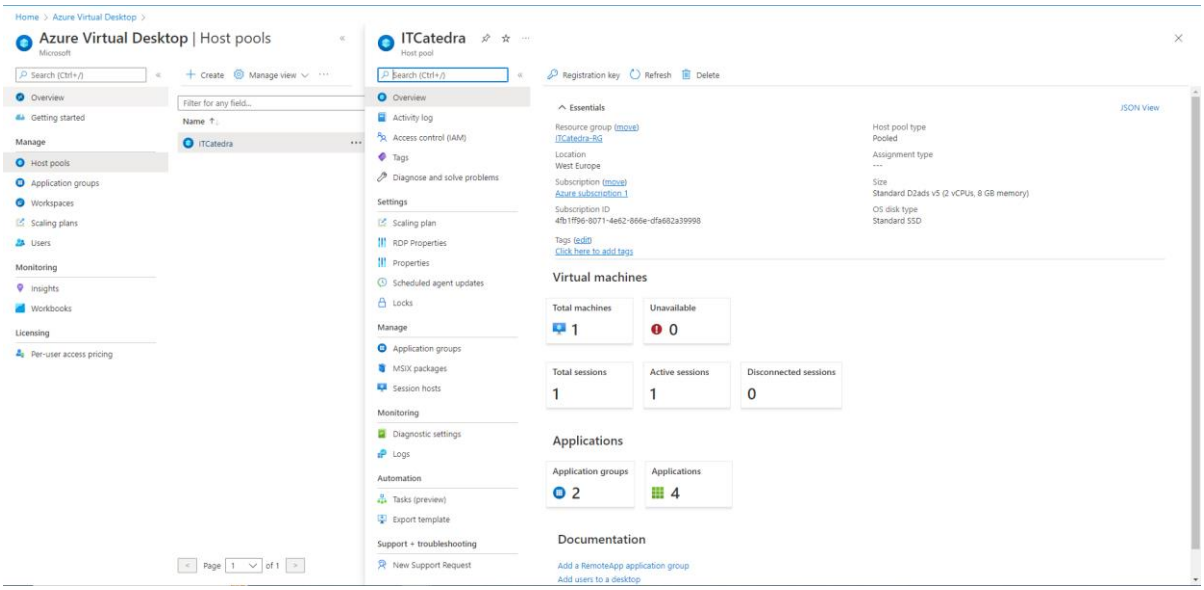

Рисунок 3.65 – Меню управління пулами хостів AVD

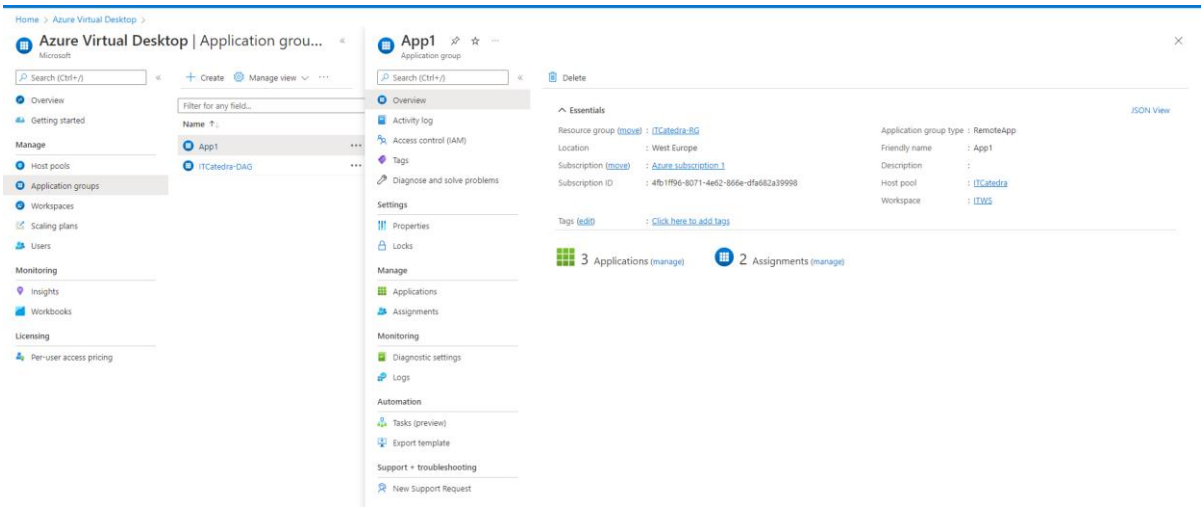

Рисунок 3.66 – Меню управління групами застосунків AVD

3.4 Переваги виконаної модернізації мережі

У результаті проведеної роботи було створено та налаштовано сервер з ОС Windows Server. Він розташований на хмарній платформі Azure і має зв’язок з локальною мережею через Site-to-Site vpn-тунель. Також здійснено інтеграцію з деякими окремими сервісами Azure. Стисле порівняння старої та нової мереж представлено в таблиці 3.1.

