

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект гібридної ІТ-інфраструктури органі-
зації на базі продуктів Microsoft»

Виконала: студентка 4-го курсу групи КІ-21-1
спеціальності 123 «Комп'ютерна інженерія»

 Анастасія КОВТОНЮК

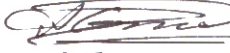
Керівник: доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

Рецензент: завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Ковтонюк Анастасія Дмитрівна

Тема роботи: «Проект гібридної IT-інфраструктури організації на базі продуктів Microsoft»

затверджена Наказом університету від 3 березня 2025 р. № 79/с

Термін здачі студентом закінченої роботи 17 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процеси організації та управління інформаційною інфраструктурою в корпоративному середовищі, що охоплюють автентифікацію, зберігання, передачу даних і централізоване адміністрування ресурсів.

Предметом дослідження є гібридна IT-інфраструктура організації, побудована на базі рішень Microsoft, зокрема технології хмарної інтеграції, методи взаємодії локального та хмарного середовища, засоби синхронізації облікових записів, організація доступу до ресурсів, а також питання забезпечення безпеки, надійності та керованості системи.

Обладнання та програмне забезпечення:

1. Хмарна платформа Microsoft Azure (сервіс Microsoft Entra ID).
2. Гіпервізор Oracle VirtualBox (локально).
3. Операційні системи Windows Server 2022 Datacenter Azure Edition (у публічній хмарі) та Windows Server 2019 Evaluation Edition (локально).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор Фальковський	03.03.2025 	03.03.2025 

Студент  Анастасія Ковтонюк
Керівник  Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025 – 05.03.2025	
2	Написання вступної частини кваліфікаційної роботи	07.03.2025 – 15.03.2025	
3	Аналіз основних теоретичних відомостей технологій інтеграції хмарних та локальних серверів	17.03.2025 – 31.03.2025	
4	Проектування гібридної IT-інфраструктури мережі	01.04.2025 – 10.04.2025	
5	Вибір обладнання та технологій	12.04.2025 – 20.04.2025	
6	Налаштування мережі	22.04.2025 – 24.04.2025	
7	Написання висновків	01.05.2025 – 16.05.2025	
8	Оформлення кваліфікаційної роботи	20.05.2025 – 13.06.2025	
9	Підготовка презентації до захисту	15.06.2025 – 16.06.2025	

Студент  Анастасія Ковтонюк
Керівник  Олена Головня

АНОТАЦІЯ

Пояснювальна записка містить: 87 сторінок текстової частини, 83 рисунка, 12 таблиць та 21 джерело.

Метою кваліфікаційної роботи є розробка проєкту гібридної ІТ-інфраструктури організації для корпоративного середовища на основі рішень Microsoft.

У цій роботі розглянуто теоретичні основи побудови гібридної ІТ-інфраструктури, а також детально проаналізовано особливості використання продуктів Microsoft, зокрема Microsoft Azure, Windows Server та служби Azure Active Directory. Розглянуто концепцію поєднання локального середовища з хмарними сервісами, переваги та виклики такого підходу, включаючи питання безпеки, масштабованості та керованості.

У практичній частині роботи продемонстровано процес розгортання гібридної ІТ-інфраструктури: створення віртуальних машин у хмарі, налаштування служби каталогів Active Directory, синхронізацію з Azure AD за допомогою інструмента Microsoft Entra Connect, а також налаштування політик доступу та зберігання даних за допомогою Azure File Share. Описано етапи конфігурації мережевої взаємодії між локальними машинами та хмарним середовищем, інтеграцію облікових записів та застосування системи централізованого управління.

Результатом проведеного дослідження є проєкт, заявлений у темі роботи, що демонструє побудову сучасної та масштабованої гібридної інфраструктури на базі продуктів Microsoft. Проєкт підтверджує ефективність використання Microsoft Azure та супутніх сервісів для організації безперервного доступу до ресурсів, централізованого управління ІТ-середовищем і захисту корпоративної інформації.

Ключові слова: ХМАРА, ВІРТУАЛЬНА МАШИНА, ГІБРИДНА ІНФРАСТРУКТУРА, ГІПЕРВІЗОР, AZURE.

					KKIK.KP.B – 123 – 05 – ПЗ			
Зм.	Арк.	№ докум.	Піпис	Дата	Проєкт гібридної ІТ-інфраструктури організації на базі продуктів Microsoft	Літ.	Арк.	Аркушів
Розроб.		Ковтонюк А.Д.		16.06.25				
Керівник		Головня О.С.		16.06.25			4	92
Реценз.		Єфіменко А.А.		16.06.25				
Н. контр.		Єфіменко А.А.		16.06.25				
Затверд.		Єфіменко А.А.		16.06.25		ФІКТ, Гр. KI-21-1		

ANNOTATION

The explanatory note contains 87 pages of text, 83 figures, 12 tables, and 21 references.

The purpose of the qualification work is to develop a hybrid IT infrastructure project for a corporate environment based on Microsoft solutions.

This paper discusses the theoretical foundations of building a hybrid IT infrastructure, as well as analyzes in detail the features of using Microsoft products, in particular Microsoft Azure, Windows Server, and Azure Active Directory. The concept of combining the local environment with cloud services, the advantages and challenges of this approach, including security, scalability and manageability, are considered.

The practical part of the paper demonstrates the process of deploying a hybrid IT infrastructure: creating virtual machines in the cloud, setting up Active Directory, synchronizing with Azure AD using Microsoft Entra Connect, and setting up access and storage policies using Azure File Share. The stages of configuring network interaction between local machines and the cloud environment, integrating accounts, and using a centralized management system are described.

The result of the research is the project stated in the work topic, which demonstrates the construction of a modern and scalable hybrid infrastructure based on Microsoft products. The project confirms the effectiveness of using Microsoft Azure and related services to organize continuous access to resources, centralized management of the IT environment, and protection of corporate information.

Keywords: CLOUD, VIRTUAL MACHINE, HYBRID INFRASTRUCTURE, HYPERVISOR, AZURE.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ГІБРИДНОЇ ІТ-ІНФРАСТРУКТУРИ	10
1.1 Хмарна та гібридна ІТ-інфраструктура.....	10
1.2 Огляд моделей надання хмарних послуг та хмарних платформ	17
1.3 Огляд віртуалізації серверів	29
1.4 Постановка технічного завдання	33
РОЗДІЛ 2 ПРОЄКТУВАННЯ ІТ-ІНФРАСТРУКТУРИ	34
2.1 Аналіз вимог до ІТ-інфраструктури організації.....	34
2.2 Вибір хмарного сервісу та інструментів	38
2.3 Розробка архітектури інфраструктури на базі Microsoft Azure	49
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ГІБРИДНОЇ ІТ-ІНФРАСТРУКТУРИ НА БАЗІ ПРОДУКТІВ MICROSOFT	53
3.1 Підготовка середовища для розгортання гібридної інфраструктури	53
3.2 Інтеграція локального середовища з Microsoft Azure.....	70
3.3 Створення спільних ресурсів та файлової інфраструктури	75
3.4 Безпека, моніторинг та резервне копіювання.....	79
ВИСНОВКИ	87
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	88
ДОДАТКИ	90

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD DS – Active Directory Domain Services

ОС – операційна система

MS – Microsoft

СКБД – система керування базами даних

S2D - Storage Spaces Direct

AWS - Amazon Web Services

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Гібридна ІТ-інфраструктура, яка поєднує локальні ресурси з хмарними сервісами – це надзвичайно важлива складова сучасного цифрового середовища. В час стрімкого розвитку технологій, зростання обсягу даних, підвищених вимог до гнучкості, безпеки та доступності інформаційних систем, впровадження гібридної моделі інфраструктури дозволяє організаціям ефективно масштабувати ресурси, оптимізувати витрати та забезпечити безперервність бізнес-процесів.

Рішення Microsoft, такі як Azure, Windows Server, Active Directory, Azure AD Connect та Azure File Share, відкривають нові можливості для реалізації централізованого управління, автоматизації адміністрування, розподіленого зберігання даних і гнучкого контролю доступу. Гібридна інфраструктура дозволяє об'єднати переваги локальних систем з функціональністю хмарних технологій, що актуальні для компаній, які прагнуть до цифрової трансформації при збереженні контролю над критичними даними.

Впровадження гібридного підходу це відповідь на виклики, які пов'язані з кібербезпекою, надійністю сервісів, нормативними вимогами та необхідністю швидкого реагування на зміну бізнес-умов. Такий підхід також сприяє побудові масштабованої, стійкої та ефективної ІТ-інфраструктури.

Метою кваліфікаційної роботи є розробка проєкту гібридної ІТ-інфраструктури організації для корпоративного середовища на основі рішень Microsoft.

Визначена мета обумовлює наступні завдання.

- Аналіз сучасних підходів до побудови гібридних ІТ-інфраструктур.
- Розробка архітектури гібридної інфраструктури з використанням Microsoft Azure та локального середовища.
- Налаштування ключових компонентів гібридної інфраструктури (Azure AD, локальний AD, Azure File Share тощо).
- Тестування роботи гібридної інфраструктури.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Об’єктом дослідження є процеси організації та управління інформаційною інфраструктурою в корпоративному середовищі, що охоплюють автентифікацію, зберігання, передачу даних і централізоване адміністрування ресурсів.

Предметом дослідження є гібридна ІТ-інфраструктура організації, побудована на базі рішень Microsoft, зокрема технології хмарної інтеграції, методи взаємодії локального та хмарного середовища, засоби синхронізації облікових записів, організація доступу до ресурсів, а також питання забезпечення безпеки, надійності та керованості системи.

У процесі виконання кваліфікаційної роботи було розроблено проект гібридної ІТ-інфраструктури організації для корпоративного середовища, який включає підбір та налаштування відповідних сервісів Microsoft, реалізацію взаємодії між локальним і хмарним середовищами.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ГІБРИДНОЇ ІТ-ІНФРАСТРУКТУРИ

1.1 Хмарна та гібридна ІТ-інфраструктура

У сучасному світі бізнес все частіше використовує гібридне середовище, де хмарні сервіси взаємодіють з локальними ресурсами. Підключення локальної інфраструктури до хмари розширює її можливості, дозволяючи ефективно керувати обчислювальними ресурсами, базами даних та іншим. Продумана інтеграція робить процес управління простішим та дозволяє швидко масштабувати ресурси відповідно до потреб організації.

Хмарні технології – це набір технологій, які дозволяють обробляти дані, а також використовувати різноманітні ІТ-ресурси (віртуальні машини, процесорна потужність, оперативна пам'ять, дискове сховище та інше) через інтернет, без необхідності в серверному обладнанні.

Існує чотири основні типи розгортання хмари (рис. 1.1):

1. Публічна хмара (public cloud)
2. Приватна хмара (private cloud)
3. Гібридна хмара (hybrid cloud)
4. Хмара спільноти (спільна хмара, community cloud)

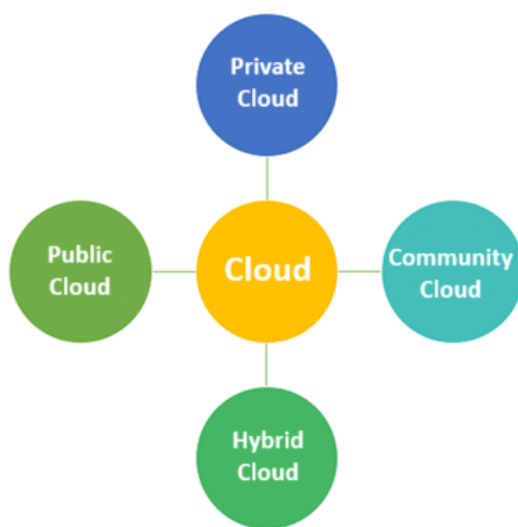


Рисунок 1.1. – Типи розгортання хмари

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Громадська хмара

Публічна хмара – це модель, у якій сторонній постачальник володіє обчислювальними ресурсами та робить ці ресурси доступними для користувачів (рис. 1.2). Передплата за таку хмару цілком поширена, але існують і безкоштовні публічні хмарні сервіси.

Вони пропонують додаткові інструменти, які допомагають користувачам отримати набагато більше від своєї хмарної архітектури, включаючи хмарні програми, сховище даних тощо.

Це модель на вимогу, де сторонній постачальник хмарних послуг може надавати індивідуальні послуги відповідно до потреб користувача. В той же час провайдери можуть об'єднувати ресурси для задоволення потреб великої групи користувачів. Переваги та недоліки публічної хмари наведено у табл. 1.1.

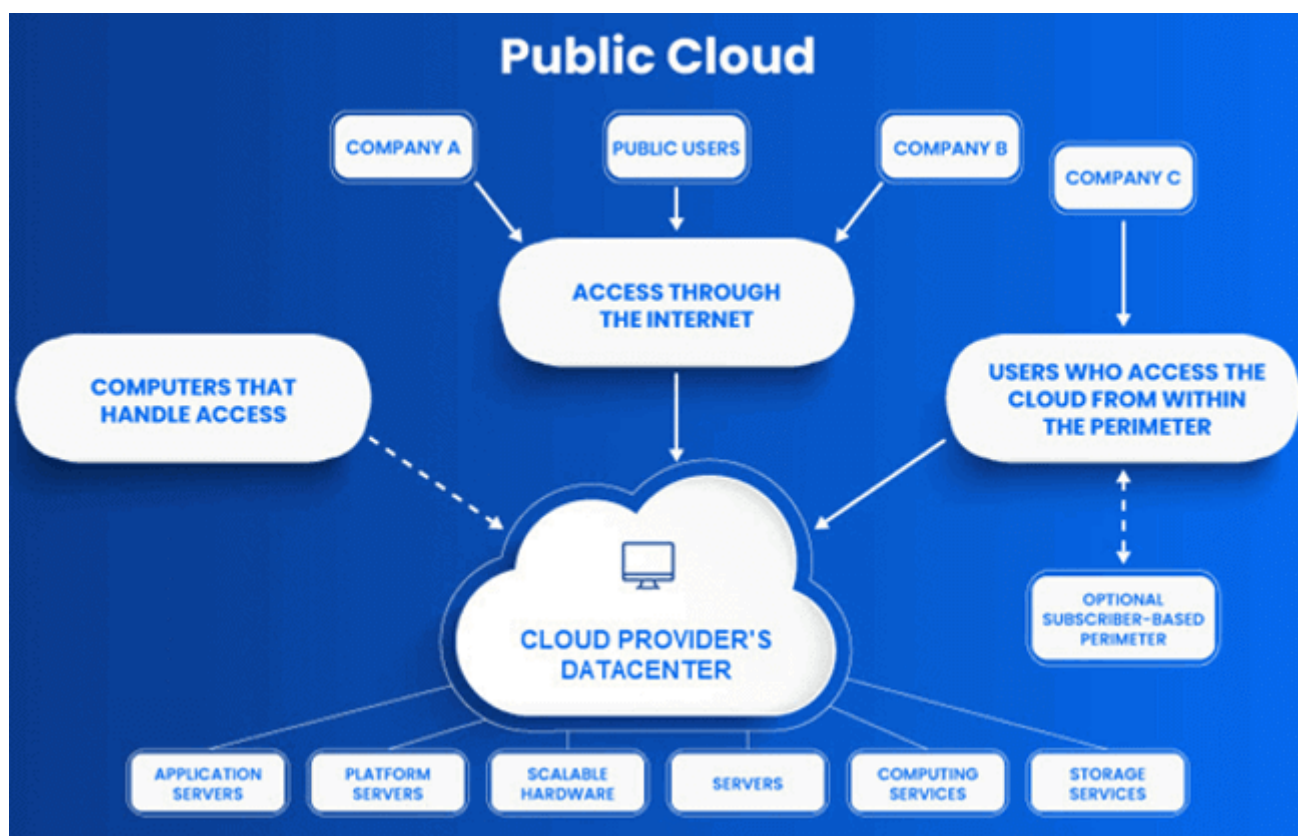


Рисунок 1.2. – Публічна хмара

Таблиця 1.1

Переваги та недоліки публічної хмари

Переваги	Недоліки
----------	----------

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

- | | |
|---|---|
| <ul style="list-style-type: none"> • Користувачі можуть додавати або видаляти ресурси за потреби. • Об'єднані ресурси допомагають знизити витрати, а більшість постачальників мають гнучкі моделі ціноутворення. • Вбудовані рішення для резервного копіювання – це полегшення відновлення. • Загальнодоступні хмарні середовища є життєздатним рішенням для компаній з обмеженими ІТ-командами та внутрішніми ресурсами. • Великі компанії, як Amazon, Microsoft, Google, пропонують надійні публічні хмарні послуги та інноваційні бізнес-рішення. | <ul style="list-style-type: none"> • Покладаючись на стороннього постачальника хмарних технологій, ви отримаєте мінімальну видимість внутрішнього процесу. • Не ідеально підходить для ресурсомістких програм, які потребують виділених серверів для належної роботи. • Не підходить для організацій, які мають особливі вимоги щодо конфіденційності даних. |
|---|---|

Приватна хмара

Приватна хмара передбачає, що ресурсами у хмарі розпоряджається лише організація, якій належить ця хмара (рис. 1.3). Таким чином, приватна хмара має переваги локального хостингу, водночас надаючи доступ до гнучкості хмарної архітектури. Це гнучка модель, у якій організація може самостійно вирішувати, яку частину архітектури треба передати аутсорсингу.

Ця модель хмарних обчислень використовується виключно певною організацією і ніколи не передається іншим організаціям. Деякі постачальники хмарних послуг також пропонують послуги з керування приватними хмарами, включаючи розгортання програм, безпеку, оновлення та інші аспекти керування ІТ-інфраструктурою.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

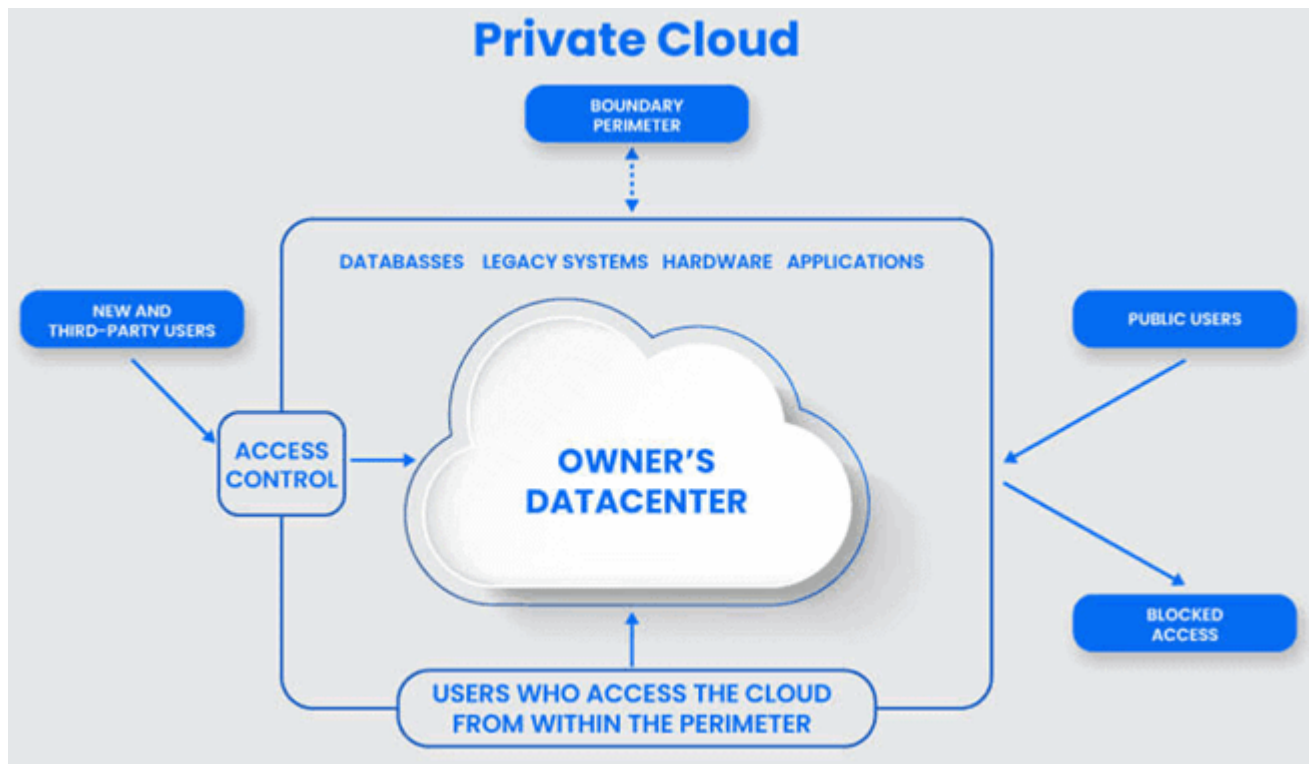


Рисунок 1.3. – Приватна хмара

Інфраструктура приватної хмари добре підходить для компаній, які повинні відповідати суворим галузевим вимогам щодо обробки даних і конфіденційності. Це гарантія, що ресурсомісткі програми мають обчислювальні ресурси, необхідні для роботи належним чином. Переваги та недоліки приватної хмари подано у табл. 1.2.

Таблиця 1.2.

Переваги та недоліки приватної хмари

Переваги	Недоліки
- Самостійне керування програмним та апаратним забезпеченням. - Немає обмеження щодо кількості або типу програм, які можна розгорнути в приватній хмарі. - Організація може захистити своє хмарне середовище брандмауером та іншими засобами, якими	- Архітектура приватної хмари передбачає значні початкові витрати, якщо ви купуєте обладнання для хостингу. - Створення приватної хмарної інфраструктури може бути складним через велику кількість доступних варіантів.

організація керує самостійно. Володіння апаратним забезпеченням хмарної архітектури може підвищити оцінку бізнесу та захистити від потенційних коливань цін на підписку.	
---	--

Гібридна хмара

Модель розгортання гібридної хмари використовує публічні та приватні елементи інфраструктури (рис. 1.4). Це гнучка модель, яка дозволяє використовувати переваги обох моделей розгортання.

Гібридне середовище може допомогти скоротити витрати, якщо потреби та вимогу відрізняються від одного процесу до іншого. Конфіденційні дані, застарілі системи та програми, які потребують конфігурації, яка не підтримується постачальником послуг на основі публічної хмари, можуть залишатися в приватній частині архітектури. Робочі навантаження, які вимагають більшої пропускної здатності та SaaS-рішень, можуть працювати на загальнодоступному хмарному сервері.

Публічні та приватні елементи інфраструктури обмінюються даними за потреби.

В наш час все більше компаній використовують гібридну хмару. Багато з цих компаній покладаються на сторонніх постачальників програм, які не вимагають розширених заходів безпеки чи спеціального середовища. Переваги та недоліки гібридної хмари підсумовано у табл. 1.3.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

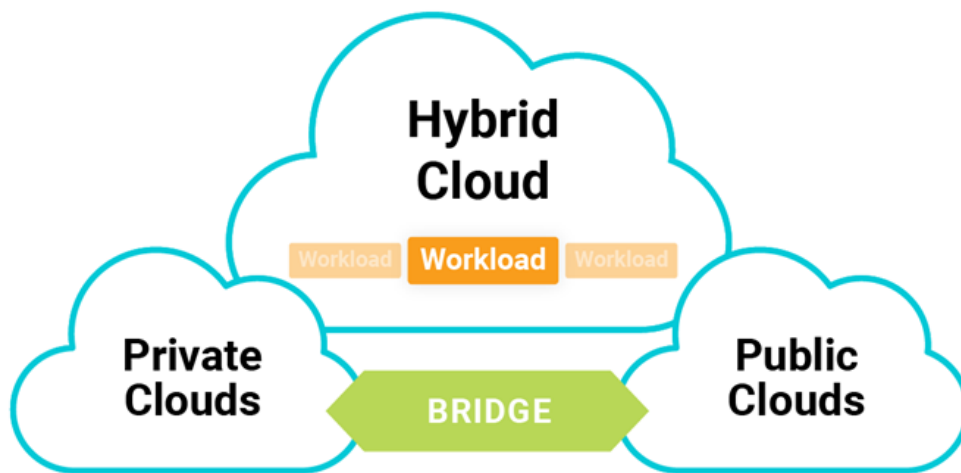


Рисунок 1.4. – Гібридна хмара

Таблиця 1.3.

Переваги та недоліки гібридної хмари

Переваги	Недоліки
• Полегшує перехід від приватної до загальнодоступної хмари та навпаки. • Скорочує час розгортання та дозволяє використовувати публічні ресурси для додавання нових можливостей до ІТ-інфраструктури. • Масштабована гібридна хмара надає доступ до більшої кількості публічних ресурсів за потреби. • Не потрібно йти на компроміс із безпекою чи нормативними вимогами.	• Гібридна інфраструктура може стати складною в управлінні, якщо потрібно керувати великою кількістю елементів. • Керування приватною частиною архітектури може бути дорогим.

Хмара спільноти

Ця модель схожа на публічну хмару, але вирішує проблеми, пов'язані із впровадженням універсальної моделі для кількох різних організацій, які об'єднують спільні вимоги, потреби, процедури, інтереси тощо (рис. 1.5).

Хмарний постачальник створює середовище, яке відповідає унікальним потребам, налаштовуючи конфігурацію сервера, впроваджуючи рішення з кібербезпеки або дотримуючись певних вимог до зберігання даних.