Таблиця 3.1 – Порівняння двох мереж

Параметр порівняння	Стара мережа	Нова мережа
Профілі користувача	Один профіль на групу користувачів	Унікальний профіль для кожного користувача
Віддалений доступ до системи	Не реалізований	Роль RDS на сервері, та віртуалізація окремих програм через сервіс Azure

Продовження табл. 3.1

Використання тонких клієнтів	Тільки в якості локальних машин	Є можливість віддаленої роботи
Додавання пам’яті до системи	Лише через підключення нових дисків	Через додавання віртуальних дисків до машини, а також через створення віртуальних папок спільного доступу
Гнучкість в розширенні	Через закупку апаратного обладнання	Через додавання віртуальних елементів
Резервне копіювання	Через внутрішні засоби ОС, копії зберігаються на фізичний диск	Через спеціальний сервіс, копії зберігаються в хмарі в окремих сховищах

Виходячи з вказаного в таблиці 3.1 можна сказати, що дана розробка збільшила відмовостійкість і гнучкість мережі, тому що все обслуговування бере на себе провайдер і гарантує безперебійне підключення. Якщо ж якийсь окремий датацентр вийде з ладу, дана інфраструктура буде перенесена в інший датацентр. Це мінімізує простій роботи. При потребі розширення достатньо ввести в інфраструктуру новий віртуальний сервіс, що простіше, ніж закупівля нового обладнання. Був реалізований віддалений доступ до системи. Це дозволяє юзерам використовувати тонкі клієнти та запускати специфічні програми.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи бакалавра було виконано оптимізацію роботи локальної обчислювальної мережі кафедри ІТ за рахунок її віртуалізації, модернізація шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій.

На початку розробки проекту був проведений аналіз предметної області, визначена актуальність дослідження. Був проведений аналіз існуючих технологій створення мереж, виділено їх переваги та недоліки. Проведений аналіз недоліків існуючої мережі, та визначені вимоги до нової мережі. Визначені оптимальні методи для модернізації мережі. Після чого, була сформульовано мета та задачі проекту. Було виконано планування робіт та розглянуто ризики, які можуть виникнути під час розробки реалізації проекту (Додаток Б).

При проектуванні створені контекстні діаграми проекту та її декомпозиція, виділені різні підпроцеси, управління, механізми, їх вхідні та вихідні дані. Була побудована діаграма варіантів використання, виділені актори та їх варіанти використання.

У практичній частині роботи було створено мережу, в основі якої стоїть сервер на базі ОС Windows Server, що розташований у хмарі на платформі Azure. Проведено інтеграцію з сервісами Azure, для збільшення гнучкості мережі. Було продемонстровано налаштування та роботу мережі, серверу та інтегрованих сервісів.

Створена мережа дозволить підвищити рівень безпеки, збільшить гнучкість при масштабуванні. Централізований пункт управління мережею підвищує зручність роботи для адміністратора. Обраний спосіб реалізації на порталі Azure дає можливість в майбутньому, без великих затрат перейти на повністю нові хмарні рішення, коли вони набудуть поширення.

Результати роботи були апробовані на науково-практичній конференції ІМА 2022 в Сумському державному університеті (додаток В).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a LAN? Cisco. URL: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html (Дата звернення: 24.05.2022).

2. Virtualization of computer network for modernization and optimization the work of the LAN within IT department// Матеріали та програма МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ студентів та молодих учених / – Суми: МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ МІЖНАРОДНИЙ УНІВЕРСИТЕТ «АСТАНА», 2022. – С. 84.

3. IBM Cloud Learn Hub / Virtualization. URL: https://www.ibm.com/cloud/learn/virtualization-a-complete-guide#toc-vmware-S5QwUXKB (Дата звернення: 24.05.2022).

4. IBM Cloud Learn Hub / Cloud servers. URL: https://www.ibm.com/cloud/learn/cloud-server (Дата звернення: 24.05.2022).

5. Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud / T. Laszewski та ін. Packt Publishing, 2018. 358 с.

6. Azure IaaS (infrastructure as a service). URL: https://azure.microsoft.com/en-us/overview/what-is-azure/iaas/#overview (Дата звернення: 24.05.2022).

7. Manage User Accounts in Windows Server Essentials | Microsoft Docs. URL: https://docs.microsoft.com/en-us/windows-server-essentials/manage/manage-user-accounts-in-windows-server-essentials (Дата звернення: 24.05.2022).

8. Welcome to Remote Desktop. URL: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds (Дата звернення: 24.05.2022).

9. Understanding the Remote Desktop Protocol (RDP). URL: https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol (Дата звернення: 24.05.2022).

10. What is a Thin Client? [Електронний ресурс] – Режим доступу до ресурсу: https://www.forcepoint.com/cyber-edu/thin-client (Дата звернення: 24.05.2022).

11. Use Group Policy to Configure Domain Member Client. URL: https://docs.microsoft.com/en-us/windows-server/networking/branchcache/deploy/use-group-policy-to-configure-domain-member-client-computers (Дата звернення: 24.05.2022).

12. What is Samba?. URL: https://www.samba.org/samba/what_is_samba.html (Дата звернення: 24.05.2022).

13. Active Directory Domain Services. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services (Дата звернення: 24.05.2022).

14. Limoncelli T. A., Hogan C. J., Chalup S. R. The Practice of System and Network Administration: Volume 2: DevOps and other Best Practices for Enterprise IT. Addison-Wesley Professional, 2016. С 1232.

15. Azure Virtual Desktop. URL: https://azure.microsoft.com/en-us/services/virtual-desktop/#overview (Дата звернення: 24.05.2022).

16. What is IDEF - Definition, Methods, and Benefits. URL: https://www.edrawsoft.com/what-is-idef.html (Дата звернення: 24.05.2022).

17. ISO/IEC/IEEE 31320-1:2012(en) Information technology — Modeling Languages. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:31320:-1:ed-1:v1:en (Дата звернення: 24.05.2022).

18. What is Use Case Diagram. URL: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-use-case-diagram/ (Дата звернення 24.05.2022).

19. Manage Azure resource groups by using the Azure portal. URL: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal (Дата звернення 24.05.2022).

20. Virtual Network documentation. URL: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

21. Create a Windows virtual machine in the Azure portal. URL: Quickstart - Create a Windows VM in the Azure portal - Azure Virtual Machines | Microsoft Docs (Дата звернення 24.05.2022).

22. Active Directory Domain Services Overview. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (Дата звернення 24.05.2022).

23. Group Policy Overview. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11) (Дата звернення 24.05.2022).

24. Managing Disk Quotas. URL: https://docs.microsoft.com/en-us/windows/win32/fileio/managing-disk-quotas (Дата звернення 24.05.2022).

25. Create a Site-to-Site connection using the Azure portal. URL: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-classic-portal (Дата звернення 24.05.2022).

26. Cisco IOS VPN Configuration Guide. URL: https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html (Дата звернення 24.05.2022).

27. About Site Recovery. URL: https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview (Дата звернення 24.05.2022).

28. What is Azure AD Connect?. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect (Дата звернення 24.05.2022).

29. Mount SMB Azure file share on Windows. URL: https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows (Дата звернення 24.05.2022).

30. Azure Virtual Desktop documentation. URL: https://docs.microsoft.com/en-us/azure/virtual-desktop/ (Дата звернення 24.05.2022).

31. Connect with the Windows Desktop client. URL: Connect to Azure Virtual Desktop with the Windows Desktop client - Azure | Microsoft Docs (Дата звернення 24.05.2022).

ДОДАТОК А

ТЕХНІЧНЕ ЗАВДАННЯ

на розробку

«Віртуалізація комп’ютерної мережі для модернізації

та оптимізації роботи LAN кафедри ІТ»

ПОГОДЖЕНО:

Доцент кафедри комп’ютерних наук

_____ Антипенко В.П.

Студент групи ІТ-81-9

_____ Шевченко Д.О.

Суми 2022

1. Призначення й мета віртуалізації комп’ютерної мережі для оптимізації роботи LAN кафедри IT

1.1Призначення віртуалізації комп’ютерної мережі для оптимізації роботи LAN кафедри IT

Призначення даної роботи полягає в модернізації мережі шляхом реалізації термінального серверу.

1.2 Мета створення проекту

Головна мета проекту є оптимізація роботи локальної обчислювальної мережі кафедри IT за рахунок її віртуалізації. Модернізацію можна здійснити шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій

1.3 Цільова аудиторія

Проект розроблюється з оглядом на використання його результатів на кафедрі IT студентам, викладачами та робочим персоналом.

2 Вимоги до проекту

2.1 Вимоги до проекту в цілому

2.1.1 Вимоги до структури й функціонування

Локальна обчислювальна мережа має містити сервер, який буде реалізований на базі хмарних технологій і використовувати обчислювальні потужності хмарного провайдеру. Сервер повинен мати можливість для виконання різних ролей, зокрема термінального серверу.

2.1.2 Вимоги до персоналу

Усе обслуговування серверу, що відноситься до апаратного забезпечення бере на себе провайдер хмарних технологій, який надає послугу. Обслуговування програмної частини сервера виконує системний адміністратор.

2.1.3 Вимоги до розмежування доступу

Підключення до реалізованої мережі має бути доступне віддаленим клієнтам через мережу Інтернет. Зв’язок має бути розділений між різними групами користувачів із розподіленими правами доступу. Обов’язково має бути аккаунт головного адміністратора. Він вже створює нові групи користувачів та окремі їх профілі. Основними такими групами мають бути студенти, викладачі та адміністратор. Студент має доступ до перегляду інформації, яка знаходиться в певних виділених каталогах, ділянку пам’яті певного розміру, де є можливість створювати каталоги та зберігати власні файли. У викладача є доступ до каталогів та файлів студентів, можливість додавати та редагувати файли та директорії на ділянці пам’яті, яка виділена для розташування учбових матеріалів. Адміністратор має доступ до всіх ділянок пам’яті, права на встановлення, видалення та оновлення програмного забезпечення. Головний адміністратор володіє всіма правами на управління сервером, повний доступ до змін в груповій політиці, до управління ролями серверу.

2.2 Структура локальної обчислювальної мережі

2.2.1 Загальна інформація про структуру проекту

Локальна обчислювальна мережа представляє з’єднання активного обладнання в межах одного кабінету. Для цього використовується пасивне мережева обладнання, а саме комутатор. Декілька комутаторів поєднуються

між собою й з’єднуються з активним мережевим обладнанням, а саме маршрутизатором. На базі хмарних технологій має бути реалізований виділений термінальний сервер, до якого має бути доступ через мережу інтернет.

2.2.2 Управління мережею

Управління мережею має здійснюватися через службу управління доменами на сервері, через аккаунт головного адміністратора. Управління сервером відбувається через спеціальну виділену панель управління, що надає провайдер хмарних послуг.

2.2.3 Вимоги щодо захисту інформації

Для забезпечення безпеки збереження інформації, та захисту від несанкціонованого доступу, мережа повинна мати як мінімум такі можливості:

– кожен користувач повинен отримувати доступ до системи лише з використанням пароля;

– для користувачів повинні бути встановлені різні рівні доступу;

– кожен користувач, відповідно до рівня доступу, повинен мати певний набір дозволених можливостей, що до перегляду та редагування інформації.

2.3 Вимоги до видів забезпечення

2.3.1 Вимоги до лінгвістичного забезпечення

Мова операційної системи буде встановлена за вибором головного адміністратора з визначеного списку, її можна буде змінити в будь-який момент.