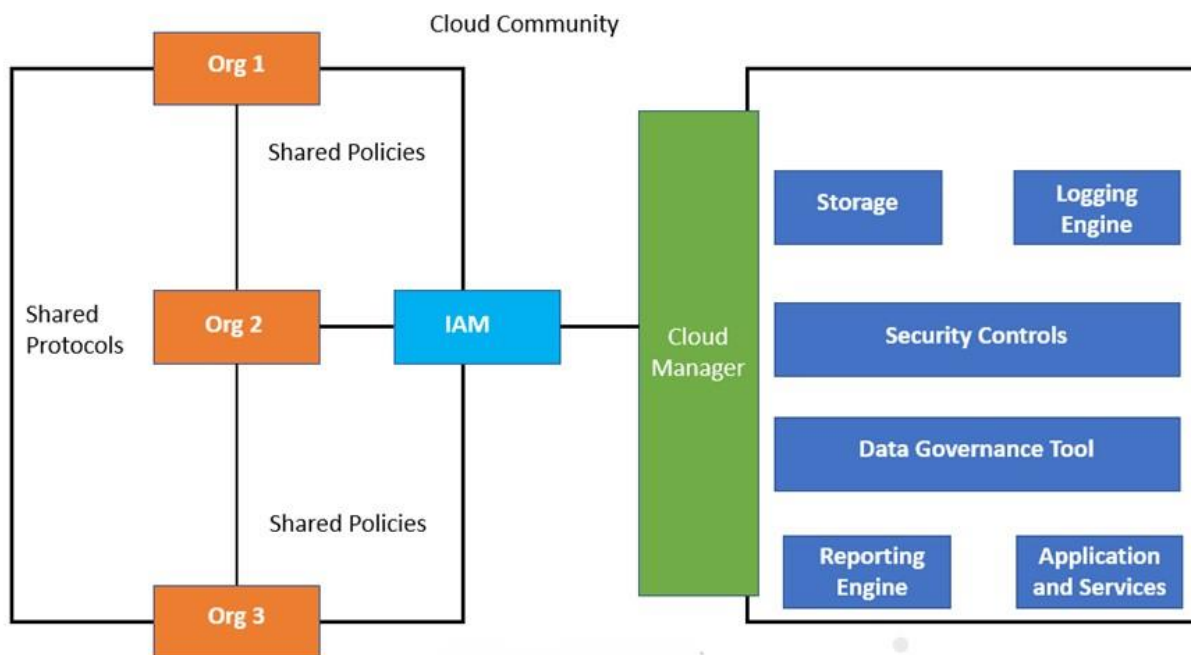


Рисунок 1.5. – Хмара спільноти

Популярність цієї моделі хмари продовжує набирати популярність, тому знайти рішення, яке відповідає потребам стане легше. Підприємства в таких галузях, як фінанси, страхування, охорона здоров'я або юридична сфера вже можуть вибирати з широкого спектру хмарних рішень спільноти. Переваги та недоліки хмари перелічено у табл. 1.4.

Таблиця 1.4.

Переваги та недоліки хмари спільноти

Переваги	Недоліки
Надає більше видимості та контролю над хмарним середовищем,	Не всі постачальники пропонують цю модель.

ніж публічна хмара. • Хмара спільноти сумісна з гібридною архітектурою, якщо потрібно зберегти деякі елементи моделі приватної хмари. • Є змога зменшити витрати, передавши відповідність вимогам своєму постачальнику хмарних послуг. • Хмарний постачальник задовольнить унікальні потреби та вимоги галузі.	• Його ціна вища порівняно з традиційним публічним хмарним рішенням.
---	--

Отже, існує чотири основні типи хмарних обчислень. Інфраструктура загальнодоступної хмари підходить, якщо скорочення витрат є пріоритетом. Вона залишається найбільш масштабованим рішенням. Приватна модель має більше сенсу для підприємств із особливими вимогами до безпеки чи конфігурації, але вона коштує дорожче. Інвестуючи в гібридну модель, ви можете використовувати переваги публічної та приватної хмари. Хмарна платформа спільноти може добре підійти, якщо галузь має особливі нормативні вимоги. [2]

1.2 Огляд моделей надання хмарних послуг та хмарних платформ

Як було зазначено вище, хмарні технології є способом надання обчислювальних потужностей як послуги через мережу.

Користувач отримує майданчик, який ще називають хмара, де може робити будь-що: від зберігання фото до побудови власної ІТ-інфраструктури. Це по суті сервер, розташований в центрах обробки даних по всьому світу, доступ до якого здійснюється через інтернет. Користувачу не потрібно самостійно його налаштувати, цим займається постачальник послуг.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Велика кількість сучасних популярних Інтернет-сервісів є також і хмарними сервісами. Раніше вся інформація зберігалася на комп'ютері, а передавалася за допомогою флешки (диску). Згодом з'явилися файлоховища, Dropbox, Google One, Microsoft Office 365. Листування перейшло в Telegram, WhatsApp, а для проведення робочих зустрічей чи приватного спілкування почали використовувати Skype, Zoom тощо. Завдяки хмарним технологіям ви можете відкрити один і той самий файл на різних пристроях одночасно. Або зайти на свою сторінку в соцмережах з нового телефону.

Принцип роботи

Технології віртуалізації лежать в основі роботи хмарних технологій. Вона дозволяє створити змодельований цифровий віртуальний комп'ютер, подібний до фізичного, з власним апаратним забезпеченням. Такий комп'ютер називається віртуальною машиною.

Основні сервісні моделі хмарних технологій

- **SaaS** (програмне забезпечення як послуга). Хмарний провайдер розробляє та обслуговує додатки, програми, розміщує їх у хмарі та надає користувачу через браузер/додаток на ПК. Клієнт може платити за послуги або користуватися ними безкоштовно. Прикладами є Microsoft 365, TikTok, Gmail.

- **PaaS** (платформа як послуга). Постачальник надає все необхідне для створення IT-сервісів: інструменти розробки, інфраструктуру та операційні системи. Приклади — AWS Elastic Beanstalk, OpenShift.

- **IaaS** (інфраструктура як послуга). Провайдер надає ресурси та сховище, які компанія використовує для розміщення, розробки сервісів. Серед провайдерів — Microsoft Azure, Google Cloud, GigaCloud.

Переваги хмарних технологій

- **Більше місця для зберігання даних (потенційно).** Хмарне сховище дозволяє зберігати більше даних, не турбуючись про оновлення та технічну підтримку фізичних накопичувачів.

- **Краща масштабованість.** За потреби, хмара дозволяє гнучко збільшувати та зменшувати кількість оперативної пам'яті, віртуальних машин, дисків тощо.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Організація дистанційної роботи.** Можливість підключення до сервісів з будь-якої точки світу та з будь-якого гаджета.

- **Економія.** Оренда хмарних ресурсів усуває необхідність купувати обладнання та зменшує капітальні витрати. Ці кошти можна спрямувати на розвиток бізнесу та завоювання нових ринків.

- **Резервування та аварійне відновлення.** Існує можливість впровадження рішень для резервного копіювання та відновлення в економічно ефективний спосіб.

Крім того, хмарні технології активно розвиваються, і надалі хмарну інфраструктуру можна розвивати, впроваджуючи у неї сучасні рішення, зокрема наступні.

- **Гібридні та мультихмарні рішення.** Прогнозується [3], що бізнес буде надавати перевагу поєднанню гібридних та мультихмарних інфраструктур, оскільки намагатиметься знайти баланс між гнучкістю, безпекою та контролем.

- **Інтернет речей.** В сучасному світі все більше пристроїв підключається до Інтернету, потреба і надійній, масштабованій хмарі тільки зростатиме. IoT створить величезну кількість даних, які необхідно зберігати і обробляти, а хмара – це зручна платформа для цього.

- **Штучний інтелект.** Зі стрімким розвитком ШІ, бізнес та користувачі все частіше звертаються до хмарних технологій для зберігання та управління своїми даними для ШІ.

- **Безсерверні обчислення.** Цей тренд може докорінно змінити уявлення про хостинг додатків і сервісів. Безсерверні обчислення не мають фізичних серверів, які потрібно обслуговувати.[3]

Для розуміння можливостей та викликів, які пропонують сучасні хмарні платформи, варто здійснити їх порівняння. Серед найпопулярніших провайдерів слід виділити Microsoft Azure, Amazon Web Services (AWS) та Google Cloud Platform (GCP) (рис. 1.6).

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

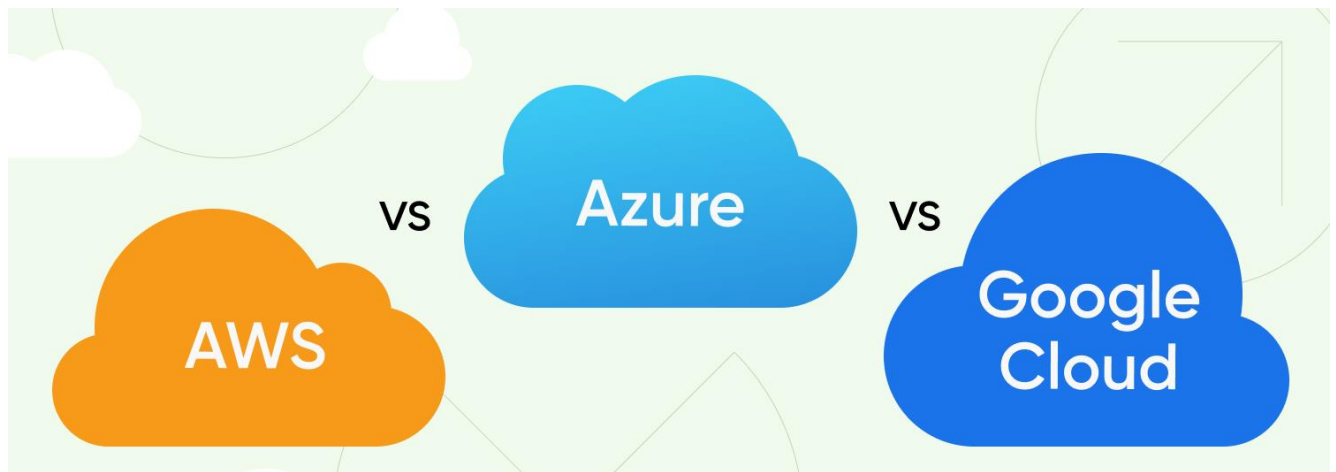


Рисунок 1.6. – Три найпопулярніші хмарні провайдери

Amazon Web Services

Amazon Web Services (AWS) – це комплексна платформа хмарних обчислень, що надається Amazon (рис. 1.7). Пропонує широкий спектр послуг, включаючи обчислювальну потужність, рішення для зберігання даних та бази даних, що дає компаніям можливість масштабуватись та впроваджувати інновації без необхідності значних початкових інвестицій. AWS довіряють мільйони, вона відома своєю надійністю, великою глобальною інфраструктурою та гнучкістю. Вона має велике портфоліо, що налічує понад 200 хмарних сервісів, від обчислювальних та периферійних обчислень до безсерверних рішень. Ключові пропозиції включають Amazon EC2 для обчислень (віртуальні машини), Amazon S3 для еластичного об'єктного сховища, Amazon EBS для мережесхвистових технологій та Amazon Lambda для безсерверних обчислень.

AWS пропонує хмарні сервіси всіх моделей надання послуг за допомогою хмари, зокрема й інфраструктури як послуги (Infrastructure as a Service, IaaS), що становить основний інтерес в межах даної роботи. AWS надає хмарні сервери, мережні, обчислювальні ресурси та ресурси зберігання без необхідності придбання або керування інфраструктурою. [4]



Рисунок 1.7. - Amazon Web Services

Microsoft Azure

Microsoft Azure - це платформа хмарних обчислень з набором служб, що постійно розширюється і також може успішно використовуватися для бізнес-завдань (рис. 1.8). Служби Azure можуть бути простими веб-службами для розміщення вашого бізнесу в хмарі (як модель SaaS) або повністю віртуалізованими комп'ютерами (як модель IaaS) для виконання призначених для користувача програмних рішень. Azure надає безліч хмарних служб, таких як віддалене сховище, розміщення баз даних і централізоване управління обліковими записами. Azure також пропонує нові можливості, такі як штучний інтелект та Інтернет речей.

Azure надає більше 200 служб, що дозволяють вирішувати будь-які завдання: від запуску існуючих додатків в віртуальних машинах до створення інтелектуальних роботів і змішаної реальності. [5]

Однією з причин популярності Azure як платформи для інфраструктури підприємств є спрощення переходу на Azure тих підприємств, які вже використовують такі продукти Microsoft, як Microsoft 365, SQL Server, SharePoint та Power BI. У такому разі інтеграція хмарних сервісів Microsoft стає логічним та ефективним розширенням існуючого технологічного стеку. Це відповідає тенденції, коли ком-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

панії бажають підтримувати свої центри обробки даних, одночасно використовуючи переваги хмари. У цьому контексті Azure стає стратегічним союзником, сприяючи плавному поєднанню локальної інфраструктури з гнучкістю та інноваціями, які пропонує хмара.

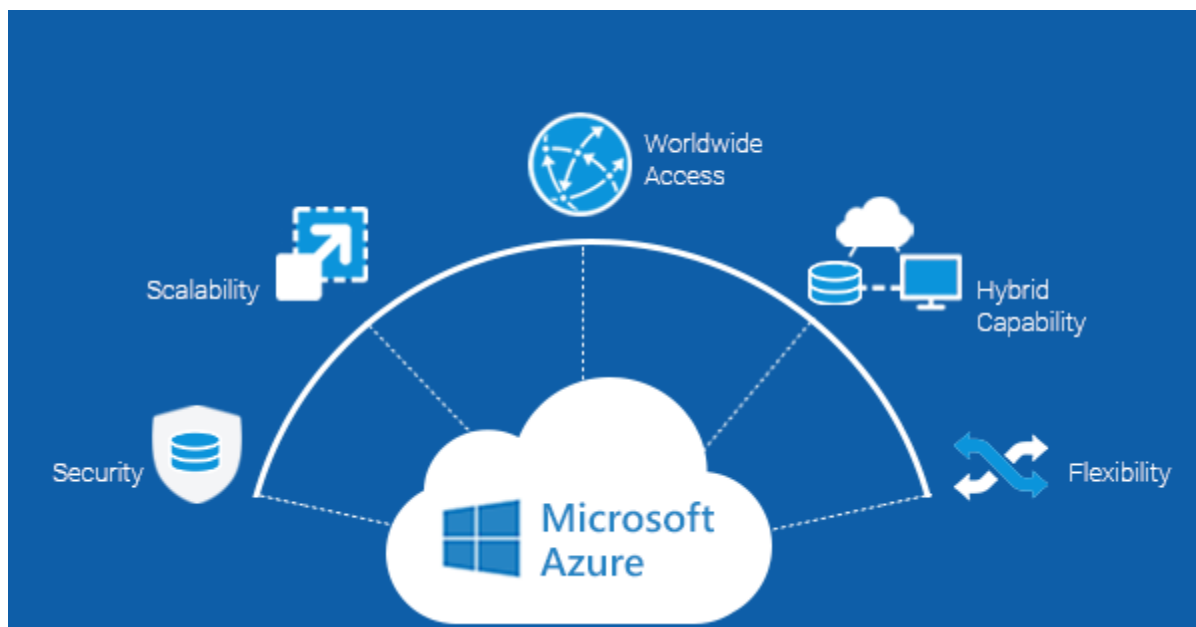


Рисунок 1.8. - Microsoft Azure

Google Cloud

Google Cloud – це набір сервісів хмарних обчислень від Google, призначений для допомоги підприємствам у використанні можливостей даних та інновацій (рис. 1.9). Хмарна платформа Google (далі GCP) з акцентом на аналіз даних, машинне навчання та технології з відкритим програмним кодом, пропонує гнучку та масштабовану інфраструктуру.

Google Cloud відомий своїми передовими можливостями безпеки, які встановлюють галузеві стандарти для надійного захисту даних та систем, а також гібридними та мультихмарними рішеннями, що пропонують значну гнучкість для організацій. GCP також надає рішення для сховищ даних, що дозволяють організаціям ефективно зберігати, керувати та аналізувати величезні обсяги даних. GCP також має інноваційні функції бізнес-аналітики (BI) та машинного навчання (ML). Компанії можуть використовувати ці інструменти для отримання значущої інформації зі своїх даних, прийняття обґрунтованих рішень, або залишатися в авангарді технологічних інновацій.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

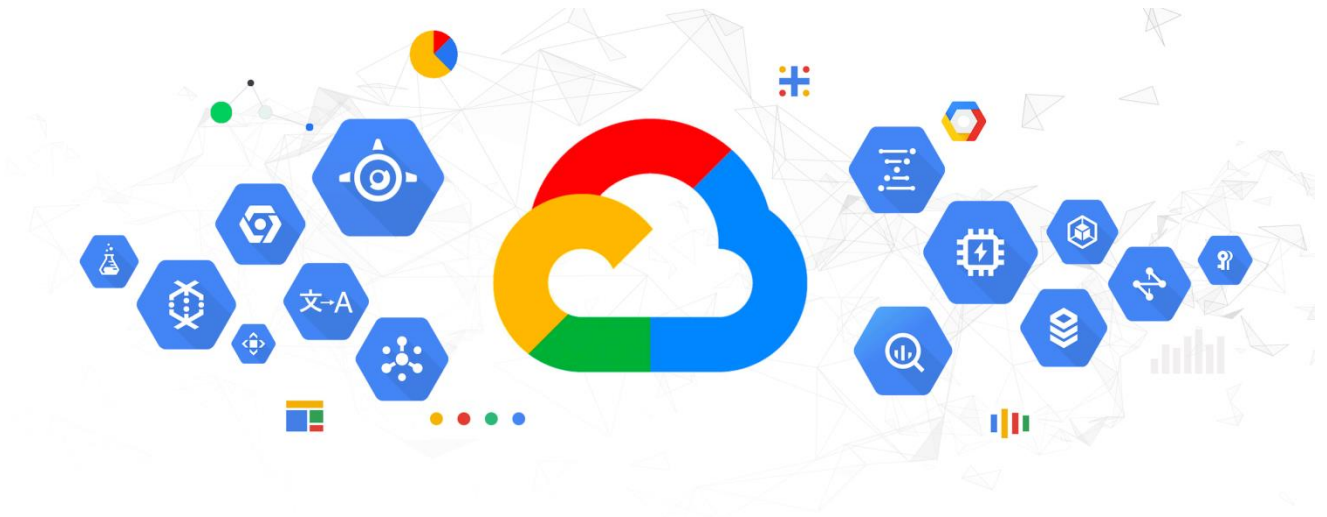


Рисунок 1.9. - Google Cloud

Ключові відмінності між AWS, Microsoft Azure та Google Cloud

Порівняння AWS, Microsoft Azure та Google Cloud передбачає розгляд різних факторів, щоб визначити найкращу платформу, яка задовольняє потреби даного дослідження. Порівняння хмарних провайдерів за роком появи, розмірами, зонами, сервісами, корпоративним використанням та екосистемою наведено в табл. 1.5.

Таблиця 1.5.

Порівняння хмарних провайдерів за роком появи, розмірами, зонами, сервісами, корпоративним використанням та екосистемою

Категорія	AWS	Microsoft Azure	Google Cloud
Місяць та рік появи	Березень 2006 року	1 лютого 2010 р.	Листопад 2011 р.
Регіони	32	47	39
Зони доступності	102	92	118
Частка ринку	22%	10%	33%
Кількість	Понад 200	Понад 200	Понад 150
Корпоративне використання	Високий	Високий	Високий
Екосистема	Хмара	Хмара+Office	Хмара+Google

		365	Workspace+Картти+Google Ads+YouTube+Аналітика
Гібридна хмара	Outpost - HW	AzureStack - HW	GDC - HW+SW, GKE Enterprise - SW
Відкрите джерело	S3, StackDriver	Hi	Kubernetes, Istio, інші
Мультихмара	Hi	Hi	GKE Enterprise

Екосистема послуг. З точки зору екосистеми, Azure та GCP, що знаходяться в авангарді екосистеми, демонструють LDAP та програми для спільної роботи, трохи випереджаючи AWS. GCP, розширюючи межі, інтегрує Google Maps, Ads, YouTube та Analytics у свою велику екосистему, підкреслюючи інновації та комплексні пропозиції послуг.

Гібридна хмара. Багато користувачів хмарних технологій хочуть уникнути прив'язки до постачальника, в цьому їм може допомогти гібридне або мультихмарне середовище. У разі використання AWS та Azure для гібридної хмари, необхідно мати спеціалізоване обладнання. У Google Cloud повний стек програмного забезпечення можна встановити на існуюче обладнання або центри обробки даних і використовувати ту частину GCP, наприклад віртуальні машини, Kubernetes та інші, якими можна буде керувати в Cloud Console.

Відкритий код. Відкритий вихідний код означає впровадження та підтримку технологій з відкритим вихідним кодом на платформах хмарних обчислень, одночасно означаючи, що вихідний код програмної програми вільно доступний користувачам для перегляду, зміни та розповсюдження. Як можна побачити, в той час як AWS та Google Cloud пропонують інтеграцію та взаємодію з різними технологіями з відкритим вихідним кодом у рамках конкретних сервісів, Azure не дуже відкритий, і реалізувати деякі сторонні інструменти в Microsoft Azure складніше. Однак, Azure тісно інтегрується з такими продуктами Microsoft, як Windows Server, Active Directory та Visual Studio, що і потрібно для виконання цієї роботи.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Мультихмара. Лише Google Cloud за допомогою GKE Enterprise дозволяє клієнтам керувати кількома кластерами не тільки в Google Cloud або локально, але й в інших хмарах, наприклад, Azure або AWS. Порівняння хмарних провайдерів за пропонованими сервісами обчислювальних потужностей надано в табл. 1.6.

Таблиця 1.6.

Порівняння хмарних провайдерів за пропонованими сервісами обчислювальних потужностей

Категорія	AWS	Microsoft Azure	Google Cloud
Віртуальні машини	Amazon EC2	Віртуальні машини Azure	Google Compute Engine
Безсерверність	AWS Lambda, FarGate	Azure Functions, ACI	Cloud Functions, AppEngine, Cloud Run
Контейнер	Amazon ECS, FarGate	ACI	GKE, Cloud Run, GKE Enterprise
Спотові інстанси	Спотові інстанси	Віртуальні машини з низьким пріоритетом	Спотові інстанси
VMWare	Маркетплейс	Маркетплейс	Вбудований
Індивідуальні віртуальні машини	Вибрані типи	Вибрані типи	Усі типи загального призначення

Віртуальні машини та спотові інстанси. Кожен постачальник хмарних послуг пропонує широкий спектр пропозицій. Amazon Lambda стала піонером у галузі безсерверних обчислень, Google Cloud з того часу розвинувся з ширшим спектром можливостей. Спотові віртуальні машини (функція, спільна для всіх провайдерів) демонструють перевагу в економічній ефективності GCP, ціна якого становить лише частину вартості AWS або Azure.

VMWare. В рамках інтеграції VMWare Google Cloud має рішення, яке легко вбудовується в платформу. AWS та Azure пропонують рішення VMWare через торгові майданчики, хоч і з меншим ступенем інтеграції.

Індивідуальні віртуальні машини. Індивідуальні віртуальні машини відносяться до створення екземплярів віртуальних машин з конкретними конфігураціями. В Amazon та Azure вони доступні, але лише на деяких вибраних типах віртуальних машин. У GCP спеціальні машини доступні на всіх типах машин загального призначення, що дозволяє користувачам GCP адаптувати специфікації віртуальних машин відповідно до конкретних вимог своїх робочих навантажень, будучи набагато ефективнішими і часто заощаджуючи десятки відсотків витрат на обчислювальну потужність.

Таблиця 1.7.

Порівняння хмарних провайдерів за пропонованими базами даних та аналітичними функціями

Категорія	AWS	Microsoft Azure	Google Cloud
Реляційність	MySQL, Postgres, Maria DB, Oracle, MS SQL	MS SQL, Mongo, Posgres, Maria, MySQL, Cassandra	Cloud SQL, Spanner, Alloy DB
Non-SQL	Dynamo DB	Cosmos DB, Azure Table Storage	Big Table
In-Memory	ElastiCache для Redis, Memcache	Azure Cache для Redis	Memorystore (Redis, Cluster)
Документ	Document DB (Mongo)	Cosmos DB	FireBase+Development Env
Граф	Neptune	Cosmos DB (Gremlin)	Neo 4j
PetaByte Scaling DB	Amazon Dynamo D	Cosmos DB	Spanner, Alloy DB, BigTable

База даних	Redshift	Synapse	BigQuery + ML
Бізнес аналітика	QuickSight	Power BI	Looker, Looker Studio, Looker Studio Pro

Бази даних масштабування у петабайтах. Існують варіанти баз даних на всіх трьох платформах. Різниця виникає лише тоді, коли йдеться про бази даних з петабайтним масштабуванням, які розроблені та оптимізовані для обробки надзвичайно великих обсягів даних, що вимірюються у петабайтах. У той час як AWS та Azure пропонують надійні варіанти керування петабайтними даними за допомогою баз даних NoSQL, Google Cloud пропонує Spanner та Alloy в реляційних базах даних та Big Table в базах даних NoSQL. Порівняння хмарних провайдерів за пропонованими базами даних та аналітичними функціями подано в табл. 1.7.

Вибір між цими платформами залежатиме від конкретних вимог, існуючої архітектури та переваг таких функцій, як глобальне поширення, моделі узгодженості та простота використання. Зокрема, GCP Spanner часто хвалять за його можливості глобального розповсюдження та узгодженість транзакцій у масштабі.

Аналітика даних. Всі три хмарні гіганти – GCP, AWS і Azure – досягають успіху в області великих даних, прогнозованої аналітики та озер даних штучного інтелекту. AWS та Azure пропонують спеціалізовані студії машинного навчання; студія Azure дуже зручна для користувача і вимагає менше технічних знань, ніж Amazon SageMaker.

Однак, хоча Reshift та Synapse є відмінними стандартними сховищами даних, GCP виділяється вбудованими можливостями штучного інтелекту та машинного навчання, додаючи інтелект у всі аспекти, від додатків до обробки даних. Відмінним прикладом може бути корпоративне сховище даних BigQuery, яке також є рішенням озера даних із вбудованим машинним навчанням, тому ви можете створювати моделі машинного навчання за допомогою SQL без використання інших мов програмування, що справді спрощує вашу бізнес-аналітику даних.