2.3.2 Вимоги до апаратного забезпечення

Віддалений клієнт для підключення може використовувати: стаціонарний персональний комп’ютер, тонкий клієнт, або ж смартфон.

2.4 Вимоги до функціонування системи

2.4.1 Потреби користувача

Потреби користувача представлені у таблиці А.1.

Таблиця А.1 – Потреби користувача

ID	Потреби користувача	Джерело
UN-01	Виділа ділянка пам’яті певного розміру для зберігання власних файлів	Студент, викладач, адміністратор
UN-02	Можливість додавати та редагувати файли учбових матеріалів	Студент, викладач
UN-03	Можливість переглядати студентські каталоги	Викладач
UN-04	Можливість оновлювати програмне забезпечення	Адміністратор
UN-05	Можливість встановлювати програмне забезпечення	Адміністратор
UN-06	Можливість видаляти програмне забезпечення	Адміністратор
UN-07	Можливість редагування групової політики сервера	Головний адміністратор
UN-08	Можливість управління ролями сервера	Головний адміністратор

2.4.2 Системні вимоги

Проаналізувавши потреби, було визначено наступні вимоги:

- наявність унікальних аккаунтів для користувачів;
- встановлення різних рівнів доступу для користувачів;
- виділення особистої ділянки пам’яті для роботи користувачів.

3 Склад і зміст робіт з проекту «Віртуалізація комп’ютерної мережі для модернізації та оптимізації роботи LAN кафедри ІТ»

Детальний опис етапів оптимізації роботи локальної обчислювальної мережі кафедри ІТ наведено в таблиці А.2.

Таблиця А.2 – Етапи оптимізації роботи локальної обчислювальної мережі кафедри ІТ

№	Склад і зміст робіт	Строк розробки
1	Визначення мети проекту	2 днів
2	Аналіз актуальної мережі	5 днів
3	Визначення недоліків актуальної мережі	3 днів
4	Визначення нових вимог до мережі	4 днів
5	Планування робіт	5 днів
6	Проектування нової мережі	18 днів
7	Встановлення та налаштування серверної операційної системи	8 днів
8	Налаштування серверної операційної системи	10 днів
9	Тестування	8 день
	Загальна тривалість робіт	63 днів

ДОДАТОК Б

Планування робіт

Метою даного проекту є оптимізація роботи локальної обчислювальної мережі кафедри ІТ за рахунок її віртуалізації. Модернізацію можна здійснити шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій.

Для досягнення поставленої мети необхідно виконати наступні задачі:

- дослідити актуальність роботи та її предметну область;
- проаналізувати можливі способи реалізації серверу;
- визначення недоліки існуючої топології та встановити нові вимоги до мережі;
- визначити оптимальні методи для модернізації локальної мережі;
- розробити схеми та практичні моделі нової мережі;
- виконати віртуалізацію мережі;
- протестувати роботу мережі, можливість віддаленого підключення, функціонування всіх сервісів.

Даний проект дозволить підвищити продуктивність роботи мережі. Зокрема збільшиться її пропускна здатність. Також зменшиться затримка її роботи, втрати даних та мережеві помилки. Взагалі дана модернізація принесе ряд переваг. Після неї зросте швидкість роботи мережі, її безпека та безпека користувачів, а також контроль адміністратора над системою.

Представлена робота розроблюється з метою використання її результатів на кафедрі інформаційних технологій.

Продуктом даного проекту буде оновлена локальна обчислювальна мережа для кафедри ІТ, яка буде відповідати поставленим вимогам з оглядом на сучасні тенденції застосування хмарного серверу.

Деталізація мети проекту методом SMART. Це дозволяє більш конкретно представити призначення розроблюваного продукту.

Для виконавця даного проекту формат постановки SMART-мети такий: «Оптимізація роботи локальної обчислювальної мережі кафедри ІТ за рахунок її віртуалізації. Модернізацію можна здійснити шляхом додавання серверу, реалізуючи його через сервіс хмарних технологій». Результати деталізації методом SMART розміщені у таблиці Б.1.

Таблиця Б.1 – Деталізація мети проекту методом SMART

Specific	Модернізувати актуальну мережу кафедри ІТ шляхом додавання термінального сервера.
Measurable	Створений сервер, який дозволить виконати підключення віддаленого клієнта та буде реалізовувати виділені ролі.
Achievable	Мета досяжна, є затверджене завдання.
Relevant	Підвищення продуктивності праці за рахунок усунення недоліків, зросте швидкість роботи, обміну даними та рівень безпеки користувача та мережі
Time-framed	Є конкретний термін – до кінця 4 курсу (09.06.2022).

Планування змісту робіт. WBS – це графічне подання згрупованих елементів проекту у вигляді пакетів робіт, які ієрархічно пов’язані з продуктом проекту. WBS необхідна для забезпечення ефективного управління проектом, визначення і структурування переліку робіт, створення структури звітності, розуміння задач виконавцем.

WBS є базовим засобом для створення організаційної структури (OBS) і системи управління проектом, оскільки дозволяє виявити проблеми організації робіт, визначення ієрархії проектних завдань (етапів робіт), підзавдань і пакетів робіт на всіх подальших фазах життєвого циклу проекту.

WBS дозволяє розподілити відповідальність за досягнення цілей проекту між його виконавцями та тим самим гарантувати, що всі роботи за проектом мають відповідальних і не випадуть з поля зору. WBS забезпечує

членам команди розуміння загальних цілей і завдань за проектом. Важливо врахувати всі роботи в проекті і кількість рівнів деталізації визначається достатністю для планування та моніторингу робіт проекту.