Таблиця 1.8.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Порівняння хмарних сервісів за вартістю, системою тарифікації та контролем бюджету

Категорія	AWS	Microsoft Azure	Google Cloud
Управління витратами	AWS Cost Explorer	Azure Cost Management and Billing	Google Cloud Console Billing
Система тарифікації та контроль бюджету	AWS Billing and Cost Management Console	Azure Cost Management and Billing Portal	Google Cloud Console Billing
Рекомендації щодо вибору розміру	Так	Так	Так
Зрозумілість рахунків	Дуже низький	Низький	Високий

AWS, Azure та GCP пропонують структуру оплати по мірі використання із зарезервованими екземплярами для економії коштів. Всі три хмарні провайдери надають клієнтам комплексний інструмент з тарифікації, управління витратами та рекомендаціями за розмірами. В цілому, всі платформи мають свої плюси і можуть бути обрані організацією залежно від її потреб. AWS пропонує безкоштовну низку рішень для нових користувачів, Microsoft Azure Cost Management надає користувачам інструменти для оптимізації витрат, GCP пропонує конкурентоспроможну цінову модель із знижками при тривалому використанні та індивідуальними типами машин. Порівняння хмарних сервісів за вартістю, системою тарифікації та контролем бюджету наведено в табл. 1.8.

Отже, усі три основні постачальники хмарних послуг, AWS, Azure та GCP, пропонують надійні послуги, що робить їх найкращими варіантами на ринку хмарних обчислень. При виборі між Azure, Google Cloud і AWS, такі чинники, як доступність регіону, екосистема сервісів, можливості гібридної хмари, обчислення, сховище, аналітика та інші послуги відіграють вирішальну роль. Зрештою вибір

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

між AWS, Azure та GCP залежить від конкретних бізнес-потреб, уподобань та існуючих стеків технологій.[4]

1.3 Огляд віртуалізації серверів

Віртуалізація серверів - це технологія, яка дає змогу одному фізичному серверу функціонувати як кілька віртуальних серверів. Ці віртуальні сервери, відомі як віртуальні машини (virtual machines, VM), можуть працювати незалежно один від одного та імітувати окремі фізичні сервери.

Переваги віртуалізації серверів (порівняно з фізичними серверами)

- **Ефективне використання ресурсів.** Віртуалізація дає змогу запускати кілька віртуальних машин на одному фізичному сервері, що збільшує використання обчислювальних ресурсів і зменшує кількість невикористовуваних ресурсів.

- **Ізоляція та безпека.** Віртуальні машини можуть працювати незалежно одна від одної, що забезпечує ізоляцію ресурсів і підвищує безпеку. У разі проблеми з однією віртуальною машиною, інші залишаються в безпеці.

- **Гнучкість і масштабованість.** Віртуалізація забезпечує гнучкість в управлінні ресурсами. Можна легко змінювати обсяг виділених ресурсів для кожної віртуальної машини залежно від вимог.

- **Спрощене управління.** Віртуалізація надає інструменти для зручного управління та моніторингу віртуальних машин. Це спрощує процеси встановлення, оновлення та обслуговування.

- **Економія енергії та простору.** Запуск декількох віртуальних машин на одному фізичному сервері дає змогу заощаджувати енергію та зменшує необхідність у великій кількості фізичних серверів, що також заощаджує місце в дата-центрі.

- **Швидке відновлення та резервне копіювання.** Віртуалізація спрощує процеси резервного копіювання та відновлення віртуальних машин, що підвищує надійність системи.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

- **Тестування.** Віртуалізація забезпечує можливість створення копій віртуальних машин для тестування нових конфігурацій або розробки додатків без впливу на робоче середовище.

- **Можливості міграції за необхідності.** Багато систем віртуалізації надають інструменти для міграції віртуальних машин між фізичними серверами, що дає змогу балансувати навантаження і забезпечувати безперервну роботу. [6]

Типи віртуалізації серверів

Існують основні три категорії методів віртуалізації.

1. **Повна емуляція** є найпоширенішим типом віртуалізації і передбачає створення повної віртуальної машини, яка емулює всі апаратні ресурси фізичного сервера, включно з процесором. Прикладом використання повної емуляції є QEMU.

2. **Квазі-віртуалізація** — це більш спеціалізована форма віртуалізації, яка не емулює всі апаратні ресурси фізичного сервера. Натомість вона дає змогу кільком віртуальним машинам спільно використовувати одні й ті самі апаратні ресурси, як-от процесор і пам'ять, надаючи інтерфейс віртуалізації для гостьових операційних систем. Цього можна досягнути за допомогою **динамічної трансляції** (dynamic translation, full virtualization), **паравіртуалізації** (paravirtualization) чи поєднання цих методів. Паравіртуалізація вимагає модифікації гостьової операційної системи, а динамічна трансляція цього не потребує.

3. **Віртуалізація на основі контейнерів** — це тип віртуалізації, який створює кілька ізольованих екземплярів користувацького простору, відомих як контейнери, що використовують одне й те саме ядро операційної системи хоста. Кожен контейнер виглядає як окремий сервер зі своєю файловою системою, мережевими інтерфейсами та IP-адресами. Така віртуалізація потребує менше ресурсів порівняно з іншими типами віртуалізації, що робить її ідеальною для веб-додатків, мікросервісів і хмарних додатків. [7]

Принцип роботи та ключові поняття віртуалізації

Віртуальні машини та гіпервізори – це дві важливі концепції віртуалізації.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Віртуальна машина – це зімітований комп’ютер, що працює на фізичному комп’ютері з окремою операційною системою та обчислювальними ресурсами. Фізичний комп’ютер називається хост-машиною, а віртуальні машини – гостьовими машинами. На одній фізичній машині може працювати кілька віртуальних машин. Віртуальні машини абстрагуються від апаратного забезпечення комп’ютера за допомогою гіпервізора.

Віртуальні машини використовуються для:

- **Ознайомлення з іншими операційними системи.** Незалежно від того, яка ОС є основною на комп’ютері, у VirtualBox можна встановити будь-яку іншу, яка є підтримуваною: численні дистрибутиви Linux, FreeBSD, macOS, будь-яку з версій Windows, Android тощо. Така інсталяція не шкодить реальній системі та не призводить до втрати важливих даних, тому що віртуальна машина працює ізольовано. Коли ВМ вже не потрібна, її можна видалити.

- **Запуск програм, які не працюють у основній ОС або її версії.** Наприклад, головна ОС на комп’ютері це Windows, а користувачеві знадобився застосунок, який доступний лише у Linux, саме в таких випадках на допомогу приходить віртуальна машина.

- **Тестування програмного забезпечення.** Іноді виникає необхідність скористатися певною програмою або протестувати новий застосунок, але немає бажання ризикувати основною операційною системою. На допомогу приходить VirtualBox. [8]

Гіпервізор – це програмний компонент, що керує віртуальними машинами на комп’ютері. Гіпервізор відповідає за те, щоб кожна віртуальна машина отримувала виділені їй ресурси та не заважала роботі інших віртуальних машин. Існує два основні типи гіпервізорів.

Гіпервізори першого типу, також відомі як гіпервізори, виконувані на “голому залізі” (bare-metal hypervisors) – це програми-гіпервізори, встановлені безпосередньо на апаратному забезпеченні комп’ютера, а не як ПЗ в операційній системі. Вони мають більш високу продуктивність і зазвичай використовуються в кор-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

поративних додатках. Наприклад, KVM використовує гіпервізор першого типу для хостингу кількох віртуальних машин операційної системи Linux.

Гіпервізори другого типу працюють як додаток на комп'ютерному обладнанні з операційною системою. Гіпервізори другого типу підходять для обчислювальних можливостей кінцевих користувачів. Прикладами гіпервізорів другого типу є Oracle VirtualBox, Vmware Workstation та Fusion.

Чим віртуалізація відрізняється від хмарних обчислень?

Як згадувалося у розділі 1, хмарні обчислення (хмарні технології) – це доставка обчислювальних ресурсів на вимогу через Інтернет із оплатою за фактом використання. Замість купівлі, обслуговування фізичних центрів обробки даних та володіння ними клієнт отримує доступ до технологічних сервісів, таких як обчислювальні потужності, сховища та бази даних через постачальників хмарних сервісів у міру необхідності.

Технології віртуалізації є основою реалізації хмарних обчислень. Постачальники хмарних послуг створюють та обслуговують власні центри обробки даних. Вони створюють різні віртуальні середовища, які використовують базові апаратні ресурси. Доступ до цих об'єднаних ресурсів надається клієнтам у межах різних хмарних сервісів. Клієнт також може розгорнути хмару на власних апаратних ресурсах, але тоді йому знадобиться самостійно підтримувати її роботу. [9]

Порівняння хмарних інстансів та віртуальних машин

Поняття «інстанс» та «віртуальна машина» часто використовуються як одне і те саме, особливо коли йдеться про хмарні обчислення. Однак між ними існують відмінності. Програмна симуляція реального комп'ютера називається віртуальною машиною. Подібно до реального комп'ютера, вона запускає операційну систему (ОС) та програми. Програмне забезпечення для віртуалізації створює віртуальні машини (virtual machines, VM), що дозволяє працювати багатьом віртуальним машинам на одному фізичному комп'ютері (хості).

Інстанс (instance) є віртуальним сервером у хмарі, який зазвичай забезпечується та керується хмарним провайдером. Хоча інстанси та віртуальні машини (VM) ідентично запускають операційні системи та програми, інстанси зазвичай

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

створюються з використанням попередньо налаштованих хмарних образів та шаблонів, які надає хмарний провайдер. Інстанси керуються через API або хмарну консоль управління і є частиною ширшої хмарної інфраструктури.

1.4 Постановка технічного завдання

На основі аналізу теоретичних відомостей про побудову IT-інфраструктури, віртуалізації, особливостей серверного ядра та хмарних технологій, було сформоване технічне завдання на розробку гібридної IT-інфраструктури для корпоративного середовища з використанням продуктів Microsoft.

Гібридна хмарна інфраструктура має забезпечувати безперервну роботу корпоративних IT-сервісів шляхом поєднання локального середовища на базі Windows Server та хмарної платформи Microsoft Azure. Дана система повинна забезпечувати централізоване управління користувачами за допомогою Active Directory, синхронізацію облікових записів із хмарною службою Azure AD, реалізацію файлового сховища Azure File Share та підтримку розгортання віртуальних машин у хмарному середовищі. Передбачено використання Windows Server як тестової платформи, що дає змогу оцінити функціональні можливості інфраструктури до її повноцінного впровадження. Усі компоненти повинні правильно функціонувати, взаємодіяти між собою, мати базовий захист та бути придатними для масштабування відповідно до потреб.

Висновок до першого розділу

У першому розділі розглянуто теоретичні відомості про хмарну та гібридну IT-інфраструктуру, де було здійснено порівняння приватної, публічної, гібридної хмари та хмари спільноти. Розглянуто моделі надання хмарних послуг та хмарних платформ, описано ключові характеристики Amazon Web Service (AWS), Microsoft Azure та Google Cloud. Детально розглянуто поняття «віртуалізація серверів», його принцип роботи та ключові поняття віртуалізації. Таким чином, у результаті ознайомлення з теоретичними відомостями було закладено основу для подальшої реалізації проекту гібридної IT-інфраструктури на базі продуктів Microsoft.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 2 ПРОЄКТУВАННЯ ІТ-ІНФРАСТРУКТУРИ

2.1 Аналіз вимог до ІТ-інфраструктури організації

Аналіз вимог до ІТ-інфраструктури є критичним етапом у процесі створення та оптимізації інформаційних систем організації. Цей процес визначає ключові потреби бізнесу, технічні характеристики, а також основні обмеження, які необхідно враховувати під час проєктування інфраструктури. Визначення цих вимог допомагає забезпечити масштабованість та надійність системи, ефективність.

Одна з перших задач це розуміння бізнес-потреб організації. ІТ-інфраструктура має відповідати загальній стратегії компанії, а також підтримувати її головні процеси. Наприклад, компанія планує розширювати ринок та запускати нові продукти, тоді інфраструктура повинна бути здатною масштабуватися, щоб підтримувати зростання обсягу даних та користувачів. Організації, які надають послуги, можуть потребувати високої доступності сервісів і мінімальний час простою.

Аналіз вимог до продуктивності включає оцінку необхідної обчислювальної потужності, обсягу пам'яті та пропускну здатності мережі. Це особливо важливо для компаній, що працюють з великими даними, інтенсивними обчисленнями або високонавантаженими веб-додатками. Важливо також враховувати, як система поводитиметься під час пікових навантажень, щоб уникнути збоїв і втрат продуктивності. Паралельно аналізується потенційний обсяг даних, який необхідно зберігати, обробляти і передавати, а також швидкість доступу до цих даних.

Важливою складовою є оцінка вимог до безпеки. Сучасні кіберзагрози стають усе складнішими, тому ІТ-інфраструктура повинна забезпечувати захист конфіденційної інформації, відповідати вимогам законодавства щодо зберігання даних та включати засоби для виявлення і нейтралізації загроз. Для цього організації використовують багаторівневий підхід, що включає апаратні й програмні засоби захисту, такі як міжмережеві екрани, системи виявлення вторгнень, шифрування даних та управління доступом. Також варто передбачити механізми резервного копіювання і відновлення даних у разі втрати чи пошкодження.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Ще одним ключовим аспектом є вимоги до надійності та доступності системи. Для багатьох організацій неперервна робота ІТ-сервісів є критично важливою, оскільки простої можуть призводити до фінансових втрат або негативного впливу на репутацію. Тому важливо передбачити використання резервного обладнання, систем аварійного відновлення та географічно розподілених центрів обробки даних. Інструменти моніторингу та управління інфраструктурою забезпечують оперативне виявлення проблем і дозволяють швидко на них реагувати.

Гнучкість і масштабованість інфраструктури є ще одним важливим фактором.

Змінювані бізнес-вимоги вимагають від ІТ-систем здатності до швидкої адаптації без значних витрат. Для досягнення цієї мети організації все частіше звертаються до використання хмарних технологій, які забезпечують можливість швидкого збільшення обчислювальних потужностей або обсягів сховищ за потреби. Крім того, хмарні сервіси дозволяють оптимізувати витрати завдяки моделі оплати “за використання”.

Вимоги до сумісності та інтеграції також відіграють важливу роль у проектуванні ІТ-інфраструктури. Система повинна безперебійно взаємодіяти з уже існуючими додатками, базами даних та обладнанням. Це вимагає використання стандартних протоколів, відкритих API та модульної архітектури, яка полегшує оновлення та розширення функціональності. Наприклад, інтеграція з ERP- або CRM-системами може стати критичною для забезпечення ефективності бізнес-процесів.

Економічна ефективність є ще одним важливим критерієм під час аналізу вимог. ІТ-інфраструктура повинна забезпечувати оптимальне співвідношення між вартістю її розгортання, обслуговування та отриманими перевагами. Це включає як прямі витрати на обладнання, програмне забезпечення та оплату хмарних сервісів, так і непрямі витрати, пов'язані з навчанням персоналу чи забезпеченням технічної підтримки.

Крім того, аналіз вимог до ІТ-інфраструктури включає врахування екологічних аспектів. Використання енергоефективного обладнання та впровадження те-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

хнологій, які зменшують вплив на навколишнє середовище, стають дедалі важливішими для багатьох організацій. Це не лише відповідає сучасним трендам сталого розвитку, а й дозволяє зменшити операційні витрати.

Під час аналізу також розглядаються аспекти управління та моніторингу. Інфраструктура повинна включати засоби для централізованого управління, автоматизації рутинних задач та створення звітів для оцінки ефективності. Використання інструментів, таких як системи управління конфігураціями, дозволяє мінімізувати людський фактор і знизити ймовірність помилок.

Отже, аналіз вимог до ІТ-інфраструктури — це комплексний процес, який охоплює технічні, організаційні, економічні та екологічні аспекти. Врахування всіх цих факторів дозволяє створити систему, яка максимально відповідає потребам організації, забезпечує її розвиток і конкурентоспроможність на ринку.

Отже, перше, що потрібно зробити компанії, яка планує впровадити хмарні технології - це детальне визначення потреб та очікувань. Воно включає наступні заходи.

- **Оцінювання бізнес-цілей.** Необхідно визначити проблеми та задачі компанії, які будуть вирішені за допомогою хмарних рішень. Наприклад, оптимізація витрат, масштабування ІТ-інфраструктури, підвищення продуктивності, відмовостійкості тощо.

- **Аналіз потреб користувачів.** Потрібно з'ясувати, які програми та сервіси співробітники використовують найчастіше і які є необхідними для них. Це може передбачати розширення можливостей взаємодії з ними, доступ до програм на віддалених робочих місцях або покращення захисту даних.

- **Аудит наявних ІТ-ресурсів.** Варто провести детальний аналіз існуючого програмного та апаратного забезпечення, щоб визначити, чи відповідає воно вимогам для майбутньої інтеграції. Це допоможе уникнути дублювання рішень або помилок під час переходу.

Коли цілі інтеграції будуть чітко визначені, можна переходити до оцінювання поточного ІТ-ландшафту компанії. На цьому етапі необхідно дослідити, як побудована поточна ІТ-інфраструктура, зокрема за допомогою наступних заходів.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

- **Інвентаризація програмного забезпечення та систем.** Важливо скласти повний перелік програм, сервісів та додатків, що використовуються в компанії: CRM, ERP, бухгалтерські програми, електронна пошта, таск-менеджери тощо. Це дозволяє визначити, які системи можуть бути перенесені в хмару, а які потребують доопрацювання.

- **Аналіз продуктивності та стабільності.** Оцінювання ефективності роботи наявних систем чи витримують вони навантаження та чи є проблеми з їхнім масштабуванням.

- **Інформаційна безпека.** Перевірка поточних заходів безпеки та відповідність стандартам, наприклад GDPR або ISO, має велике значення, оскільки безпека є одним із ключових аспектів під час міграції у хмару.

Після проведення аналізу наявної інфраструктури компанія повинна визначити основні процеси та завдання, які потребують інтеграції з хмарними рішеннями. Це стає у пригоді для правильного планування майбутньої ІТ-інфраструктури та уникнення можливих труднощів. Ключові аспекти:

- **Визначення пріоритетів інтеграції.** Оцінка критично важливих бізнес-процесів допомагає зрозуміти, що необхідно перенести в хмару в першу чергу. Наприклад, це може бути CRM-система, яка потребує швидкого доступу до даних із будь-якої точки світу, або аналітичні інструменти для ухвалення стратегічних рішень.

- **Оцінка складності інтеграції.** Не всі системи можуть легко інтегруватися з хмарними рішеннями. Варто детально вивчити технічні обмеження кожної системи, щоб врахувати їх під час міграції.

- **Планування масштабування та відмовостійкості.** Хмарні обчислення дають змогу швидко масштабувати ресурси та забезпечувати їхню доступність. Компанія повинна чітко розуміти, які сервіси потребують підвищеної надійності та резервного копіювання, щоб уникнути простоювання або втрати даних. [1]

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

2.2 Вибір хмарного сервісу та інструментів

У цьому підрозділі розглядається вибір хмарного сервісу, операційної системи, програмного забезпечення та гіпервізору для створення ефективної робочої ІТ-інфраструктури. Основна увага приділяється сервісам, за допомогою яких буде зроблена інтеграція між звичайним сервером та комп'ютерами.

Вибір хмарного сервісу. У таблиці 2.1. наведено результати порівняння хмарних сервісів Microsoft Azure, AWS та GCP. В процесі порівняння враховано можливість створення віртуальних машин, наявність сховища даних, наявність хмарних баз даних, можливість інтеграції з продуктами Microsoft, безпека та підтримка різних ОС.

Таблиця 2.1.

Порівняння хмарних сервісів

Хмар- ний сер- віс	Створення віртуаль- них машин	Схови- ще да- них	Хмар- ні бази даних	Інтеграція з продук- тами Mi- crosoft	Безпе- ка	Підтрим- ка різних ОС
Microsoft Azure	+	+	+	+	+	+
Amazon Web Ser- vices	+	+	+	-	+	+
Google Cloud Platform	+	+	+	-	+	+

Для реалізації частини інфраструктури було обрано Microsoft Azure. Хмарний сервіс є багатофункціональним рішенням і перевагою в ньому є інтеграція з продуктами Microsoft, які будуть задіяні в подальшій реалізації.

Microsoft Azure є однією з найбільших хмарних платформ, вона обслуговується понад 160 дата-центрами та зростає з кожним роком, використовується різ-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

ними компаніями для абсолютно різних завдань. Одні компанії, реалізуючи стратегію розвитку внутрішніх бізнес-процесів, обирають шлях розміщення своєї інфраструктури за моделлю IaaS. Інші компанії зосереджені на створенні програмного забезпечення, різних додатків і використовують Azure за моделлю SaaS.

Існує багато сценаріїв використання платформи MS Azure. Різноманітність сервісів, їх постійний розвиток, поява нових, максимальне забезпечення захисту даних дозволяють Azure займати лідируючі позиції.

Azure використовують як платформу для створення або розміщення інфраструктури. Використовують модель IaaS – інфраструктура як сервіс. Платформа має велику кількість віртуальних машин, типів сховищ та видів каналів зв'язку для забезпечення високих робочих навантажень, а найголовніше – легко і швидко масштабовану інфраструктуру. [10]

Платформа орієнтована на різні категорії користувачів. Розробники можуть використовувати Azure для створення тестових середовищ і запуску додатків на різних операційних системах. Системні адміністратори застосовують платформу для налаштування серверних систем і відпрацювання сценаріїв відновлення після аварій. Тестувальники отримують змогу проводити комплексні перевірки додатків у різних конфігураціях, забезпечуючи високу якість кінцевого продукту. Навчальні заклади використовують Azure для підготовки студентів у сферах роботи з хмарними технологіями та програмним забезпеченням.

Крім того, Azure підтримує гібридні середовища через технології, такі як Azure Arc, що дозволяє об'єднувати локальні та хмарні ресурси в єдину інфраструктуру. Це забезпечує безперервність бізнес-процесів і гнучкість управління системами. Завдяки багатофункціональності, високому рівню безпеки та інтеграції з іншими сервісами Microsoft, Azure є універсальним рішенням для компаній, які прагнуть оптимізувати свої ІТ-ресурси.

Вибір локального гіпервізора. У таблицях 2.2. і 2.3. наявні результати порівняння гіпервізорів VMware vSphere, Microsoft Hyper-V, Oracle VM VirtualBox, Citrix Hypervisor (XenServer), KVM (Kernel-based VM). Під час порівняння враховано підтримку основної ОС (host OS) і гостьової ОС (guest OS), вартість (мініма-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

льна/безкоштовно), продуктивність, масштабованість, інтерфейс управління, інтеграція з хмарою, резервне копіювання.

Таблиця 2.2.

**Порівняння гіпервізорів
за підтримкою ОС, вартістю та продуктивністю**

Гіпервізор	Підтримка основної ОС (host OS) і гостьової ОС (guest OS)	Вартість	Продуктивність
VMware vSphere	Гіпервізор I типу, який підтримує тільки гостьову ОС (guest OS)	-	+
Microsoft Hyper-V	Гіпервізор I типу, але при цьому має й основну ОС – Windows. Працює на рівні апаратного забезпечення.	+/-	+
Oracle VM VirtualBox	Гіпервізор II типу, який підтримує основну ОС (host OS) та гостьову ОС (guest OS)	-	+
Citrix Hypervisor (XenServer)	Гіпервізор I типу, який підтримує тільки гостьову ОС (guest OS)	+ (є платні функції)	+
KVM (Kernel-based VM)	Гіпервізор I типу (є частиною ядра Linux), який підтримує тільки гостьову ОС (guest OS)	+	+

Таблиця 2.3.

Порівняння гіпервізорів за масштабованістю, інтеграцією з хмарою та резервним копіюванням

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Гіпервізор	Масштабованість	Інтеграція з хмарою	Резервне копіювання
VMware vSphere	+	+	+
Microsoft Hyper-V	+	+	+
Oracle VM VirtualBox	+/-	+	+
Citrix Hypervisor (XenServer)	+/-	+	+
KVM (Kernel-based VM)	+	+	+

Після порівняння гіпервізорів для даної роботи було обрано Oracle VM VirtualBox. VMware vSphere платний, для KVM (Kernel-based VM) потрібна Linux, Citrix Hypervisor (XenServer) - гіпервізор I типу, який підтримує тільки гостьову ОС (guest OS), Microsoft Hyper-V має необхідність встановлення додаткового програмного забезпечення.

VirtualBox — це гіпервізор II типу, що дає користувачеві можливість встановлювати, запускати й використовувати інші операційні системи, як звичайні застосунки.

Віртуальна машина створює ізольоване середовище на комп'ютері з віртуальних компонентів реального ПК: жорсткого диска, відеокарти, різних контролерів пристроїв, оперативної пам'яті.

Oracle VM VirtualBox підтримує інтеграцію з іншими інструментами віртуалізації та платформами, що робить його універсальним рішенням для користувачів із різними вимогами. Його відкритий вихідний код дозволяє спільноті користувачів і розробників регулярно оновлювати та вдосконалювати продукт. Завдяки своїй безкоштовності, простоті та широким можливостям VirtualBox є відмінним вибором для розробників, системних адміністраторів, тестувальників і навчальних закладів. Це програмне забезпечення забезпечує ефективність і гнучкість у створенні, налаштуванні та управлінні віртуальними середовищами, що робить його

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

популярним інструментом як для особистого, так і для професійного використання.

Вибір серверної операційної системи

Ubuntu – популярний дистрибутив Linux, який має настільну та серверну версії. Ubuntu працює швидко та поставляється безкоштовно, а також дозволяє підключати додаткові пристрої до системи.

Встановити і налаштувати Ubuntu дуже легко. Понад 20 мільйонів користувачів працюють з Ubuntu. Нові релізи постійно випускаються як з довгостроковою підтримкою (Ubuntu LTS), так і з короткостроковою підтримкою.

Переваги Ubuntu

- **Стабільність роботи.** Система часто використовується на високонавантажених серверах, тому ОС не вимагає частих перезавантажень, навіть у разі оновлень або встановлення та видалення програм.

- **Безкоштовна ОС.** Установка відбувається за декілька хвилин, в мережі є багато версій для безкоштовного завантаження, не потребує ключів та може використовуватися на безлічі комп'ютерів одночасно.

- **Передбачуваність системи.** Кожен новий реліз виходить з періодичністю 6 місяців.

Однією з важливих причин встановлення Ubuntu є те, що ця система має менше відомих вразливостей, ніж, наприклад, Windows Server. Ubuntu можна використовувати як окрему ОС, так і в комбінації з іншою ОС на пристрої.