WBS повинна давати команді управління проектом та замовнику чітку картину кінцевого продукту проекту та всіх процесів, за допомогою яких він буде створений.

Основне призначення WBS- структури - визначити зміст проекту через декомпозицію його продуктів. Кожна WBS-структура є інструментом, який допомагає керівникові проекту здійснити декомпозицію робіт проекту до рівня, необхідного для досягнення його цілей.

Планування змісту структури робіт даного IT-проекту (WBS) здійснювалося за допомогою програми WBS Schedule. На рисунку Б.1 представлено WBS з розробки проекту.

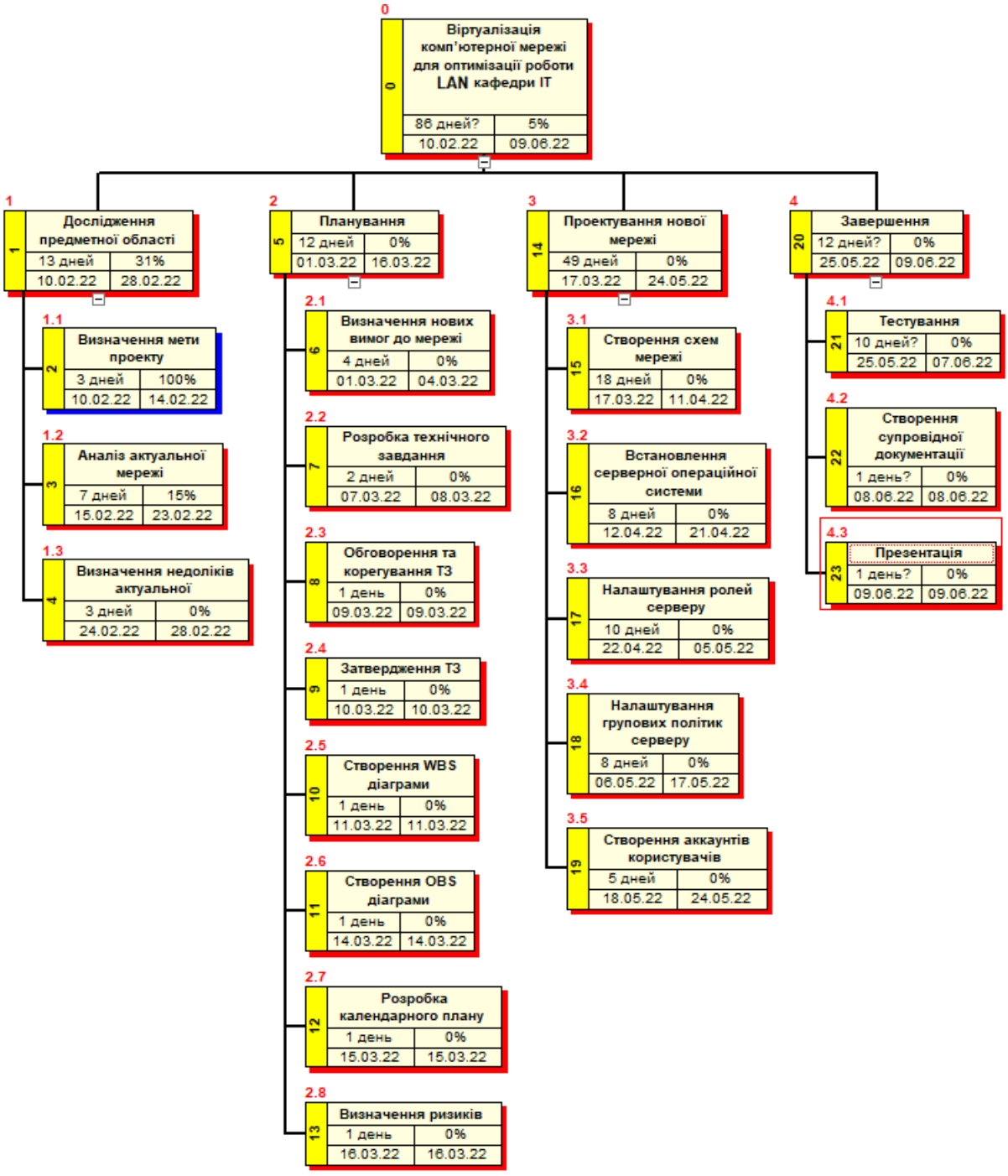

Рисунок Б.1 – WBS-структура робіт проекту

Планування структури виконавців. OBS – графічне відображення учасників проекту (фізичних та юридичних осіб) та їхніх відповідальних осіб, залучених до реалізації проекту. Елементами OBS можуть бути: окремі виконавці (керівники, фахівці, службовці), організації, структурні підрозділи і служби, у яких зайнята та або інша кількість фахівців, що

виконують певні функціональні обов'язки, зовнішні постачальники обладнання, послуг та інші організації.

OBS є найважливішим механізмом управління проектами. OBS дає можливість реалізувати всі пакети робіт, передбачені WBS-структурою, а також функції, процеси й операції, необхідні для досягнення поставлених перед проектом цілей. OBS є основою формування і здійснення діяльності команди проекту.

Слід відрізняти організаційну структуру організації та організаційну структуру проекту. На етапі планування, коли розробляють OBS-структуру проекту, досить часто невідомо, які конкретні організації та їхні відповідальні особи будуть залучені до проекту. Відповідь на це запитання буде отримана тільки після проведення відповідних тендерів на виконання робіт. Тому попередньо в OBS-структуру вводять умовні позначення виконавців та їх відповідальних осіб, які потім змінюють на конкретні дійсні назви та прізвища.

Планування змісту структури організації (OBS) здійснювалося за допомогою програми WBS Schedule.

На рисунку Б.2 представлено організаційну структуру планування проекту.

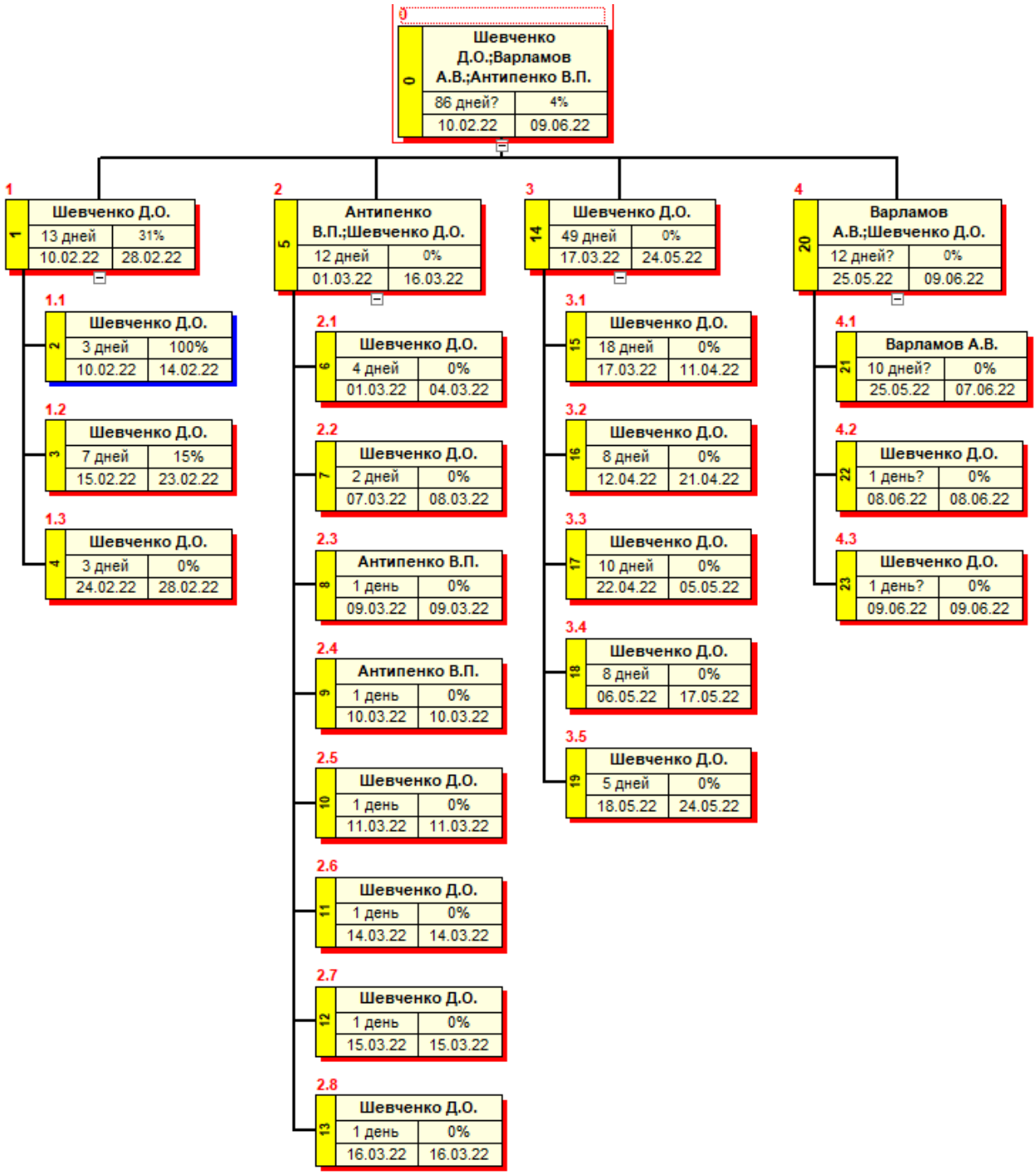

Рисунок Б.2 – OBS-структура робіт проекту

Діаграма Ганта. На діаграмі Ганта всі роботи за проектом представлені у вигляді горизонтальних відрізків, паралельних осі часу. Використання моделі проекту, побудованої в програмному середовищі MS Project, дозволяє контролювати й оптимізувати план виконання робіт, наочно відстежувати хід його виконання. Завдяки цьому можна отримати достовірне уявлення

про тривалість процесів з обмеженнями у ресурсах, урахуванням вихідних днів та свят.

Календарний графік проекту представлено на рисунках Б.3.