Недоліки Ubuntu

- Не всі розробники ПЗ орієнтовані на Ubuntu, тому деякі програми не підтримуються.

- Щоб перенести дані з іншої ОС на Ubuntu, часто немає спеціальних інструментів, які б спростили цей процес. [11]

Windows Server – лінійка серверних ОС від Microsoft. Комп'ютер, на якому встановлена така ОС може виконувати ролі файлового сервера, сервера служби веб-додатків, сервера терміналів, поштового сервера, сервера віддаленого доступу, служби DNS або служби каталогів.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Windows Server швидка та надійна ОС. Платформа додатків забезпечує надійність, а інтегроване середовище доступності і безпеку інформації.

ОС легко розгорнути і провести її адміністрування. Вона дає можливість управляти мережею за допомогою політик і автоматизації виконання завдань.

В наш час багато локальних мереж об'єднані з екстрамережами та веб-вузлами. У зв'язку з цим вимоги до безпеки системи різко зросли. Сучасні ОС Windows Server ретельно перевіряються на наявність слабких місць і точок помилок.

Багато особливостей Windows Server дають можливість співробітникам організації працювати більш продуктивно. Файловими ресурсами дозволяють керувати файлові служби та служби друку. Служба каталогів називається Active Directory. Ця служба допомагає зберігати відомості про мережеві об'єкти, крім того, вона допомагає адміністратору швидко знайти цю інформацію. Ця служба також спрощує роботу з проєктування, розгортання та управління каталогами мережі. [12]

Сервери Microsoft мають вищу початкову вартість, оскільки вимагають попередньої оплати ліцензії. Вартість залежить від версії та кількості користувачів, що може призвести до значних витрат великих організацій.

Важливо враховувати загальну вартість володіння (total cost of ownership, TCO) у довгостроковій перспективі. Це включає такі фактори, як обслуговування, підтримка і оновлення.

Windows Server є надійним та інтуїтивно зрозумілим варіантом для організацій, які покладаються на додатки Microsoft і потребують послідовної та надійної платформи. Водночас він може бути досить дорогим і вразливим до кібератак. [13]

Windows Server включає розширені функції віртуалізації, які реалізуються через Hyper-V, що забезпечує створення та управління віртуальними машинами з високою продуктивністю і масштабованістю. Це дає змогу ефективно використовувати апаратні ресурси та швидко відновлювати роботу в разі збоїв. Додатково, операційна система пропонує сучасні мережеві рішення, такі як програмно обу-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

мовлена мережа (software-defines networking, SDN), що дозволяє централізовано керувати мережевими ресурсами, забезпечуючи їх гнучкість і безпеку.

Завдяки інструментам автоматизації, таким як PowerShell, і централізованим інструментам управління, як Windows Admin Center, операційна система забезпечує зручність адміністрування та виконання рутинних завдань. PowerShell дозволяє створювати сценарії для автоматизації процесів і налаштування серверів, тоді як Windows Admin Center забезпечує простий вебінтерфейс для управління інфраструктурою. У результаті Windows Server стає оптимальним вибором для організацій, які шукають надійну платформу для створення сучасної інфраструктури, інтегрованої з хмарними технологіями, що забезпечує високу продуктивність, безпеку та гнучкість.

Windows Server Evaluation Edition – це версія ОС Windows Server, яка надає змогу ознайомитися з функціональними можливостями платформи перед її комерційним використанням. Вона повнофункціональна, але має обмежений період використання, який становить 180 днів, після його закінчення користувач може активувати повну ліцензійну версію. Evaluation Edition створена для організацій, адміністраторів, розробників і технічних фахівців, які хочуть протестувати нові можливості Windows Server у реальних умовах, оцінити продуктивність, сумісність та відповідність своїм бізнес-потребам, але поки не готові платити за це гроші.

Одна із головних переваг Windows Server Evaluation Edition – це доступ до ключового функціоналу ОС без обмежень, які могли б мати вплив на якість тестування. Користувачі отримують повний набір можливостей для створення та управління віртуальними машинами, налаштування мережесервісів, впровадження високодоступних рішень та управління корпоративною інфраструктурою. Ця версія надає організаціям дозвіл на виконання масштабного тестування продуктивності, безпеки та сумісності з іншими продуктами перед тим, як прийняти рішення про купівлю ліцензії.

Одним із ключових аспектів Windows Server Evaluation Edition є її інтеграція з хмарними сервісами Microsoft Azure. Користувачі мають можливість підк-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

лючати локальні сервери до хмарної інфраструктури, створюючи гібридні рішення, які поєднують переваги локальних і хмарних ресурсів. Наприклад, адміністратори можуть використовувати Azure для резервного копіювання, відновлення даних або створення віртуальних серверів для додаткових робочих навантажень. Інтеграція з Azure також дозволяє автоматизувати процеси, спрощувати управління ресурсами та забезпечувати високу доступність додатків.

Враховуючи всі плюси та мінуси, для даної IT-інфраструктури було обрано Windows Server Evaluation Edition.

Для організацій, які прагнуть досягти високої продуктивності, надійності та безпеки, створення IT-інфраструктури на базі серверного ядра є одним із результатів рішень для оптимізації роботи. Серверне ядро пропонує просту та мінімістичну платформу без графічного інтерфейсу, яка призначена для виконання лише основних завдань. Цей метод зменшує обсяг використання системних ресурсів, знижує ризики кіберзагрози та збільшує стабільність цієї системи.

Основа серверного ядра це його вузька спеціалізація, що включає виконання специфічних ролей та сервісів. Однією з найпоширеніших ролей є служба Active Directory Domain Services (AD DS), яка забезпечує централізоване управління ідентифікацією та доступом користувачів у мережі. Також серверне ядро часто використовується для розгортання служб DHCP та DNS, які необхідні для автоматичного налаштування IP-адрес і забезпечення коректної роботи системи доменних імен. Ще один ключовий момент це файловий сервер, який дозволяє централізувати зберігання даних і спростити управління доступом до них.

Доменні служби Active Directory (AD DS) – це основа кожної доменної мережі Windows. AD DS керує базою даних, яка зберігає інформацію про учасників домену, включаючи пристрої та користувачів, перевіряє їхні облікові дані та визначає їхні права доступу. Сервер, на якому виконується ця служба, називається контролером домену (domain controller, DC).

AD DS зберігає інформацію про облікові записи користувачів, такі як імена, паролі, номери телефонів та інше. Це дозволяє іншим авторизованим користувачам у тій же мережі отримувати доступ до цієї інформації.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

AD – власна служба каталогів Microsoft. Вона працює на Windows Server та дозволяє адміністраторам керувати дозволами та доступом до мережевих ресурсів. AD зберігає дані як об’єкти. Об’єкт – це окремий елемент, такий як користувач, група, програма, пристрій, наприклад принтер.

AD DS – це основні функції в Active Directory, які дозволяють керувати користувачами та комп’ютерами, а також надають дозвіл на організацію даних в логічні ієрархії для адміністраторів. AD DS забезпечує сертифікати безпеки, систему єдиного входу (SSO), LDAP і керування правами.

Домен AD є колекцією об’єктів у мережі Microsoft Active Directory. Користувач або група можуть бути окремим об’єктом, або це може бути апаратний компонент, наприклад комп’ютер чи принтер. Кожен домен містить базу даних, що містить інформацію про ідентифікацію об’єкта.

DS створює єдину точку доступу до ресурсів мережі, тому користувачі можуть отримати доступ до AD з будь-якого комп’ютера в даній мережі, якщо це дозволено відповідними налаштуваннями. Це дозволяє ІТ-командам ефективніше співпрацювати та обмежити точки доступу конфіденційними ресурсами. [14]

Ієрархічна структура AD включає наступні компоненти:

- **Домени.** Група об’єктів, таких як користувачі або групи пристроїв, які використовують одну й ту саму базу даних AD, утворює домен.

- **Організаційні одиниці (organizational units, OU).** У межах домену організаційні одиниці використовують для впорядкування об’єктів у межах доменів.

- **Дерева Active Directory.** Кілька доменів, згрупованих разом у логічну ієрархію, утворюють дерево AD. Зв’язки між доменами в дереві називаються відношеннями довіри (trusts relationships, “trusts”).

- **Ліси AD.** Цей функціональний рівень AD складається з кількох дерев, згрупованих разом. Дерева в лісі AD мають спільні довірчі відносини, так само як домени в дереві мають спільні довірчі відношення. Такі відношення дозволяють складовим частинам дерева або лісу спільно використовувати схеми каталогів та специфікації конфігурації.[15]

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Інтеграція з хмарними рішеннями, зокрема Microsoft Azure, є однією з основних переваг серверного ядра.

Вибір операційної системи для хмарного образу

Windows Server 2022 Datacenter Azure Edition – це спеціальна версія Windows Server, створена спеціально для роботи як віртуальна машина Azure IaaS в Azure або як віртуальна машина на кластері Azure Stack HCI. Azure Edition неможливо запускати під керуванням клієнта або Windows Server Hyper-V, а також запускати його на гіпервізорах сторонніх розробників або в хмарних сховищах сторонніх розробників.

Вибір інструментів та додатків

Для повноцінного функціонування IT-інфраструктури, яка базується на інтеграції Microsoft Azure та статичної інфраструктури Active Directory, потрібно обрати відповідні інструменти та додатки.

Інструменти та додатки в Microsoft Azure

1. Azure Active Directory (Azure AD)

Використовується для управління доступом до хмарних сервісів і додатків. Azure AD забезпечує можливості автентифікації, керування обліковими записами та реалізації єдиного входу (SSO). Його можна інтегрувати з локальним Active Directory через Azure AD Connect для створення гібридної ідентифікаційної інфраструктури.

2. Azure Virtual Machines

Дозволяє створювати віртуальні сервери для розгортання додатків, баз даних, сервісів і навіть розширень локальної інфраструктури Active Directory. VM може виступати як додатковий контролер домену.

3. Azure Backup

Цей сервіс забезпечує автоматичне резервне копіювання локальних серверів, віртуальних машин та інших даних, включаючи контролери домену Active Directory.

4. Azure File Storage

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Забезпечує зберігання спільних файлів у хмарі з можливістю підключення через SMB-протокол для локальної інфраструктури Active Directory.

6.Azure Monitor і Log Analytics

Ці інструменти використовуються для моніторингу активності хмарних сервісів і локальної інфраструктури через інтеграцію з Active Directory.

7.Azure Key Vault

Зберігає облікові дані, ключі шифрування та сертифікати для додатків і служб, включаючи ті, які інтегруються з локальним Active Directory.

Інструменти та додатки для локального Active Directory

- Використані в даній роботі:

1.Active Directory Domain Services (AD DS)

Основна служба для управління доменами, обліковими записами користувачів, групами та політиками доступу.

2.Active Directory Certificate Services (AD CS)

Забезпечує централізоване управління сертифікатами для захищених комунікацій і автентифікації.

3.Active Directory Federation Services (AD FS)

Інструмент для реалізації єдиного входу (SSO) до різних додатків, включаючи інтеграцію з Azure AD.

4.Group Policy Management (GPMC)

Використовується для управління політиками безпеки та налаштування середовища користувачів у локальній інфраструктурі.

5.System Center Configuration Manager (SCCM)

Забезпечує централізоване управління пристроями та програмним забезпеченням у домені.

Гібридні інструменти (для інтеграції Azure і локального Active Directory)

- Використані в даній роботі:

1.Azure AD Connect

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Основний інструмент для синхронізації облікових записів між локальним Active Directory та Azure AD.

2. Azure AD Domain Services

Хмарна версія Active Directory, яка дозволяє організаціям використовувати знайомі функції домену (групові політики, LDAP-запити) без потреби в локальній інфраструктурі.

3. Azure Migrate

Інструмент для планування та виконання міграції локальних сервісів у хмару.

- Можуть бути використані в подальшій реалізації:

1. Hybrid Identity Management

Набір функцій для управління ідентичностями в гібридних середовищах. Включає паролісинхронізацію, автентифікацію через AD FS і безпарольний вхід.

5. Microsoft Endpoint Manager

Платформа для управління пристроями та додатками у гібридному середовищі Azure AD і локального домену.

Ці інструменти та додатки забезпечують повноцінну підтримку гібридних сценаріїв, дозволяють ефективно управляти ідентичностями, забезпечують високий рівень безпеки та масштабованості як у хмарній, так і в локальній інфраструктурі. Вибір конкретних рішень залежить від вимог проєкту, обсягів даних, потреб у доступності та рівня автоматизації.

2.3 Розробка архітектури інфраструктури на базі Microsoft Azure

Розробка інфраструктури

На рисунку 2.1. показано схему мережі для проєкту гібридної IT-інфраструктури на базі Microsoft.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

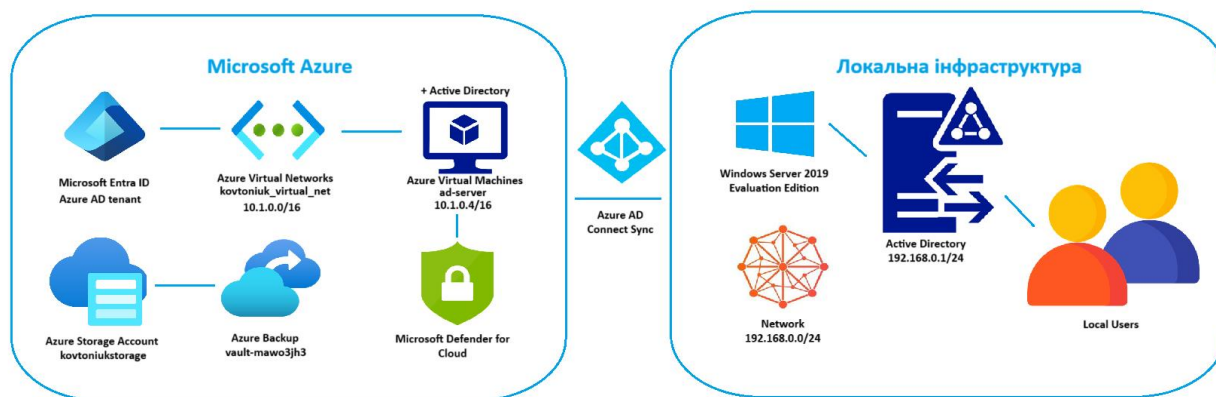


Рисунок 2.1. – Схема мережі

Таблиця 2.4.

Схема адресації

Пристрій	IP-адреса/Маска
Azure Virtual Networks (kovtoni-uk_virtual_net)	10.1.0.0/16
Azure Virtual Machines (ad-server)	10.1.0.4/16
Мережа (локальна)	192.168.0.0/24
Active Directory (локально)	192.168.0.1/24

Ця схема зображає гібридну IT-інфраструктуру на базі продуктів Microsoft.

Локальне підключення:

- Мережа використовує підмережу з IP-адресами у діапазоні 192.168.0.0/24.
- Віртуальна машина має IP-адресу 192.168.0.1/24.

Хмарне підключення:

- Створена віртуальна мережа використовує підмережу з IP-адресами у діапазоні 10.1.0.0/16.
- Віртуальна машина, створена в хмарі, використовує IP-адресу 10.1.0.4/16 з діапазону адрес віртуальної мережі.

Azure AD Connect Sync використовується для інтеграції хмарного середовища та локального. Застосунок Azure AD Connect Sync завантажується на локальну машину та підключається до середовища Azure через облікові дані.

Azure Storage Account потрібно створити для подальшого налаштування резервного копіювання (Azure Backup).

Microsoft Defender for Cloud забезпечує моніторинг подій, які можуть зашкодити хмарному середовищу.

Active Directory (локально) налаштований для створення користувачів, груп та організаційних одиниць в локальному середовищі.

Інтеграція Microsoft Azure з локальним Active Directory є одним із ключових аспектів сучасної IT-інфраструктури на базі Windows-мереж, що дозволяє забезпечити безперервність бізнес-процесів, покращити керування ресурсами та забезпечити високий рівень безпеки. Процес інтеграції цих систем дозволяє об'єднати локальну інфраструктуру з хмарними сервісами Microsoft Azure, що відкриває широкі можливості для організацій будь-якого масштабу.

Основною метою інтеграції локального Active Directory з Azure є забезпечення єдиного централізованого управління ідентифікацією користувачів і доступом до ресурсів як у локальному середовищі, так і в хмарі. Цей процес починається з налаштування служби Azure Active Directory Connect (Azure AD Connect), яка слугує мостом між локальним AD і хмарним Azure AD. Azure AD Connect синхронізує облікові записи користувачів, групи та інші об'єкти, забезпечуючи їх узгодженість між обома середовищами. Це дає змогу користувачам використовувати єдиний набір облікових даних для доступу до всіх необхідних ресурсів.

Однією з головних переваг інтеграції локального Active Directory з Azure є можливість використання хмарних сервісів, таких як Microsoft 365, Azure Virtual Desktop, а також різноманітних SaaS-додатків. Крім того, Azure AD пропонує функції розширеного управління ідентифікаціями, такі як умовний доступ, багатфакторна автентифікація (MFA) і управління ризиками, що значно підвищує загальний рівень безпеки організації. Наприклад, умовний доступ дозволяє створювати гнучкі політики, які контролюють, хто, коли і з яких пристроїв може отримати доступ до корпоративних ресурсів.

Інтеграція Microsoft Azure з локальним Active Directory також надає організаціям можливість використовувати гібридну модель ідентифікації для розподіле-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

них середовищ. Завдяки функції Azure AD Hybrid Identity можна забезпечити безперебійний доступ до локальних і хмарних ресурсів, що особливо важливо для організацій із розгалуженою структурою. Це досягається за рахунок використання одноразового входу (Single Sign-On), який забезпечує зручність для користувачів і спрощує управління доступом для адміністраторів.

Таким чином, інтеграція Microsoft Azure з локальним Active Directory є складним, але надзвичайно важливим процесом, який дозволяє організаціям максимально ефективно використовувати можливості хмарних технологій. Вона не лише забезпечує централізоване управління ідентифікаціями та доступом, але й підвищує рівень безпеки, оптимізує процеси управління ресурсами та відкриває нові перспективи для масштабування бізнесу. Успішна реалізація цієї інтеграції потребує ретельного планування, належної підготовки та використання передових інструментів, які пропонує Microsoft.

Висновок до другого розділу

У другому розділі було проведено аналіз вимог до IT-інфраструктури організації, визначено ключові функціональні, технічні та безпекові аспекти, які повинні бути враховані при побудові IT-інфраструктури. Було здійснено обґрунтований вибір хмарного сервісу Microsoft Azure як основної платформи для реалізації гібридної інфраструктури. Розглянуто сервіси Microsoft, такі як Azure Active Directory, Azure File Share, віртуальні машини, служби зберігання та безпеки. У межах підрозділу з розробки архітектури запропоновано цілісну модель гібридної IT-інфраструктури, в якій поєднані локальні ресурси на базі Windows Server із хмарними компонентами, забезпечуючи взаємодію через Azure AD Connect Sync. Враховані принципи надійності, продуктивності, безпеки та гнучкого управління. Отже, другий розділ сформував основу для реалізації практичної частини, в якій буде здійснено налаштування та тестування ключових компонентів.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ГІБРИДНОЇ ІТ-ІНФРАСТРУКТУРИ НА БАЗІ ПРОДУКТІВ MICROSOFT

3.1 Підготовка середовища для розгортання гібридної інфраструктури

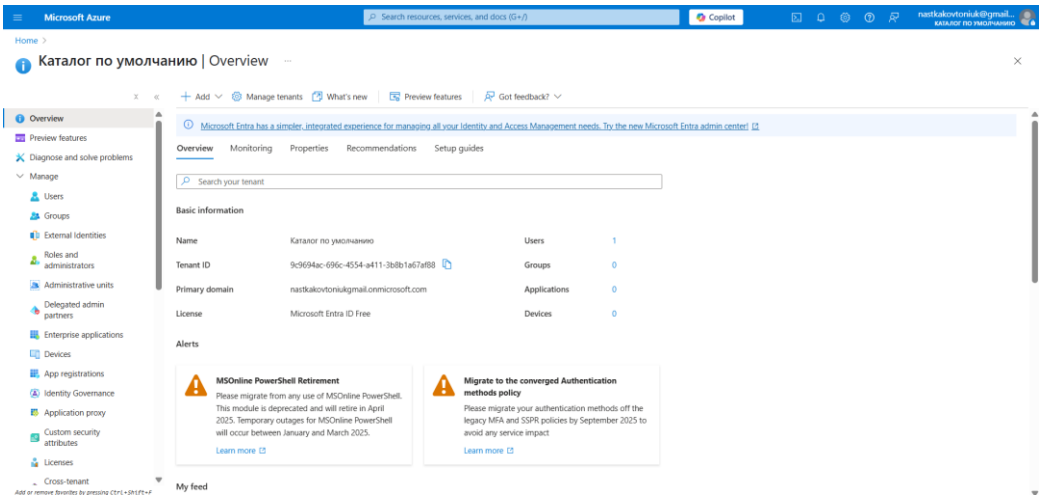
Створення Microsoft Entra ID

Основою моделі корпоративної інфраструктури є Microsoft Entra ID (попередня назва - Azure AD).

Microsoft Entra ID (раніше відомий як Microsoft Azure Active Directory або Azure AD) – це хмарне рішення для керування ідентифікацією та доступом (IAM). Це служба керування каталогами та ідентифікацією (див. додаток А), яка працює в хмарі та пропонує послуги автентифікації та авторизації для різних служб Microsoft , таких як Microsoft 365, Dynamics 365, Microsoft Azure та сторонніх служб. Entra ID надає користувачам можливість єдиного входу, незалежно від того, чи є їхні програми хмарними чи локальними.

Entra ID пропонує різні методи автентифікації (див. додаток А), включаючи автентифікацію на основі пароля, багатофакторну, за допомогою смарт-картки та сертифіката. Вона також підтримує кілька розширених функцій безпеки, таких як політики умовного доступу, автентифікація на основі ризиків та захист ідентифікаційних даних. [16]

Обліковий запис організації в MS Entra ID називається **тенант (tenant)**, що також може бути перекладене як **орендар**. Для того, щоб його створити в меню потрібно обрати Microsoft Entra ID та обрати створення нового тенанту (tenant) (рис. 3.1).



		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.1. – Результат створення тенанта (tenant)

Після створення нового орендаря, маємо тільки одного користувача – глобального адміністратора, але для перевірки належного функціонування потрібно створити ще декілька користувачів різними способами.

Перший спосіб найлегший – звичайне створення користувача, де йому надається ім'я користувача (User principal name), відображуване ім'я (Display name) та його пароль (рис. 3.2).

The screenshot shows the 'Create new user' page in the Microsoft Azure portal. The page has a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, there is a breadcrumb trail: 'Home > Каталог по умовчанию | Overview > Users >'. The main heading is 'Create new user' with a subtitle 'Create a new internal user in your organization'. There are four tabs: 'Basics' (selected), 'Properties', 'Assignments', and 'Review + create'. A note states: 'Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more'. Under the 'Identity' section, there are several fields: 'User principal name' (user), 'Mail nickname' (user), 'Display name' (user), and 'Password' (auto-generated). The 'Account enabled' checkbox is checked. The domain is 'nastkakovtoniukgmail.com'.

Рисунок 3.2. – Створення звичайного користувача

Також, можна запрошувати інших користувачів, які будуть гостями, знаючи їхню електронну адресу (рис. 3.3). Потрібно ввести електронну адресу, відображуване ім'я та повідомлення, яке гість побачить, коли йому на пошту прийде запрошення (рис. 3.4).

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Users >

Invite external user

Invite an external user to collaborate with your organization

Basics

Properties

Assignments

Review + invite

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating. [Learn more](#)

Identity

Email *

ki211_kad@student.ztu.edu.ua

Display name

ki211_kad

Invitation message

Send invite message☒

Message

please join my group

Cc recipient

Invite redirect URL *

https://myapplications.microsoft.com/?tenantid=9c9694ac-696c-4...

Рисунок 3.3. – Запрошення користувача

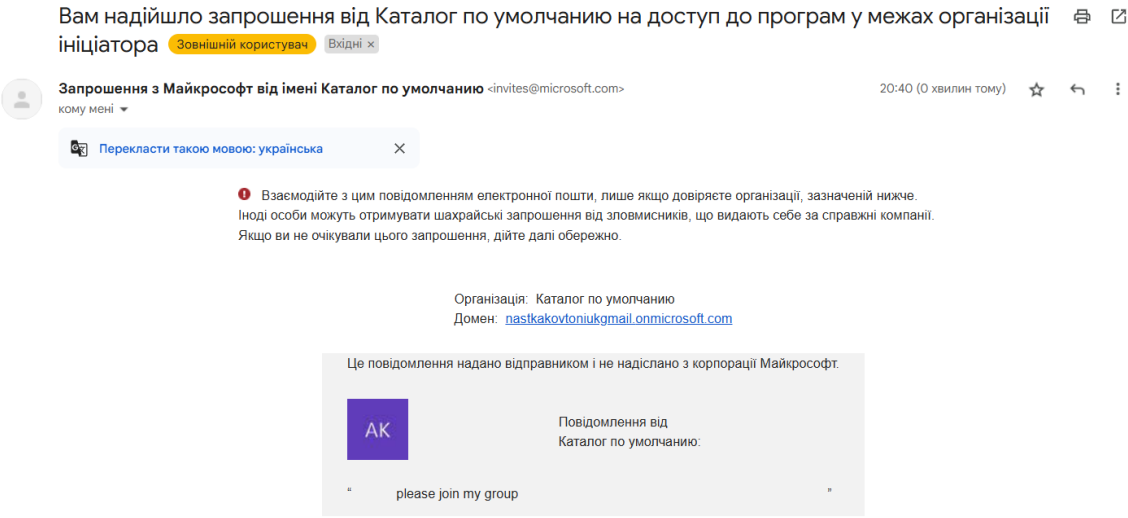


Рисунок 3.4. – Запрошення, яке прийшло на пошту

Як результат створення та запрошення користувачів, можна побачити їх всіх у вкладці «Користувачі» (рис. 3.5).

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

nastkakovtoniuk@gmail.com
КАТАЛОГ ПО УМОВЧАНИЮ

Home >

Users

Каталог по умовчанию

+ New user

Edit (Preview)

Delete

Download users

Bulk operations

Refresh

Manage view

Per-user MFA

Got feedback?

All users

Azure Active Directory is now Microsoft Entra ID

Search

Add filter

4 users found

	Display name	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
☐	Anastasia Kovtoniuk	nastkakovtoniuk_gmail.co...	Member	No	MicrosoftAccount		
☐	ki211_kad	ki211_kad_student.ztu.ed...	Guest	No	nastkakovtoniukgmail.onmicros...		Invitation
☐	nastka	nastka@nastkakovtoniuk...	Member	No	nastkakovtoniukgmail.onmicros...		
☐	user	user@nastkakovtoniukgm...	Member	No	nastkakovtoniukgmail.onmicros...		

Рисунок 3.5. – Вкладка «Користувачі»

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

Після створення користувачів необхідно створити групи безпеки (рис. 3.6 – 3.7), в які згодом вони будуть додані (рис. 3.8 – 3.9).

Microsoft Azure

Search resources, services, and docs (5+)

Home > Каталог по умовчальному > Groups > Groups | Overview >

New Group

Got feedback?

Group type *

Security

Group name *

Administrators

Group description

security administrators

Membership type

Assigned

Owners

No owners selected

Members

No members selected

Рисунок 3.6. – Створення групи безпеки

Microsoft Azure

Search resources, services, and docs (5+)

Home > Каталог по умовчальному > Groups > Groups | Overview >

All groups

New group

Download groups

Refresh

Manage view

Delete

Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your identity and access management needs. Try the new Microsoft Entra admin center!

Search

Add filter

Search mode

Contains

2 groups found

☐	Name	Object Id	Group type	Membership type	Email	Source
☐	Administrators	2ec2e44d-3bf8-44e7-93ae-ae1cc9533dc0	Security	Assigned		Cloud
☐	Users	1d36f054-ef61-410c-9267-bbbacc8c0bd	Security	Assigned		Cloud

Рисунок 3.7. – Створені групи безпеки

Microsoft Azure

Search resources, services, and docs (5+)

Home > Каталог по умовчальному > Groups > Groups | Overview > All groups > Administrators

Members

Add members

Bulk operations

Refresh

Manage view

Delete

Got feedback?

Direct members

All members

Search

Add

0 group members found

No members have been found

Add members

Try changing or adding filters if you don't see what you're looking for.

Search

33 results found

All Users Groups Devices Enterprise applications

☐	Name	Type	Details
☐	AAD Request Verification Service...	Enterprise ap...	c728155f-7b2a-4502-a08b-b8af9b269319
☐	Administrators	Group	
☒	Anastasia Kovtoniuk	User	nastka@kovtoniuk@gmail.com
☐	AADReporting	Enterprise ap...	1b912ec3-e9d4-4c4d-e53e-76aa7ad2b07
☐	Users	Group	
☐	k211_kad	User	k211_kad@student.ctu.edu.ua
☐	Azure Credential Configuration E...	Enterprise ap...	eaf89292-c8d3-4433-b5ee-b09d066b1a6

Selected (2)

Reset

Anastasia Kovtoniuk

nastka@kovtoniuk@gmail.com

nastka

nastka@nastka@kovtoniuk@gmail.com

Select

Рисунок 3.8. – Додавання користувачів в групи

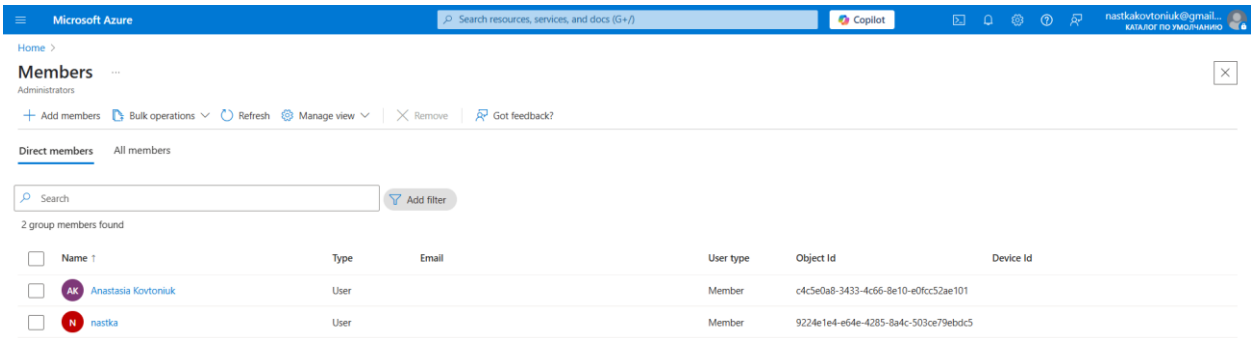


Рисунок 3.9. – Результат додавання користувачів в групи

Однією із класних можливостей є зміна ролей для користувачів (рис. 3.10). Глобальний адміністратор призначається автоматично з обліковим записом, з якого було створено тенант. Інші ролі такі як Адміністратор, користувачу можна призначити власноруч (рис. 3.11).

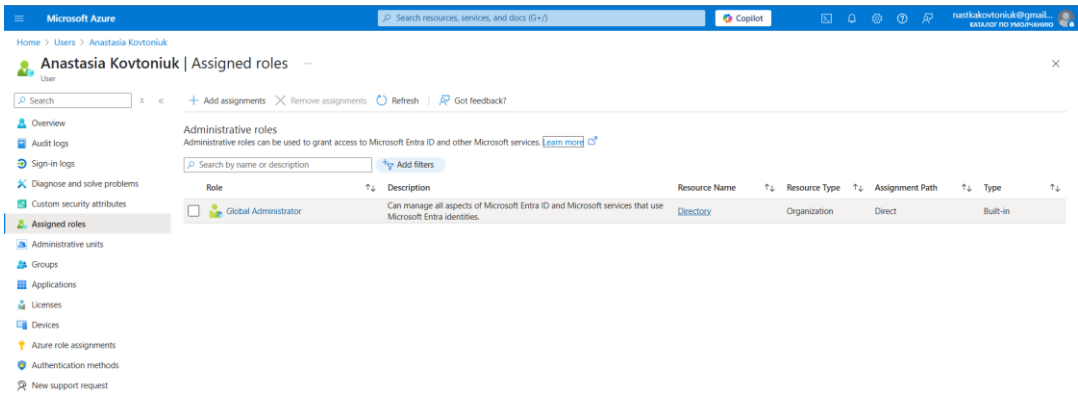


Рисунок 3.10. – Автоматично призначені ролі

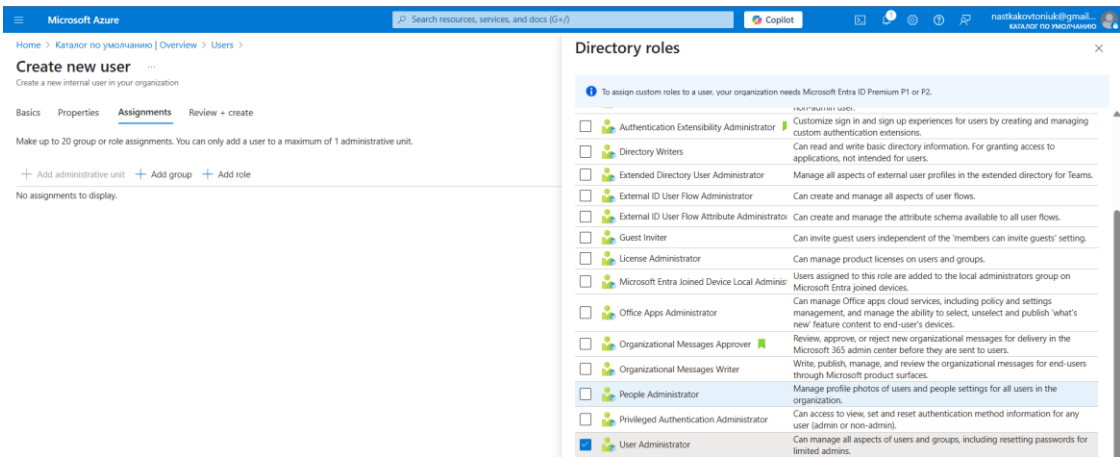


Рисунок 3.11. – Призначення ролей

Після створення та налаштування користувачів та груп в Microsoft Entra ID потрібно створити віртуальну мережу (Azure VNet) (рис. 3.12, рис. 3.13, рис. 3.14).

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Virtual networks](#) >

Create virtual network

Basics

Security

IP addresses

Tags

Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure subscription 1

Resource group *

(New) kovtoniuk

[Create new](#)

Instance details

Virtual network name *

kovtoniuk_virtual_net

Region *

(US) East US

[Deploy to an Azure Extended Zone](#)

Рисунок 3.12. – Створення віртуальної мережі

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Virtual networks](#) >

Create virtual network

Basics

Security

IP addresses

Tags

Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

[+ Add a subnet](#)

10.1.0.0/16

10.1.0.0

/16

10.1.0.0 - 10.1.255.25565 536 addresses

Delete address space

Subnets	IP address range	Size	NAT gateway
default	10.1.0.0 - 10.1.0.255	/24 (256 addresses)	-

Add IPv4 address space

Рисунок 3.13. – Налаштування діапазону IP-адрес

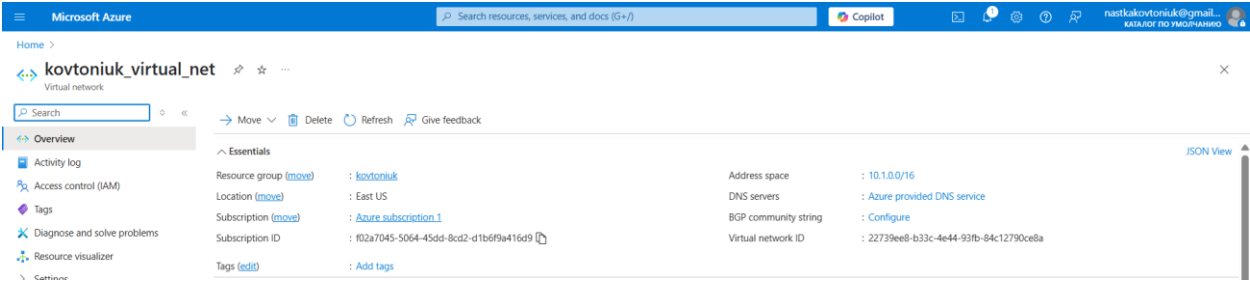


Рисунок 3.14. – Створена віртуальна мережа

Ця мережа згодом знадобиться при створенні віртуальної машини.

Microsoft Azure дає можливість створювати віртуальні машини з різними ОС на базі готових хмарних образів (рис. 3.15 – 3.16), дана віртуальна машина буде Windows Server 2022 Datacenter Edition, на якій буде розгорнуто Active Directory.

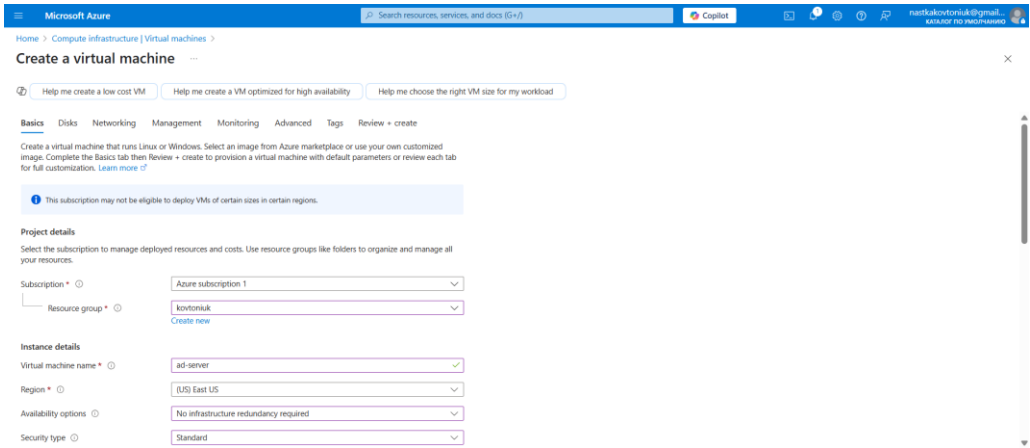


Рисунок 3.15. – Створення віртуальної машини

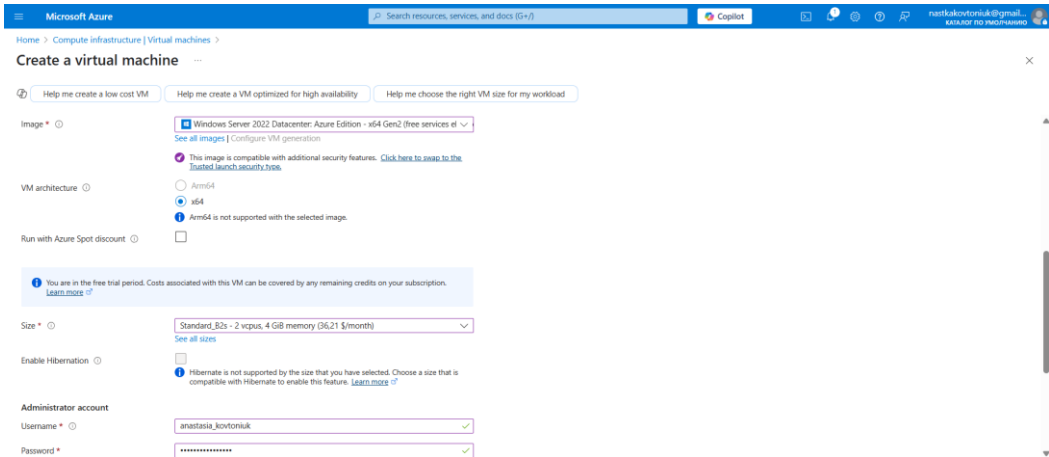


Рисунок 3.16. – Створення віртуальної машини

Під час створення ВМ потрібно буде ввести логін та пароль для адміністратора (рис. 3.17), який буде використовуватися для входу на комп'ютер.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

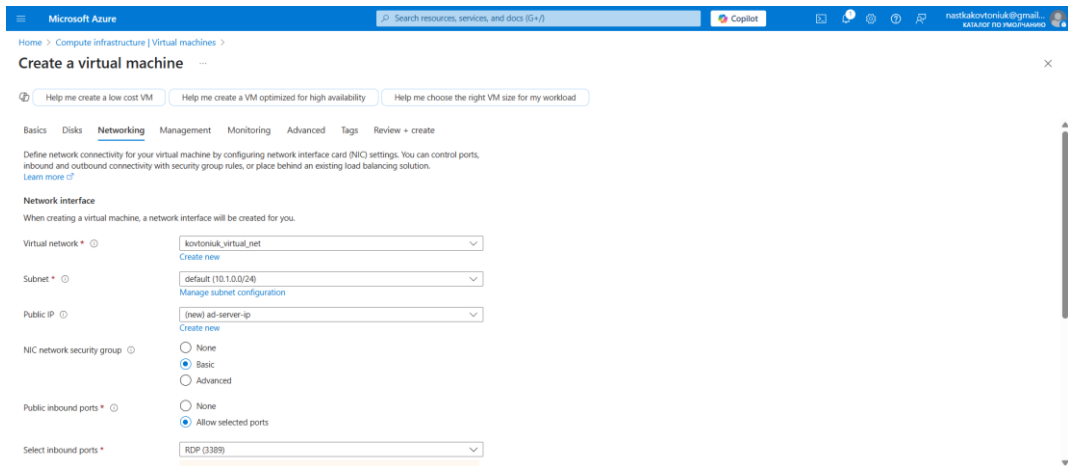


Рисунок 3.17. – Додавання ВМ до віртуальної мережі, створеної раніше

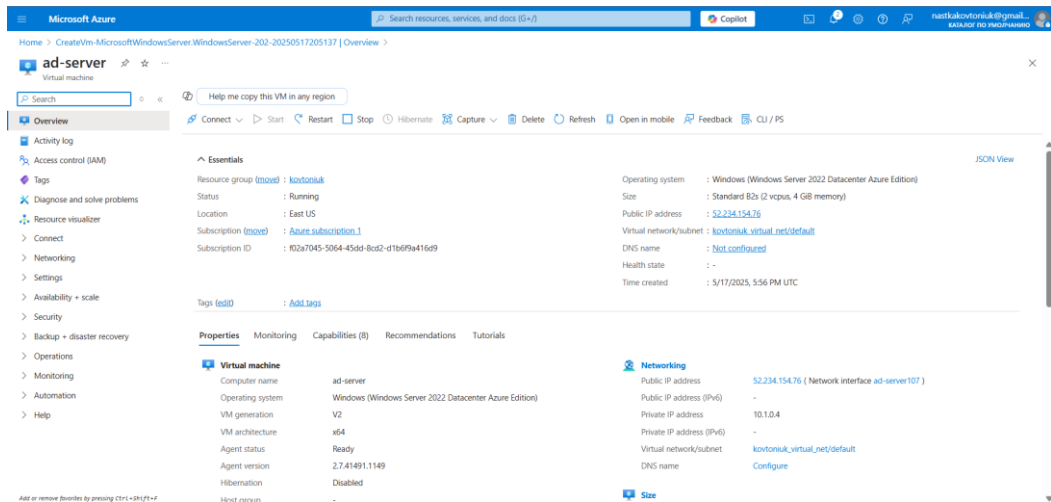


Рисунок 3.18. – Створена віртуальна машина

Віртуальна машина створена (рис. 3.18). Для підключення до неї потрібно скористатися RDP. RDP файл можна завантажити з головної сторінки опису ВМ (рис. 3.19 – 3.20).

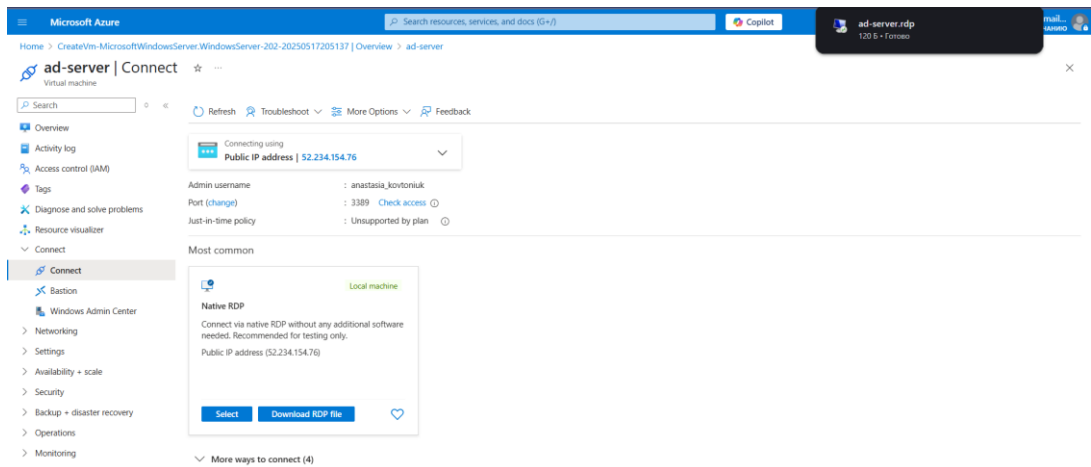


Рисунок 3.19. – Завантаження RDP файлу

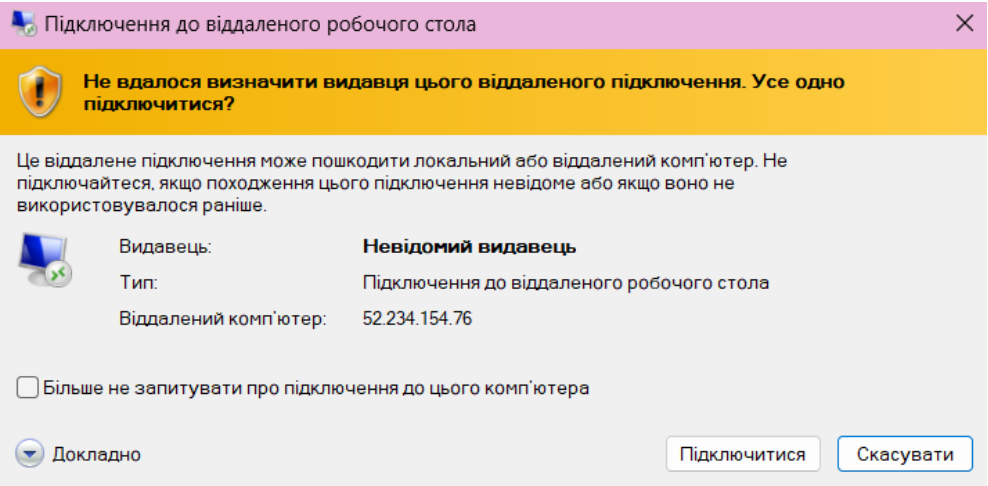


Рисунок 3.20. – Підключення до віддаленого робочого стола

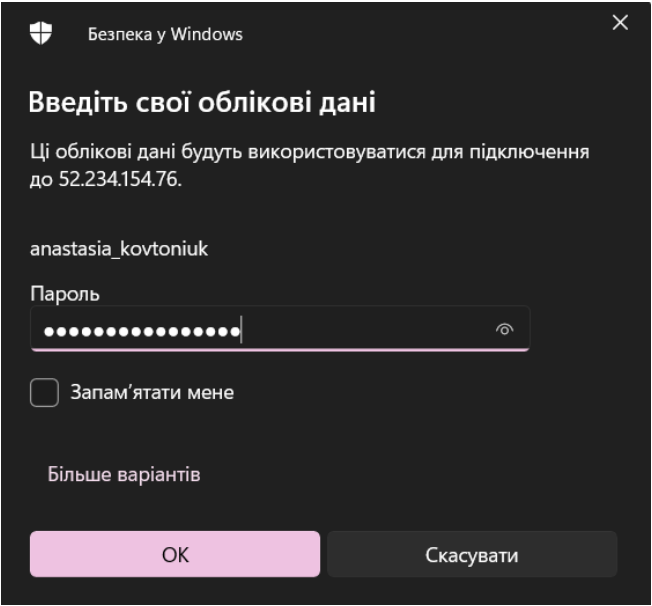


Рисунок 3.21. – Введення облікових даних

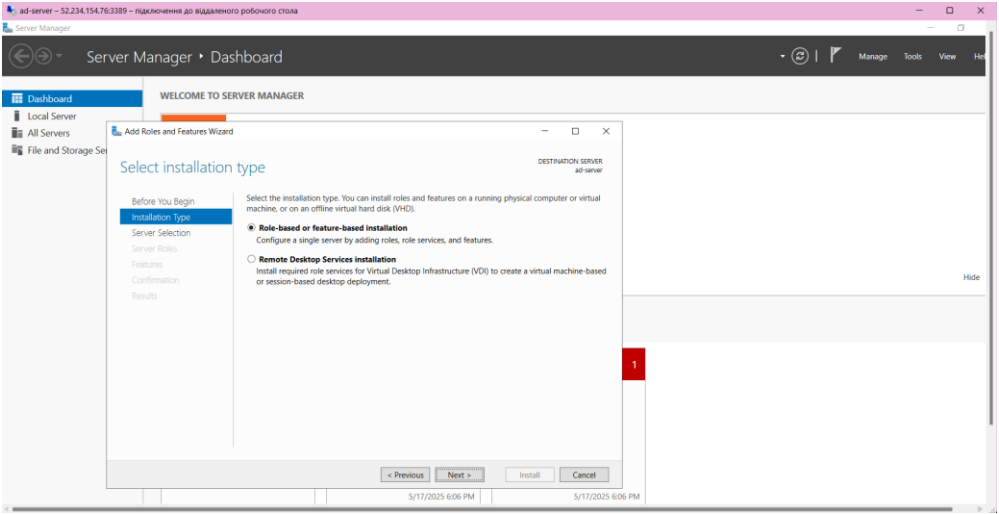


Рисунок 3.22. – Вдале підключення до віртуальної машини

Тепер, коли підключення вдале (рис. 3.21 – 3.22), наступний крок – це встановлення ролей AD DS (рис. 3.23 – 3.24).