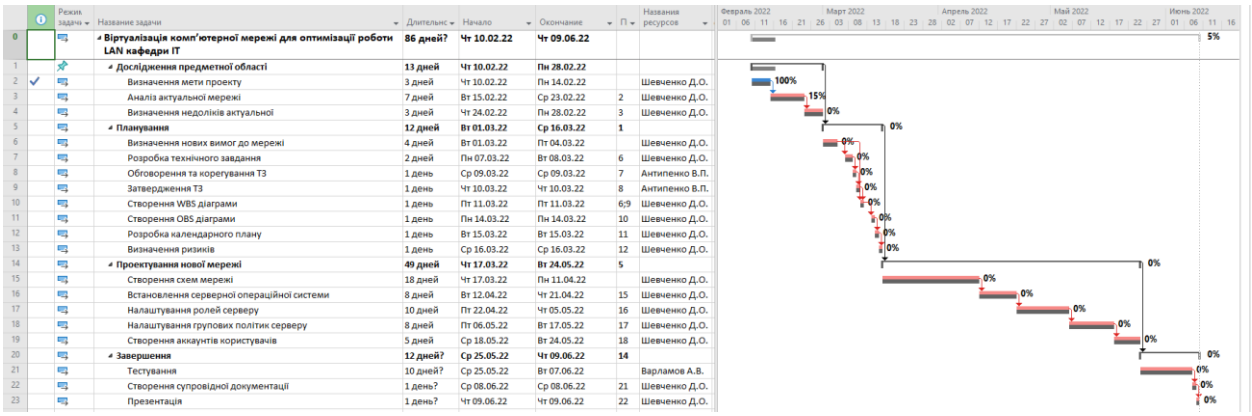

Рисунок Б.3 – Календарний графік проекту

Управління ризиками проекту. Під час виконання якісної оцінки ризиків треба визначити ризики, які мають бути усунені якнайшвидше. У залежності від ступеня важливості ризику – реагування буде відповідне. Наступним етапом є виконання кількісного оцінювання ризиків. Кількісне та якісне оцінювання можуть виконувати одночасно або окремо, що залежить від ступеня забезпечення проекту. У таблиці Б.3 представлено шкалу для класифікації ризиків за величиною впливу на проект та ймовірністю виникнення.

Таблиця Б.3 – Визначення ймовірності, впливу та рангу ризиків проекту.

№	Назва ризику	Ймовірність (0,1 – 0,9)	Вплив (0,05-0,8)	Ранг
1	Зміна вимог ТЗ	0,5	0,8	0,4
2	Проблеми з підключенням до Інтернету	0,3	0,4	0,12
3	Збій електромережі	0,3	0,4	0,12

Продовження табл. Б.3

4	Хвороба працівника	0,5	0,8	0,4
5	Недостатня кваліфікація працівника	0,3	0,4	0,12
6	Збій у роботі техніки розробника	0,5	0,8	0,4
7	Нечітко виділені вимоги	0,1	0,4	0,04
8	Неправильний розподіл часу	0,1	0,2	0,02
9	Непрацездатність хмарного сервісу	0,1	0,4	0,04
10	Виявлення помилок під час тестування	0,5	0,1	0,05
11	Збій програмного забезпечення	0,3	0,4	0,12

Для того, щоб знизити негативний вплив ризиків на проект треба виконати планування реагування на них. До нього входить визначення ефективності розробки та оцінка наслідків впливу на проект. Оцінювання виконується за показниками, що описані в таблиці Б.3. У результаті планування реагування було отримано матрицю ймовірності виникнення ризиків та впливу ризику, що зображена на рисунку Б.4. Зеленим кольором на матриці позначають прийнятні ризики, жовтим – виправдані, а червоним – недопустимі.

Таблиця Б.4 – Матриця ймовірності та впливу згідно проекту

Ймовірність	Вплив загрози(ризику)				
	Дуже малий 0,05	Малий 0,1	Середній 0,2	Великий 0,4	Дуже великий 0,8
0,9					
0,7					

Продовження табл. Б.4

0,5		R10(0.05)			R1(0.4) R4(0.4) R6(0.4)
0,3				R2(0.12) R3(0.12) R5(0.12) R11(0.12)	
0,1			R8(0.02)	R7(0.04) R9(0.04)	

Класифікація ризиків за рівнем, відповідно до отриманого значення індексу, представлена у таблиці Б.4. У таблиці Б.5 описано ризики та стратегії реагування на кожен з них.

Таблиця Б.4 – Шкала оцінювання за рівнем ризику.

№	Назва	Межі	Ризик, які входять (номера)
1	Прийнятні	0,005≤ R ≤0,05	7, 8, 9, 10
2	Виправдані	0,05< R ≤0,14	2, 3, 5, 11
3	Недопустимі	0,14< R ≤0,72	1, 4, 6

Таблиця Б.5 – Ризики та стратегії реагування

ID	Статус ризику	Опис	Ймовірність	Вплив	Ранг ризику	План А	Тип стратегії реагування	План Б
1	Відкритий	Зміна вимог ТЗ	Середній	Високий	0,4	Обговорити питання на початку проекту	Ухилення	-
2	Відкритий	Проблеми з підключенням до Інтернету	Низький	Високий	0.12	Підключити два провайдери інтернету	Ухилення	Залучити спеціаліста для усуннення проблем
3	Відкритий	Збій електромережі	Низький	Високий	0.12	Залучити спеціаліста для усунення збоїв	Зменшення	-
4	Відкритий	Хвороба працівника	Середній	Високий	0.4	Проводити профілактику захворювань	Зменшення	-

Продовження табл. Б.5

5	Відкритий	Недостатня кваліфікація працівника	Низький	Високий	0.12	Підвищити кваліфікацію працівника	Зменшення	Долучити стороннього спеціаліста
6	Відкритий	Збій у роботі техніки розробника	Середній	Високий	0.4	Залучити спеціаліста для усуннення проблем	Зменшення	Змінити обладнання
7	Відкритий	Нечітко виділені вимоги	Низький	Високий	0.04	Обговорити не зрозумілі пункти завдання	Зменшення	-
8	Відкритий	Неправильний розподіл часу	Низький	Середній	0.02	Перевизначити терміни виконання завдання	Зменшення	Працювати понаднормово
9	Відкритий	Непрацездатність хмарного сервісу	Низький	Високий	0.04	-	-	-