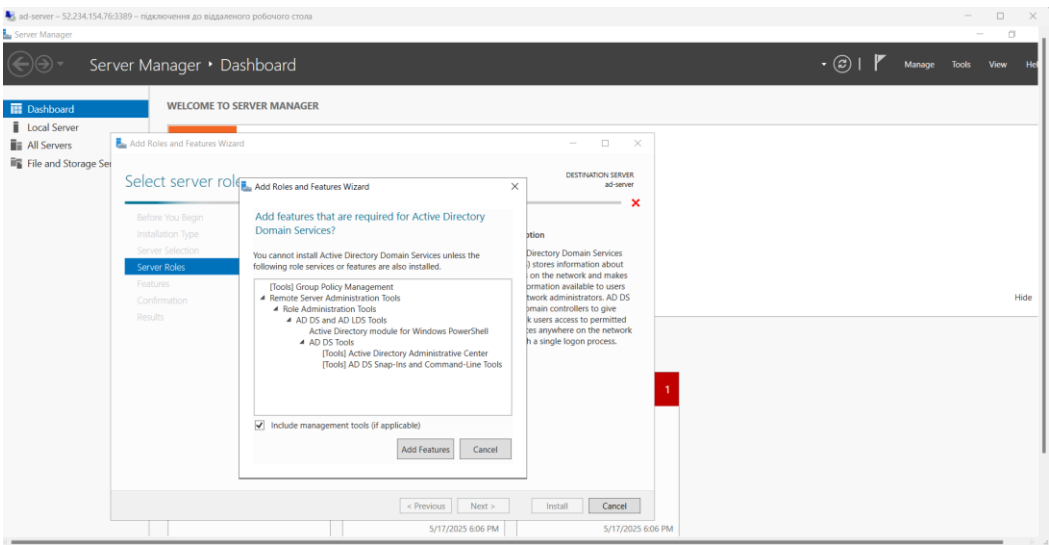


Рисунок 3.23. – Встановлення ролей

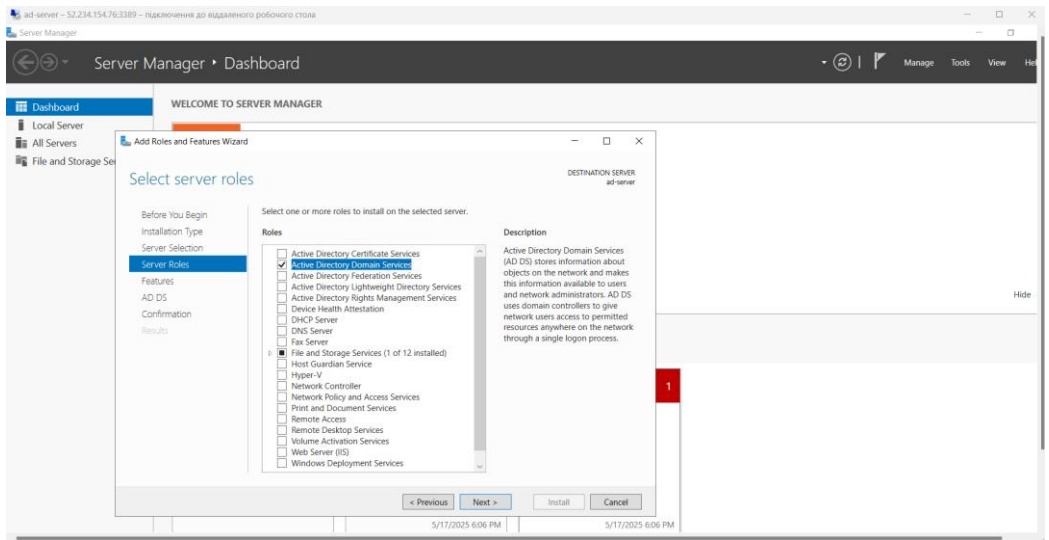


Рисунок 3.24. – Встановлення ролей

Після налаштування ролей Active Directory потрібно створити новий домен (рис. 3.25) та налаштувати його (рис. 3.26 – 3.27).

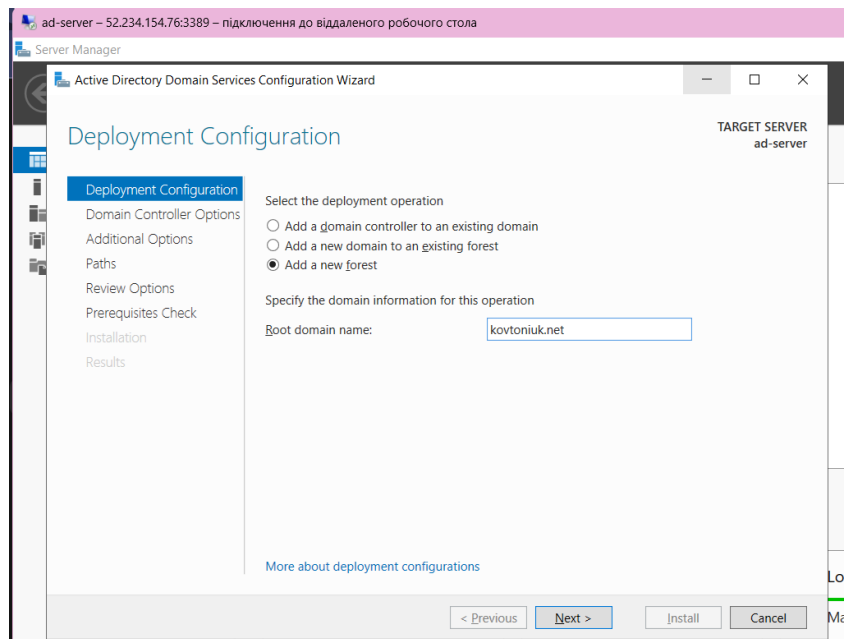


Рисунок 3.25. – Створення нового домену kovtoniuk.net

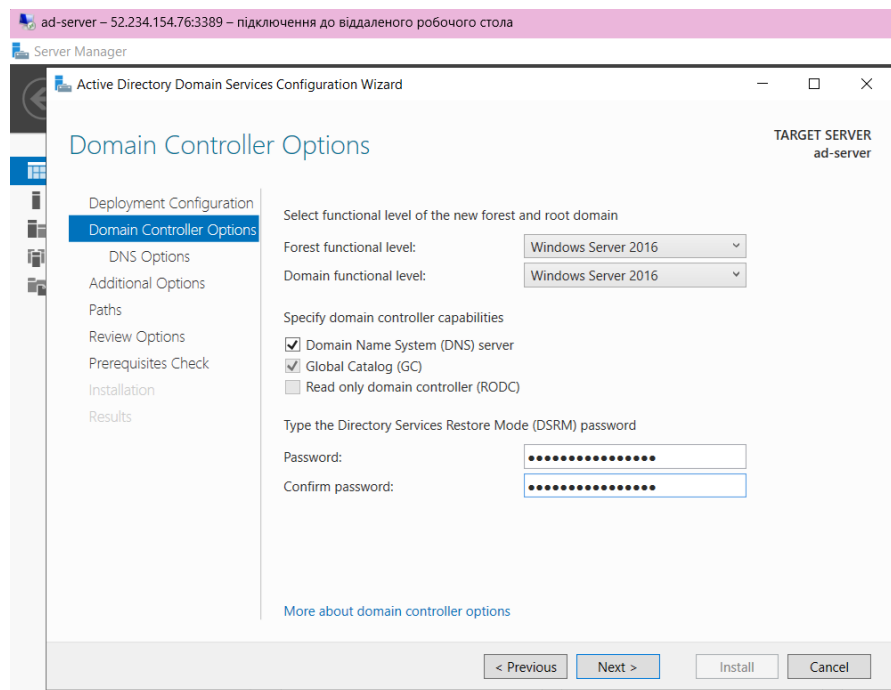


Рисунок 3.26. – Налаштування паролю

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

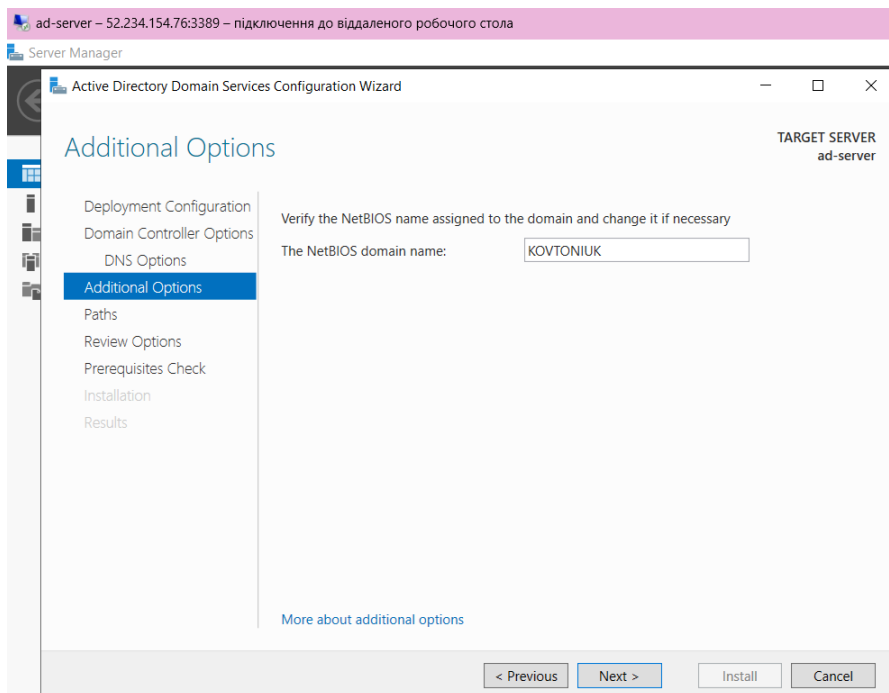


Рисунок 3.27. – Доменне ім'я

Для того, щоб перевірити правильність налаштувань, спробуємо створити організаційні одиниці (рис. 3.28) та користувачів в домені (рис. 3.29, рис. 3.30, рис. 3.31).

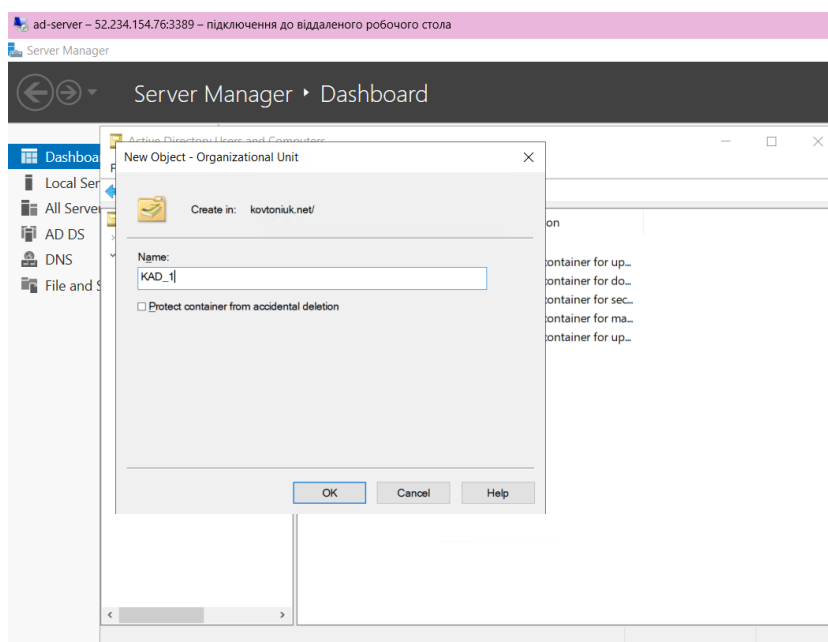


Рисунок 3.28. – Створення організаційної одиниці

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

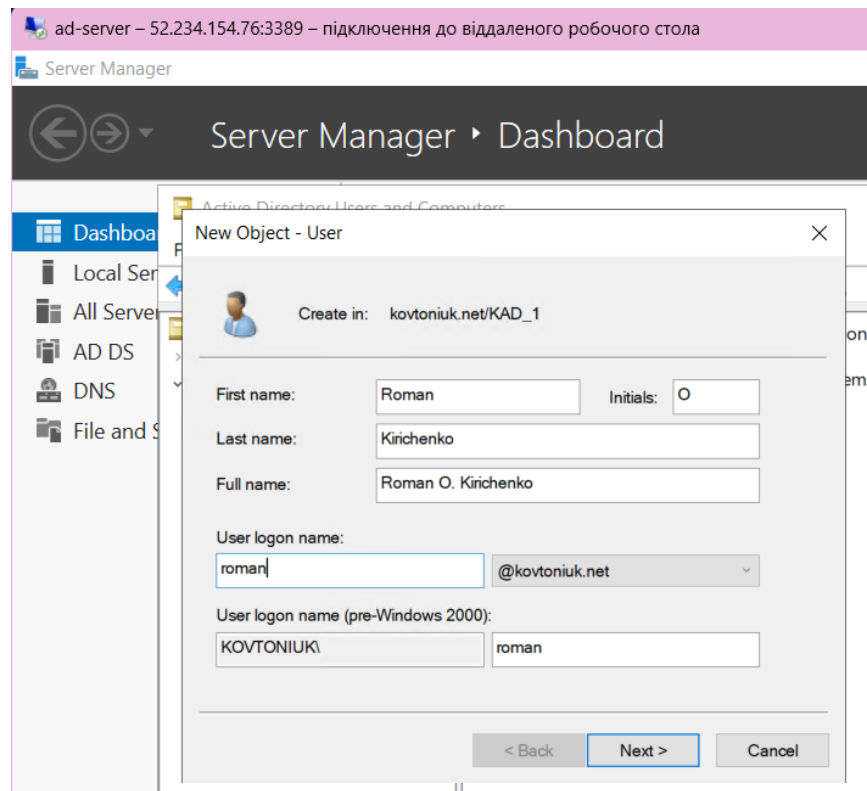


Рисунок 3.29. – Створення користувача

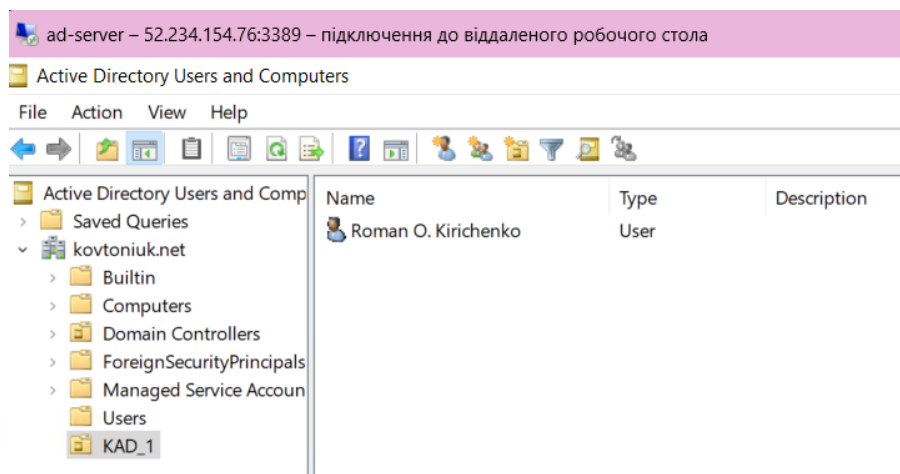


Рисунок 3.30. – Результат створення організаційної одиниці та користувача

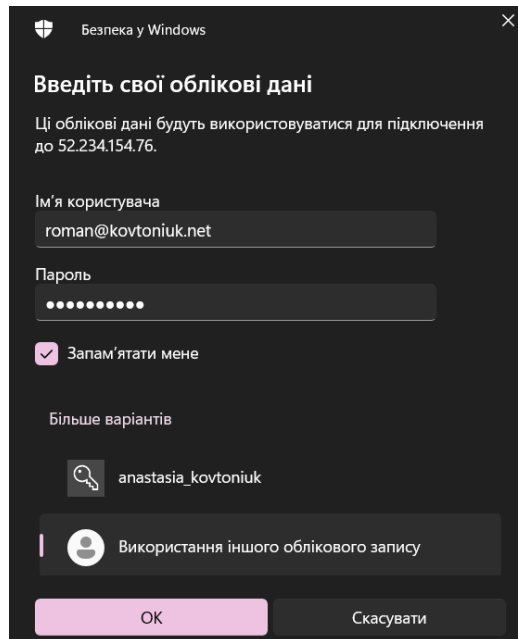


Рисунок 3.31. – Спроба входу під створеним обліковим записом

Базове налаштування хмарного серверу закінчено, тепер налаштування локального серверу. Розгортання VM буде відбуватися на гіпервізорі Oracle VM VirtualBox (рис. 3.32) та використовуватиметься операційна система Windows (рис. 3.33, рис. 3.34, рис. 3.35).

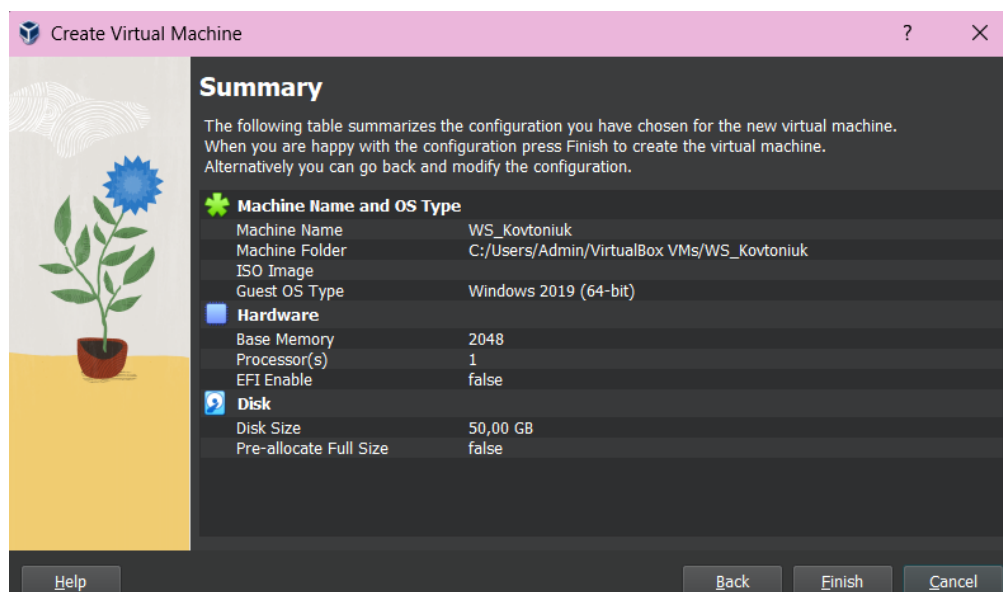


Рисунок 3.32. - Створення віртуальної машини

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

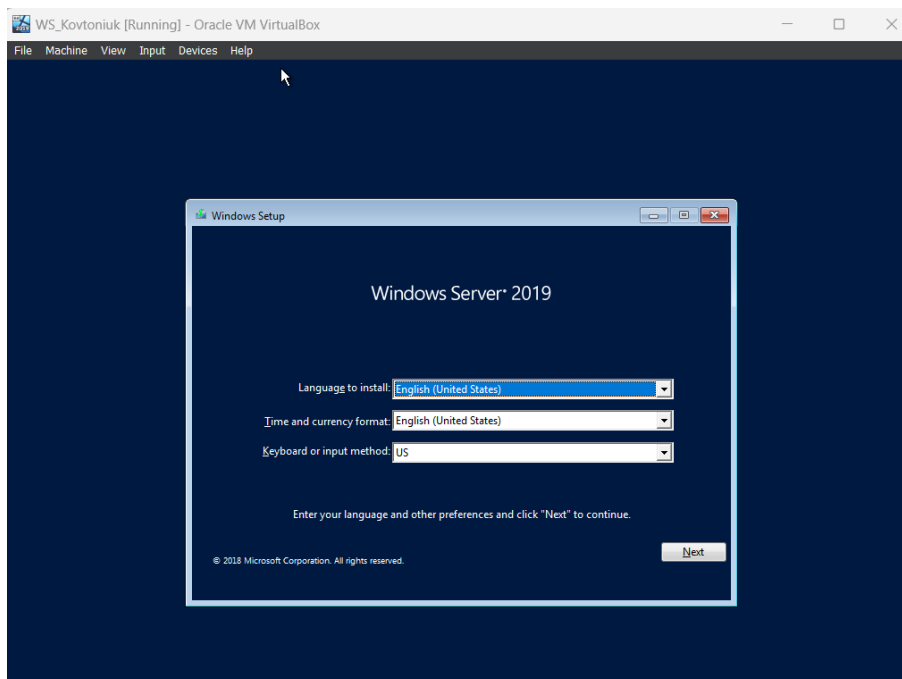


Рисунок 3.33. – Завантаження Windows Server 2019

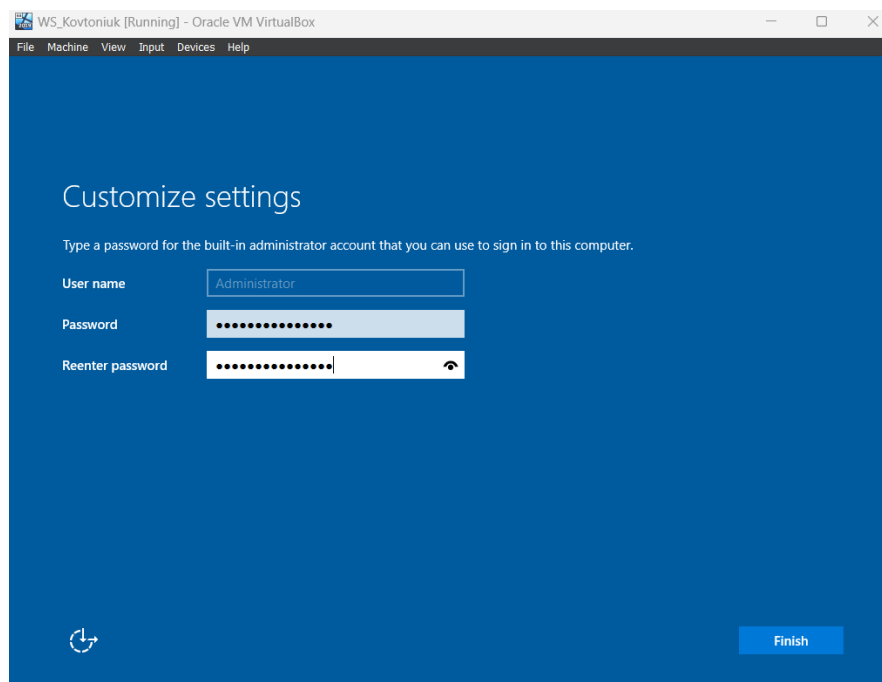


Рисунок 3.34. – Налаштування паролю для адміністратора

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

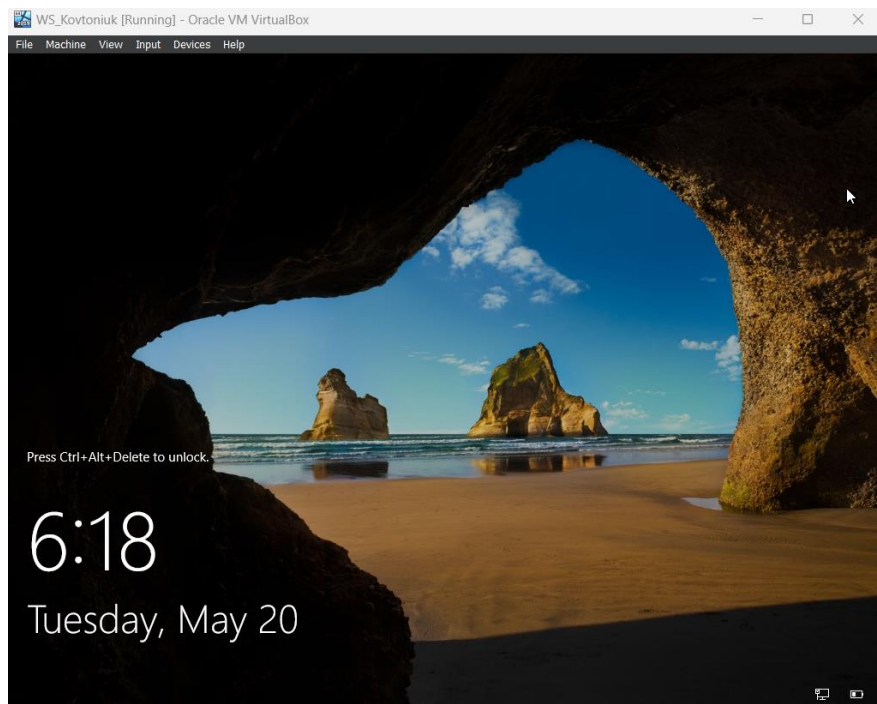


Рисунок 3.35. – Результат успішного встановлення

Переходимо до налаштування AD DS (рис. 3.36) на локальному сервері.

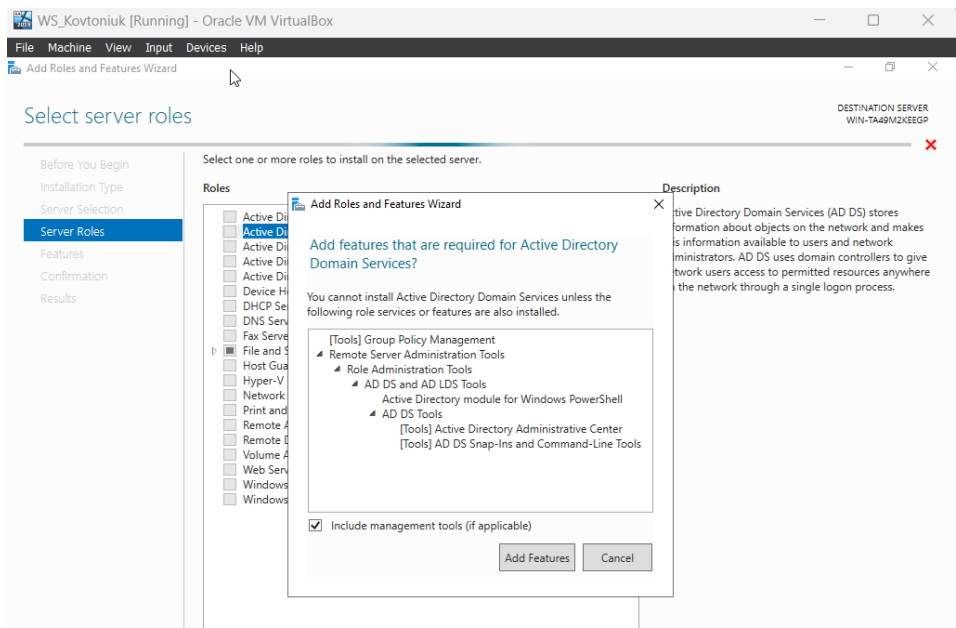


Рисунок 3.36. – Налаштування ролей

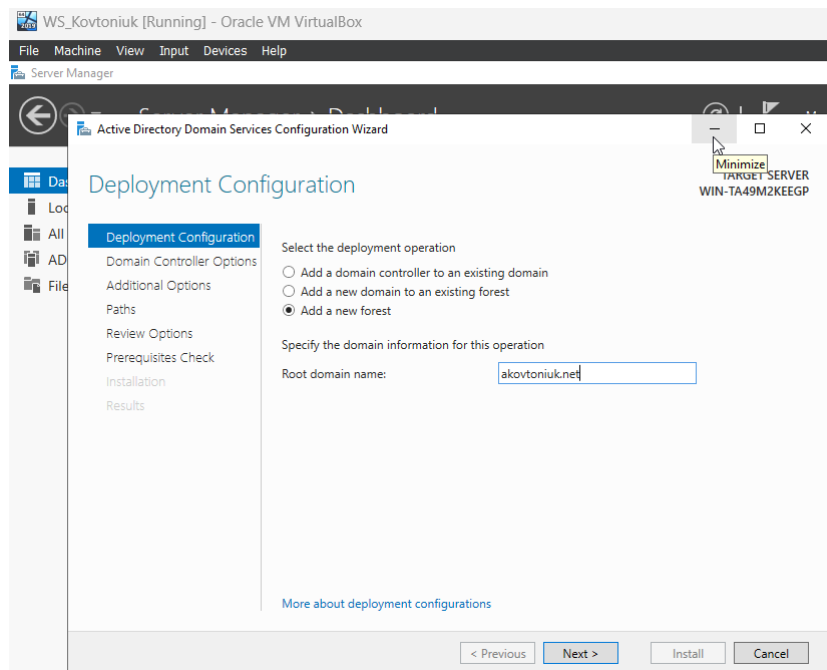


Рисунок 3.37. – Створення нового домену

ВМ створена на базі Microsoft Azure та дана ВМ будуть використовувати різні домени (рис. 3.37), але це не стане на заваді їхньої інтеграції (рис. 3.38).