Продовження табл. Б.5

10	Відкритий	Виявлення помилок під час тестування	Середній	Середній	0.05	Виправити помилки	Зменшення	Проігнорувати помилки якщо вони не значні
11	Відкритий	Збій програмного забезпечення	Низький	Високий	0.12	Виправити помилку, що призводить до збою	Зменшення	Перевстановити програмне забезпечення

ДОДАТОК В

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Virtualization of computer network for modernization and optimization the work of the LAN within IT department

Danylo Shevchenko, *Student of IT-81*;
Viktoriia Antypenko, *Associate Professor*

Department "Information Technology"
Sumy State University, Sumy, Ukraine

There is a high increase in using the cloud services during the last years. Nowadays, their popularity is growing among various organizations due to quarantine restrictions, hostilities etc. Cloud technology (CT) is a model of access to dedicated resources via the Internet. Their concept allows to implement remote access for users to computing resources, utilities and numerous other services.

The main condition for the CT functioning is the connection to the World Wide Web. Cloud computing technologies are evolving rapidly and have significant potential. Modern products for development and operation may require large productivity of hardware resources. Thus, the demand for equipment upgrades is relevant. Cloud technologies can solve this problem of excessive exactingness on utilities for end-user equipment.

Of course, it is possible to implement distant work for the staff using a local server by installing the software applications and performing a terminal connection. However, this requires significant resources, both financial and human. Cloud providers allow to organize remote work relatively quickly. Virtual servers do not require physical maintenance, the purchase of uninterruptible power supplies as well as they simplify both backup and recovery after possible failures, solving the issue of increasing the productivity of hardware resources.

There are many options for organizing a network infrastructure in the cloud. Of course, it is needed to start from the tasks type, but the main one usually is a terminal connection to a remote desktop in order to access the necessary software applications and utilities. Certainly, on the basis of this server it is possible to implement other services like file, mail, print servers etc. This technology allows more flexible system management and increases user and data security.

Cloud providers have many different offers for various needs. For instance, it is realizable to select a dedicated server and use virtualization technology to configure it along with a virtual network infrastructure. Or apply one of the already-made solutions that the providers have. Then the

ДОДАТОК Г

Скрипт для налаштування для систем CiscoIOS

```
!Налаштування політики списків доступу, щоб дозволити проходження трафіку
! Дозволити передачу трафіку по інтерфейсу для представлених мереж
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
! Дозволити трафік протоколів між зазначеними хостами
access-list 101 permit esp host 13.80.74.71 host 1.2.3.4
access-list 101 permit udp host 13.80.74.71 eq isakmp host 1.2.3.4
access-list 101 permit udp host 13.80.74.71 eq non500-isakmp host 1.2.3.4
! Конфігурація Internet Key Exchange (IKE). Налаштування параметрів
аутентифікації, шифрування, хешування та PSK.
crypto ikev2 proposal ITCatedra-S2S-Connection-proposal
encryption aes-cbc-256 aes-cbc-128 3des
integrity  sha1
group      2
exit
crypto ikev2 policy ITCatedra-S2S-Connection-policy
proposal ITCatedra-S2S-Connection-proposal
match address local 1.2.3.4
exit

crypto ikev2 keyring ITCatedra-S2S-Connection-keyring
peer 13.80.74.71
address 13.80.74.71
pre-shared-key ExampleKey
exit
exit
crypto ikev2 profile ITCatedra-S2S-Connection-profile
match address  local 1.2.3.4
match identity remote address 13.80.74.71 255.255.255.255
authentication remote pre-share
authentication local  pre-share
lifetime       3600
dpd 10 5 on-demand
keyring local  ITCatedra-S2S-Connection-keyring
exit
```

```
! Налаштування IPsec, включає властивості шифрування, аутентифікації та тунельного режиму
crypto ipsec transform-set ITCatedra-S2S-Connection-TransformSet esp-gcm 256
mode tunnel
exit
crypto ipsec profile ITCatedra-S2S-Connection-IPsecProfile
set transform-set  ITCatedra-S2S-Connection-TransformSet
set ikev2-profile  ITCatedra-S2S-Connection-profile
set security-association lifetime seconds 3600
exit
! Налаштування тунельного інтерфейсу через який буде передаватися трафік
int tunnel 11
ip address 169.254.0.1 255.255.255.255
tunnel mode ipsec ipv4
ip tcp adjust-mss 1350
tunnel source 1.2.3.4
tunnel destination 13.80.74.71
tunnel protection ipsec profile ITCatedra-S2S-Connection-IPsecProfile
exit
!Створення статичного маршруту для тунелю IPSec
ip route 10.0.0.0 255.255.0.0 Tunnel 11
```

ДОДАТОК Д

Скрипт для для монтування директорії

```
$connectTestResult = Test-NetConnection -ComputerName
itcstrg.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
 # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"itcstrg.file.core.windows.net`"
/user:`"localhost\itcstrg`"
/pass:`"5a/V9t8geuFzJX3ZSSPdj31QlH6z+w+udQVYbMGTBgusMvBM9TevOQCDLlr2+Yo1Il0F9m
HF/I1r+AStprzLrQ==`""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\itcstrg.file.core.windows.net\papka" -Persist
} else {
    Write-Error -Message "Unable to mount storage"
}
```