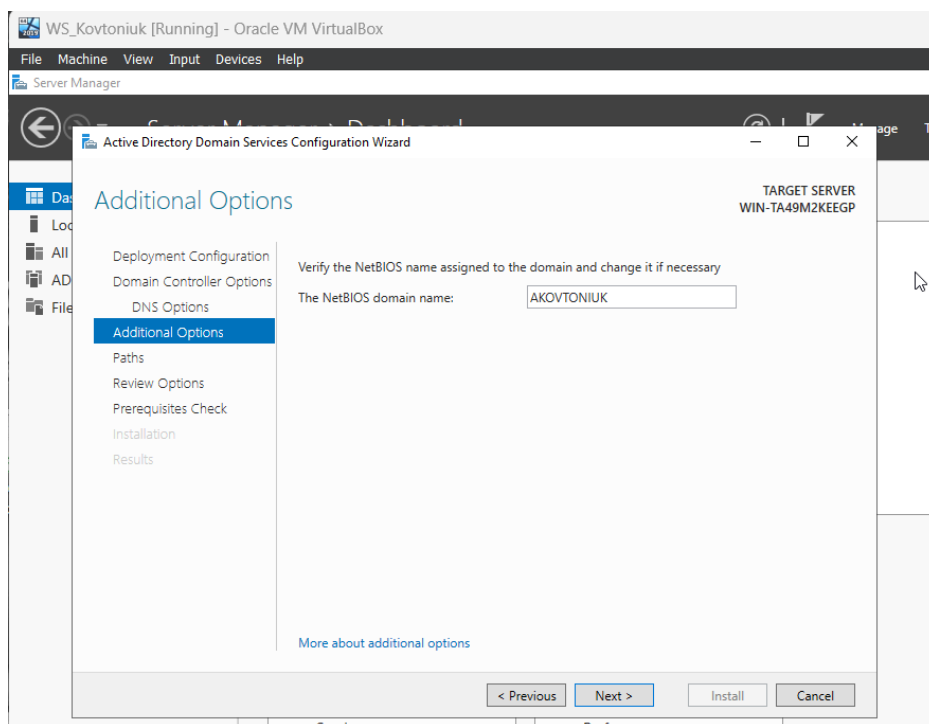


Рисунок 3.38. – Доменне ім'я

Створюємо користувача (рис. 3.39) для перевірки правильності функціонування домену.

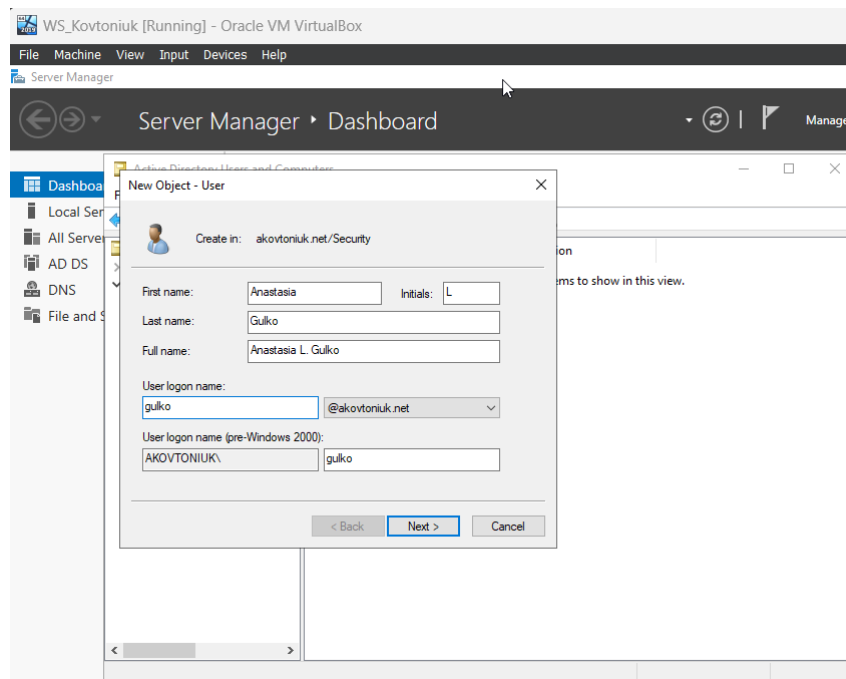


Рисунок 3.39. – Створення користувача

В цьому підрозділі було розглянуто ключові моменти налаштування та розгортання віртуальних машин в хмарному середовищі та локальному. Налаштовано AD DS на віртуальних машинах та перевірено правильність функціонування домену.

3.2 Інтеграція локального середовища з Microsoft Azure

Для інтеграції локального середовища з Microsoft Azure буде використано Azure AD Connect Sync.

Azure AD Connect дозволяє підключати локальну інфраструктуру ідентифікації до Azure Active Directory (Azure AD). Це дозволяє керувати ідентифікаторами в гібридній інфраструктурі, що складається з публічної хмари та локальних ресурсів. Після інтеграції локальних каталогів з Azure AD ви можете використовувати функції цієї служби для спрощення керування ідентифікаторами та надання локальним користувачам легшого доступу до хмарних ресурсів. [17]

Для початку потрібно завантажити Azure AD Connect Sync (рис. 3.41) з офіційного сайту Microsoft (рис. 3.40).

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

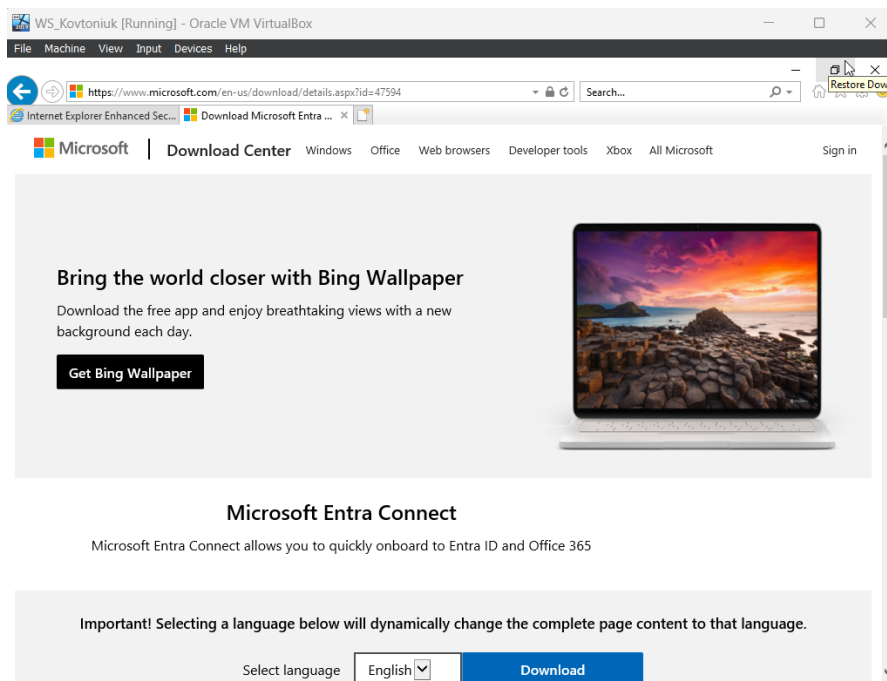


Рисунок 3.40. - Офіційний сайт Microsoft

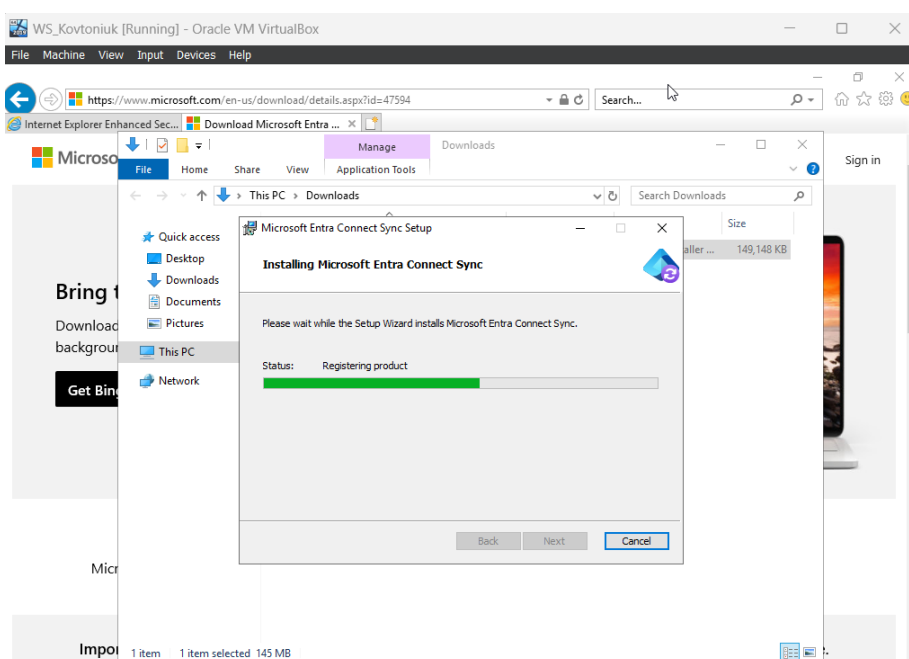


Рисунок 3.41. – Завантаження Azure AD Connect

Після завершення завантаження, можна побачити вікно налаштування Azure AD Connect (рис. 3.42) (також можна називати Microsoft Entra Connect Sync).

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

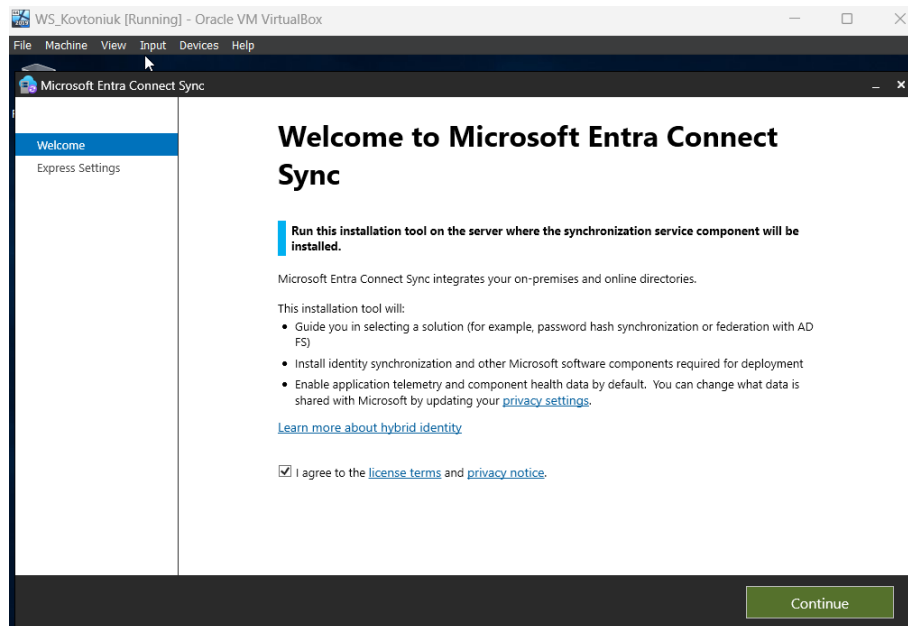


Рисунок 3.42. – Вікно налаштувань

Є два варіанти налаштувань.

Перший варіант, коли ми самі обираємо потрібно параметри та виконуємо більше налаштувань, або експрес встановлення, де система сама обирає потрібні параметри для встановлення.

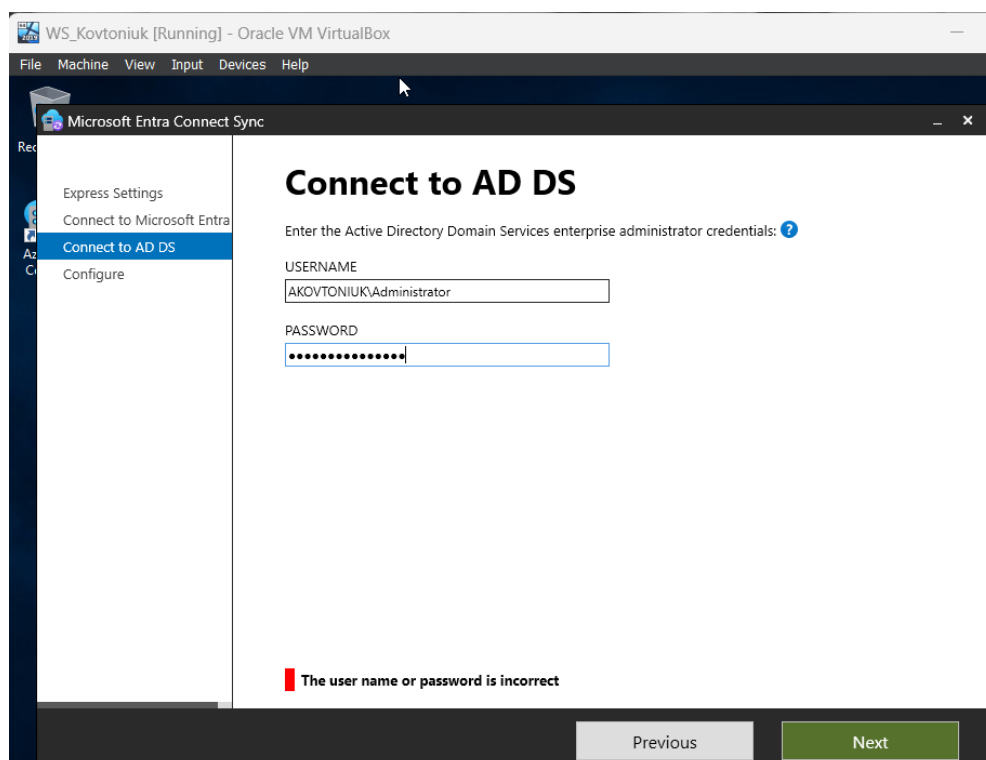


Рисунок 3.43. – Приєднання до AD DS

Перед тим як з'явиться це вікно, потрібно ввести свої облікові дані глобального адміністратора Microsoft Entra ID (рис. 3.43).

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

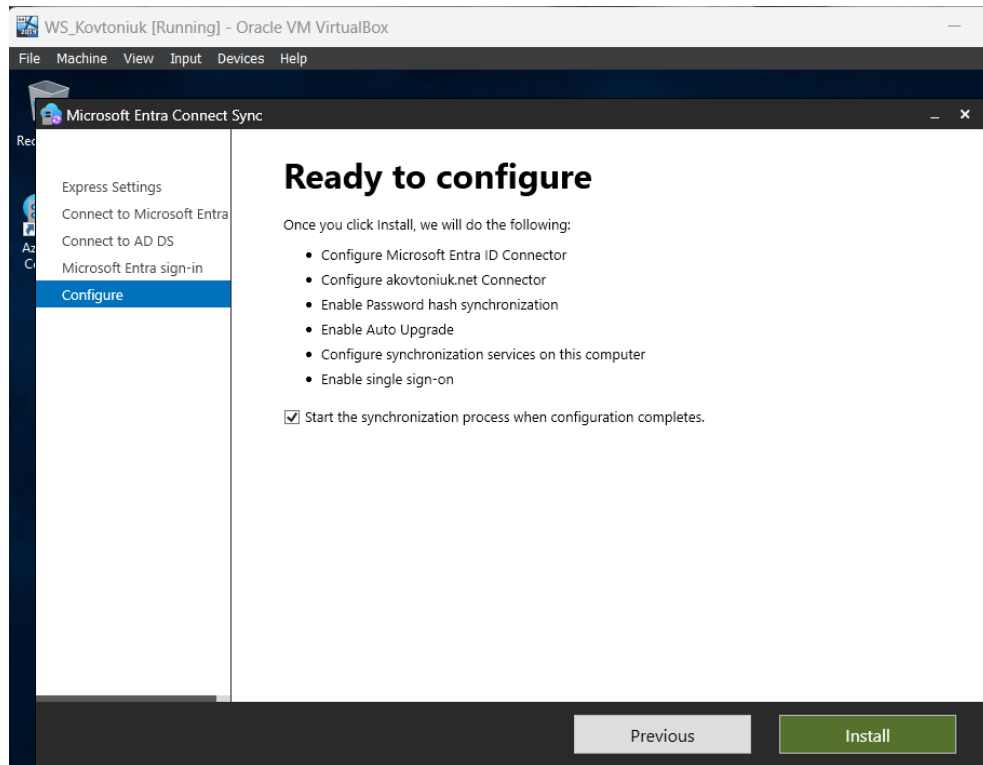


Рисунок 3.44. – Початок конфігурації

Розглянемо, що будемо мати після того, як конфігурація закінчиться (рис. 3.44).

- **Configure Microsoft Entra ID Connector.** Налаштовує зв'язок між локальним сервером та хмарною службою Microsoft Entra ID.

- **Configure akovtoniuk.net Connector.** Налаштовує конектор для локального домену akovtoniuk.net – визначає, як саме буде відбуватися синхронізація з локальною Active Directory цього домену.

- **Enable Password hash synchronization.** Включає синхронізацію хешів паролів користувачів з локального середовища в хмарне, що дозволяє їм входити у хмарні сервіси, використовуючи свої локальні паролі.

- **Enable Auto Upgrade.** Автоматичне оновлення Entra Connect — щоб завжди використовувалась актуальна версія з останніми виправленнями й функціями без потреби ручного втручання.

- **Configure synchronization services on this computer.** Інсталюються й запускаються всі необхідні служби синхронізації на цьому сервері, щоб забезпечити стабільну роботу обміну даними між локальним і хмарним середовищами.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Enable single sign-on.** Включає функцію єдиного входу (SSO) — користувачі можуть входити в хмарні та локальні системи без повторного введення облікових даних (зручно й безпечно).

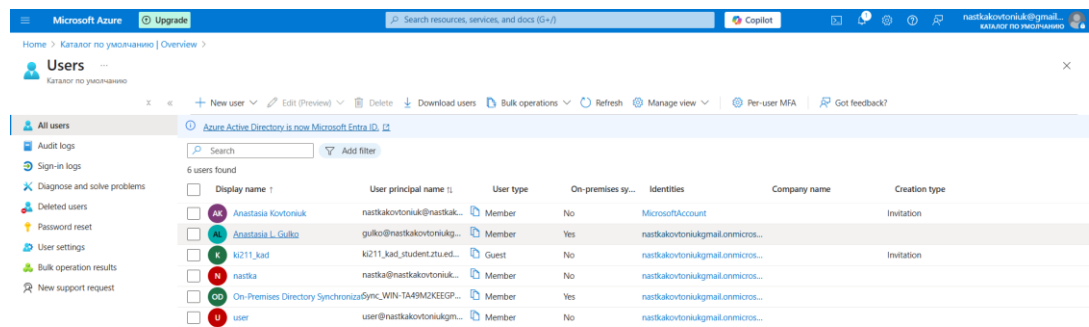


Рисунок 3.45. – Вкладка «Користувачі» в Microsoft Entra ID після синхронізації з локальним AD

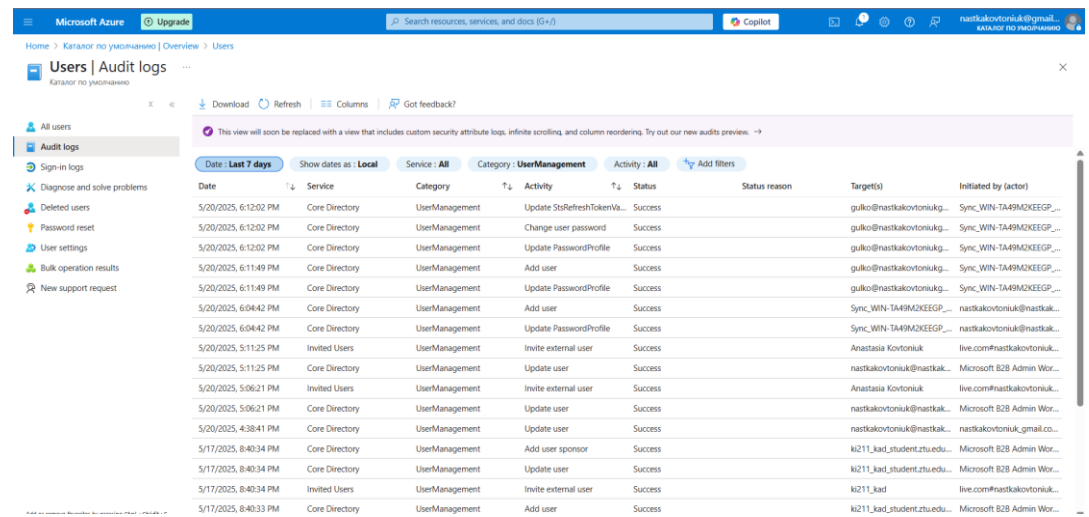


Рисунок 3.46. – Журнал аудиту

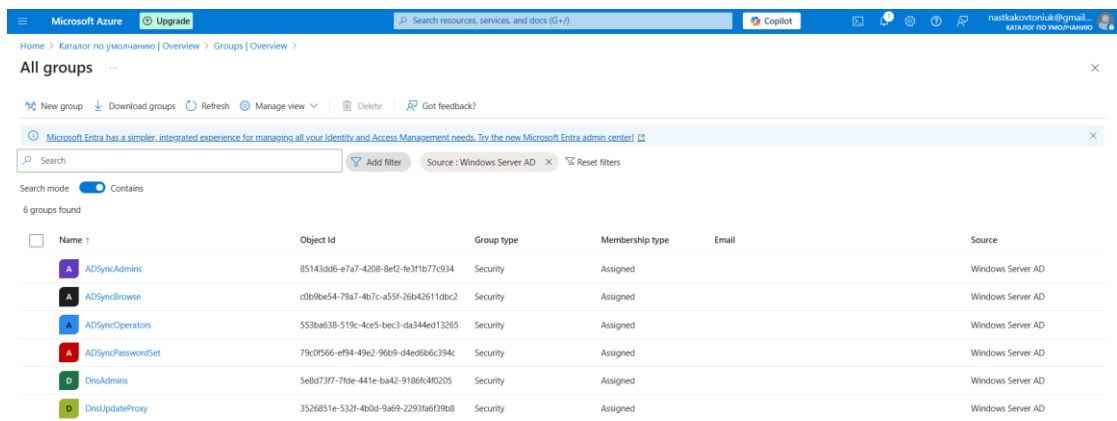


Рисунок 3.47. – Вкладка «Групи» після синхронізації

Отже, в цьому підрозділі відбулася синхронізація між хмарним сервером та локальним (рис. 3.45, рис. 3.46, рис. 3.47). Використовувалися такі інструменти як Microsoft Entra ID Connect Sync.

3.3 Створення спільних ресурсів та файлової інфраструктури

Azure File Shares – це хмарний сервіс обміну файлами, який надає безпечне, масштабоване та високодоступне рішення для зберігання та обміну файлами в хмарі. За допомогою Azure File Shares ви можете зберігати, обмінюватися файлами та отримувати до них доступ з будь-якого місця, будь-коли та з будь-якого пристрою. Незалежно від того, чи ви власник малого бізнесу, фрілансер чи організація корпоративного рівня, Azure File Shares може допомогти задовольнити наявні потреби в зберіганні та обміні файлами. [18]

Створення Azure File Share. Перш ніж створити його потрібно створити Групу ресурсів (рис. 3.48).

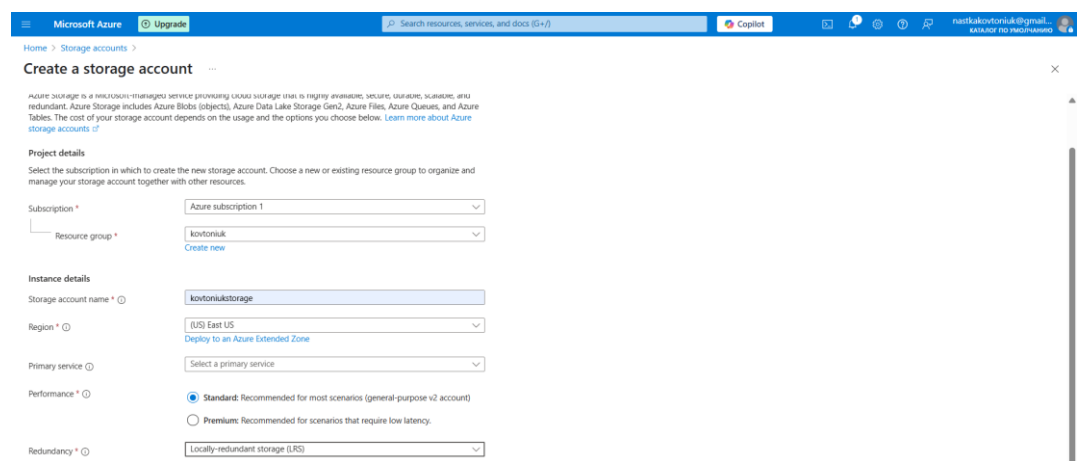


Рисунок 3.48. – Створення Групи ресурсів

Після її створення потрібно перейти на вкладку створення нового файлового ресурсу (рис. 3.49, рис. 3.50, рис. 3.51).

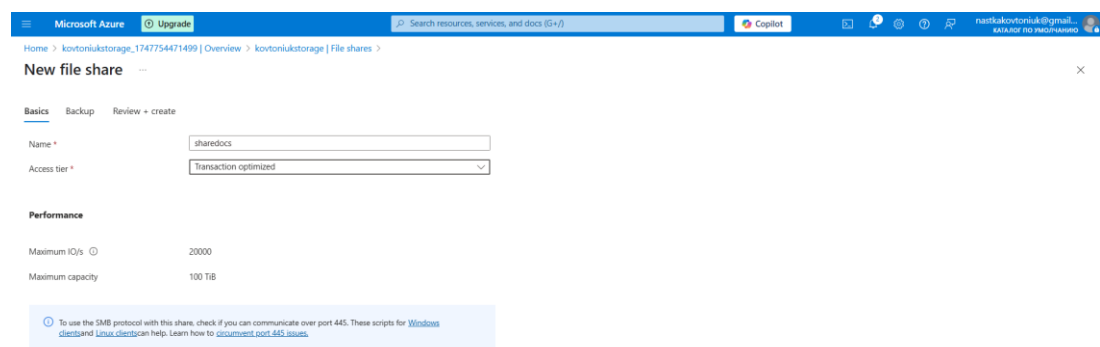


Рисунок 3.49. – Створення нового файлового ресурсу

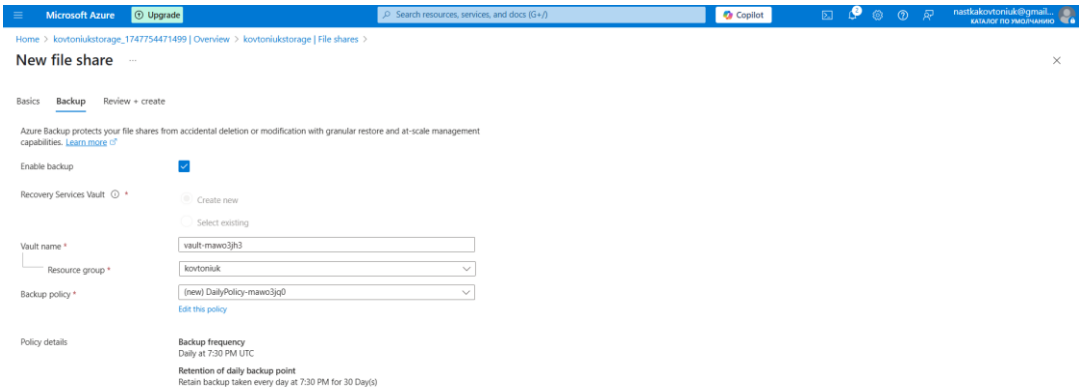


Рисунок 3.50. – Налаштування резервного копіювання

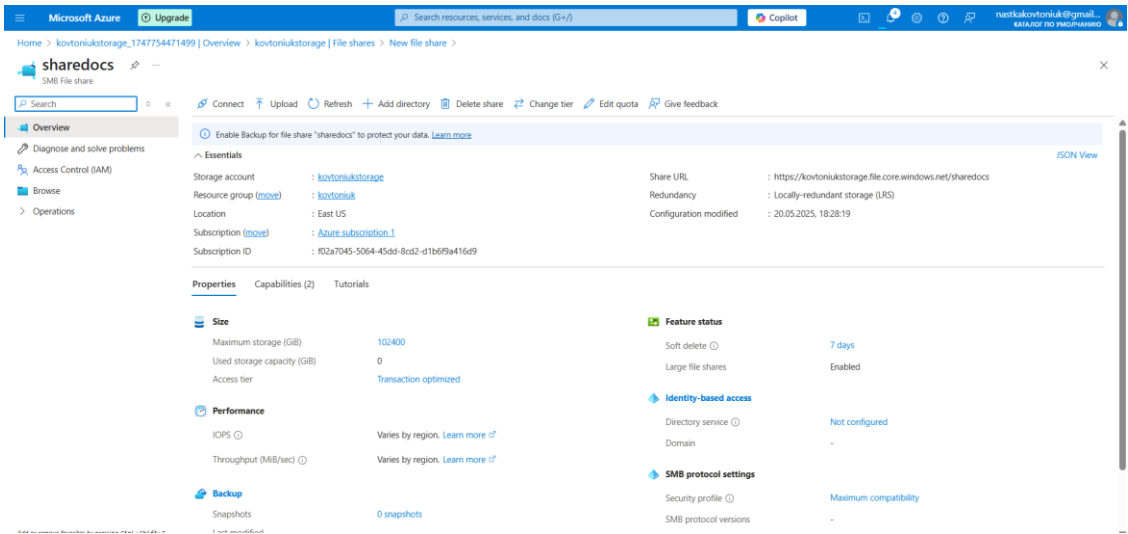


Рисунок 3.51. – Створений файловий ресурс

Для того, щоб до цього ресурсу, можна було підключитися з ПК потрібно згенерувати SAS Token або Key.

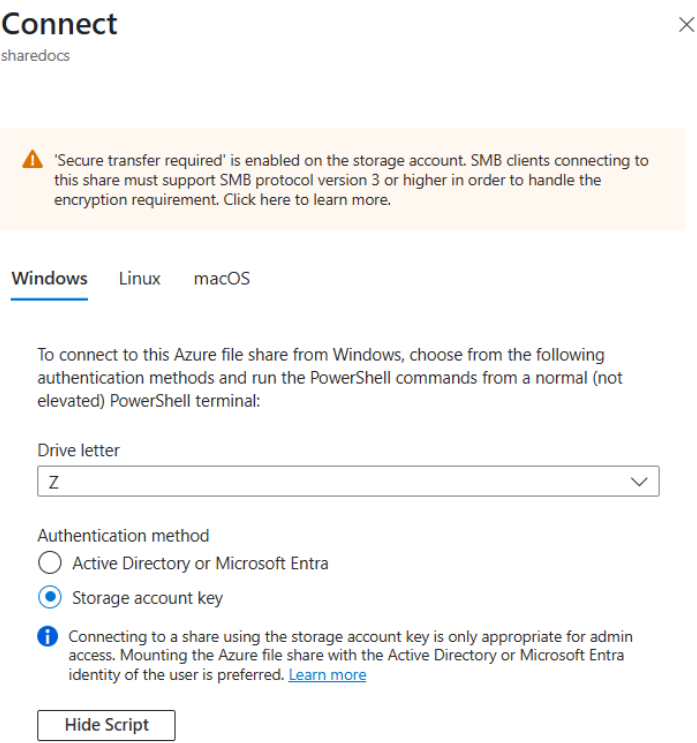


Рисунок 3.52. – Вкладка «Підключення»

На цій вкладці (рис. 3.52) перевіряємо скрипт для підключення та копіюємо його (рис. 3.54).

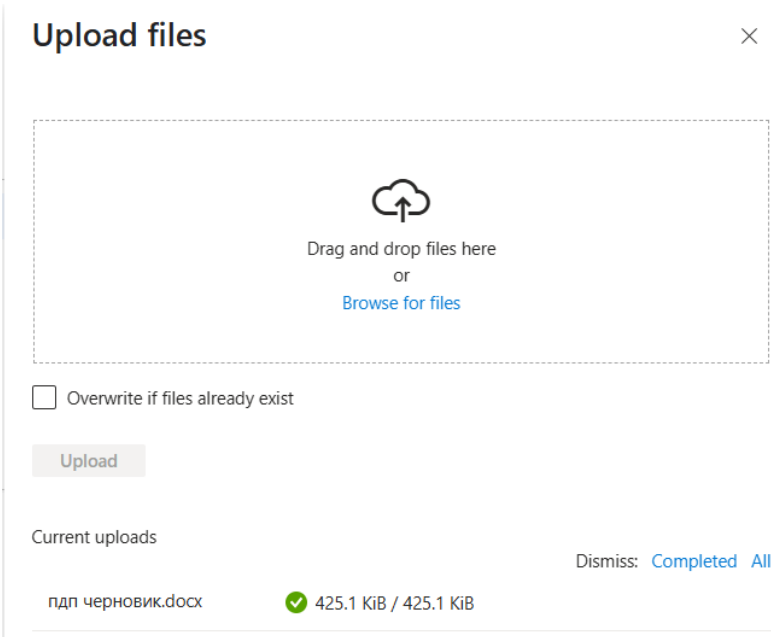


Рисунок 3.53. – Завантаження файлу

Тепер перевіримо чи буде видно файл на віртуальних машинах. Для цього потрібно зайти на ВМ в PowerShell в режимі адміністратора та ввести скрипт для підключення до файлового сервісу (рис. 3.54).

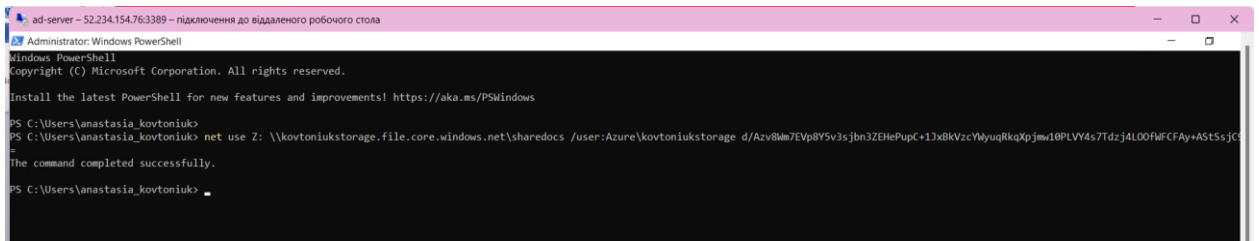


Рисунок 3.54. – Підключення з хмарної VM

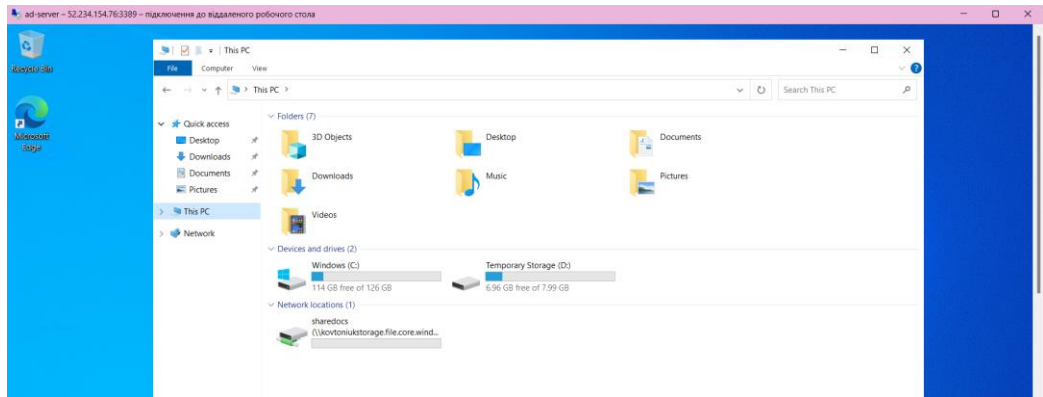


Рисунок 3.55. – Результат підключення

Після підключення можна побачити папку з файлами (рис. 3.55).

Тепер те саме, тільки на VM локальній (рис. 3.56).

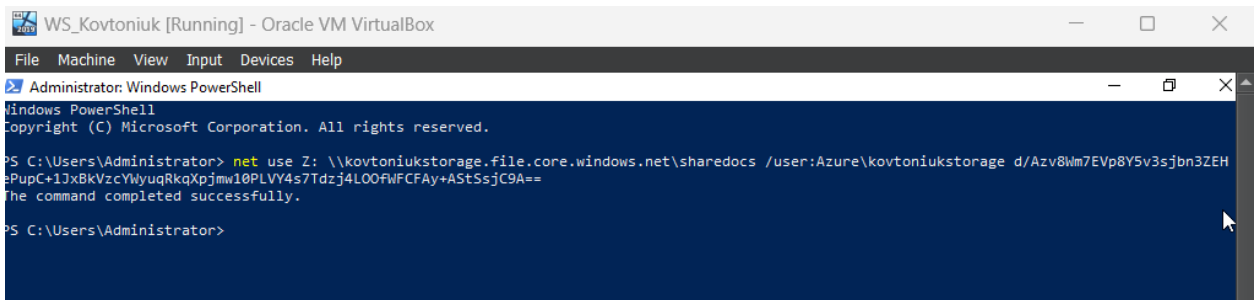


Рисунок 3.56. – Підключення з локальної VM

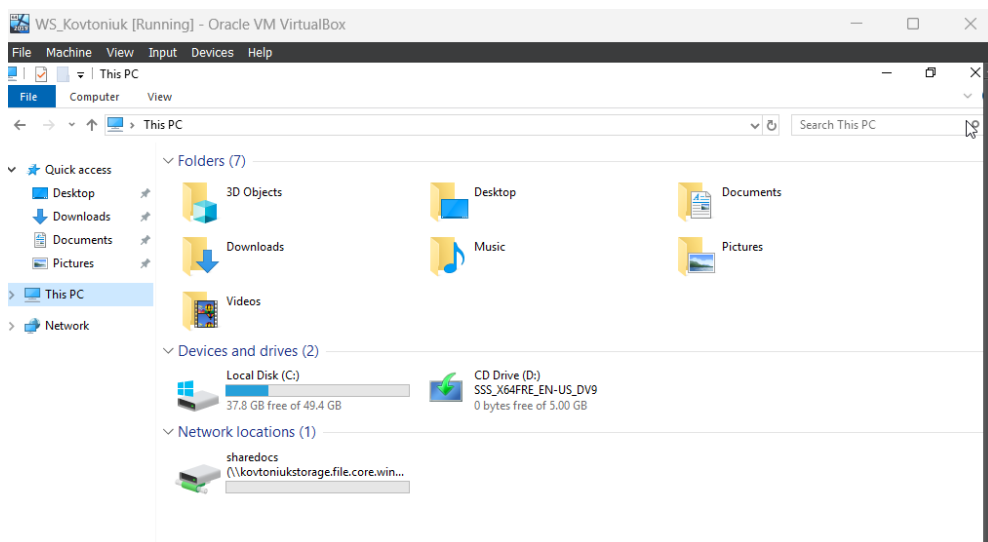


Рисунок 3.57. – Результат підключення

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

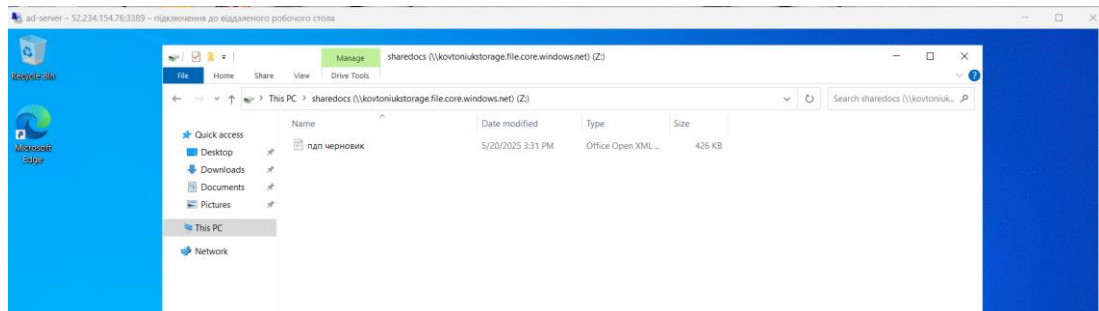


Рисунок 3.58. – Результат підключення

В цьому підрозділі було створено спільний файловий ресурс (рис. 3.57) для передачі інформації між віртуальними машинами (рис. 3.58).

3.4 Безпека, моніторинг та резервне копіювання

Для моніторингу та безпеки використано Microsoft Defender for Cloud (рис. 3.59, рис. 3.60, рис. 3.61) та Azure Security Center.

Microsoft Defender for Cloud — це хмарна платформа захисту програм (CNAPP), яка включає заходи безпеки та методи, розроблені для захисту хмарних програм від різних кіберзагроз і вразливостей. Defender for Cloud включає:

- Рішення для операцій безпеки розробки (DevSecOps), яке об'єднує управління безпекою на рівні коду в багатохмарних та багатоконвеєрних середовищах.
- Рішення для керування станом безпеки хмари (CSPM), яке визначає дії для запобігання порушенням.
- Платформа захисту хмарних робочих навантажень (CWPP) із захистом для серверів, контейнерів, сховищ, баз даних та інших робочих навантажень. [19]

Azure Security Center — це інструмент керування безпекою, який дозволяє вам отримувати уявлення про стан безпеки в гібридних хмарних робочих навантаженнях, зменшувати ризики атак і швидко реагувати на виявлені загрози. [20]

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

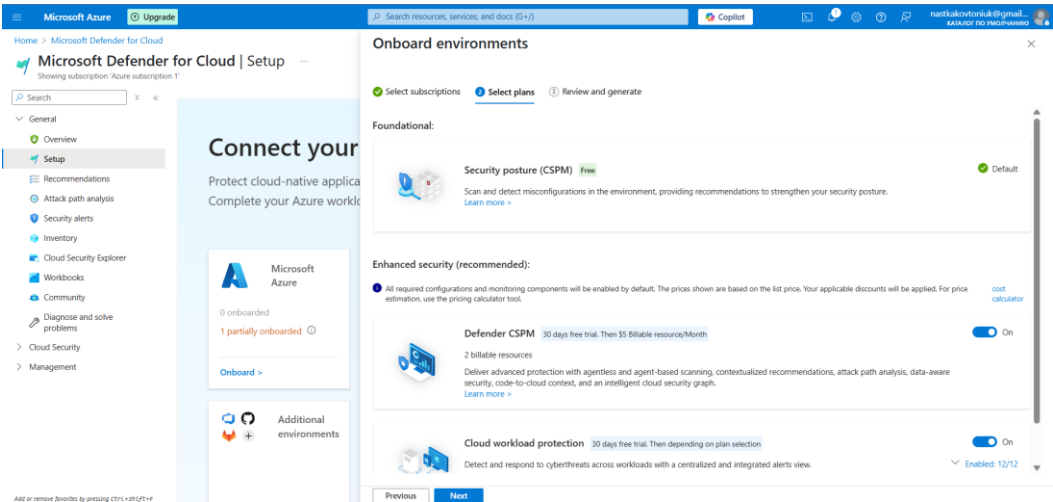


Рисунок 3.59. – Увімкнення базової політики

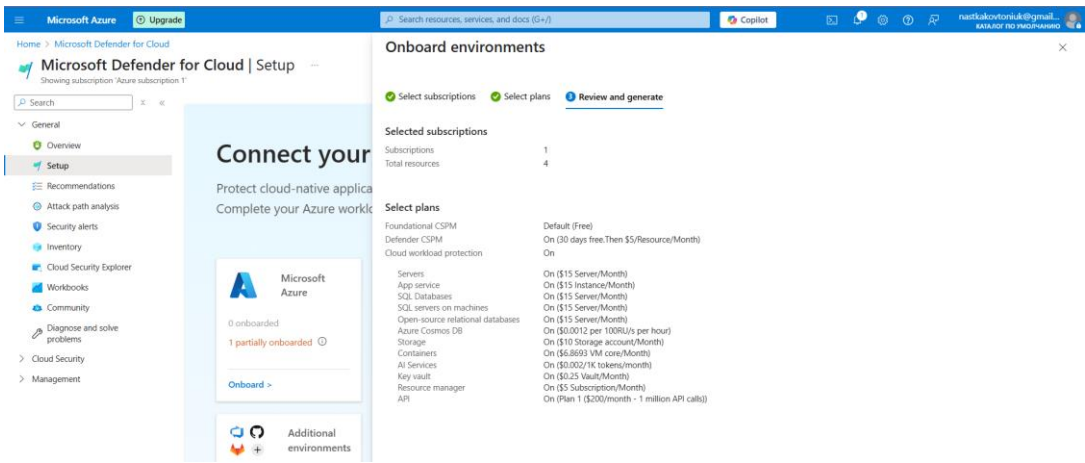


Рисунок 3.60. – Увімкнення базової політики

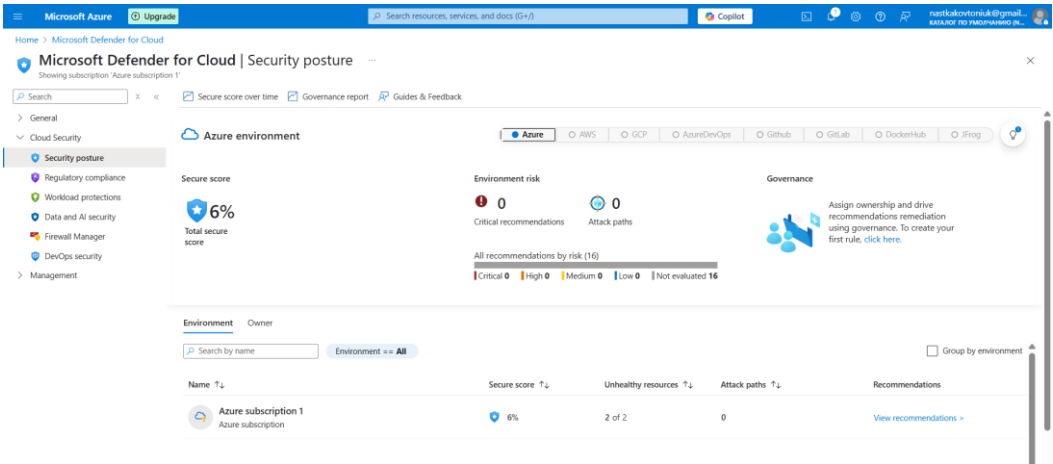


Рисунок 3.61. – Вкладка Microsoft Defender for Cloud

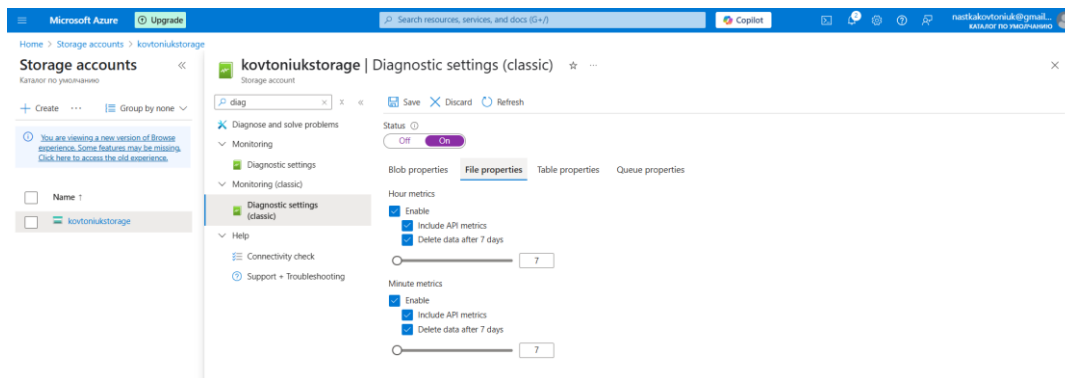


Рисунок 3.62. – Налаштування моніторингу

Після налаштувань (рис. 3.62) було проведено тест на коректну роботу Microsoft Defender for Cloud. Під час симуляції загрози було використано команду (рис. 3.63) –

powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden
\$ErrorActionPreference = 'silentlycontinue';(New-Object
System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\test-MDATP-
test\invoice.exe');Start-Process 'C:\test-MDATP-test\invoice.exe', де
- powershell.exe -NoExit -ExecutionPolicy Bypass — запускає PowerShell без
обмежень політики безпеки (небезпечно).

- DownloadFile(...) — намагається завантажити файл 1.exe з адреси
http://127.0.0.1/ (тобто з локального комп'ютера).

- Start-Process — відкриває файл invoice.exe, який щойно був збережений.

Якщо все проходить успішно, то нове сповіщення з'явиться у вкладці «Спо-
віщення Defender для хмари» через декілька хвилин (рис. 3.64), також прийде
сповіщення на пошту (рис. 3.65).

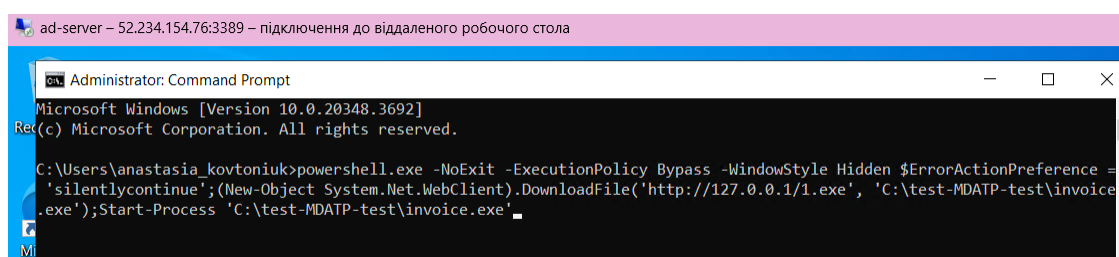


Рисунок 3.63. – Введення команди

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

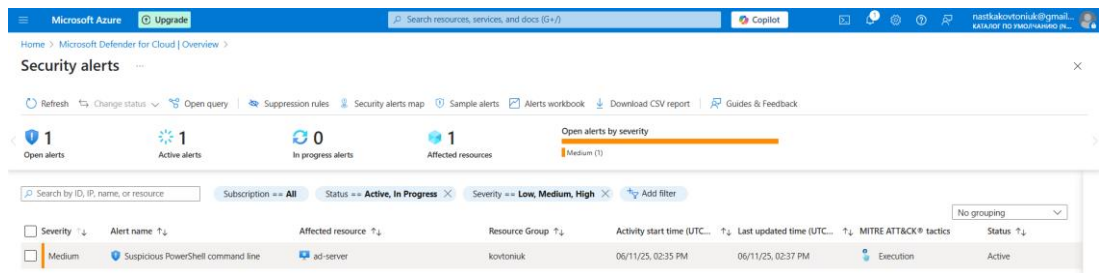


Рисунок 3.64. – Отримане сповіщення про небезпеку у вкладці «Сповіщення Defender для хмари»

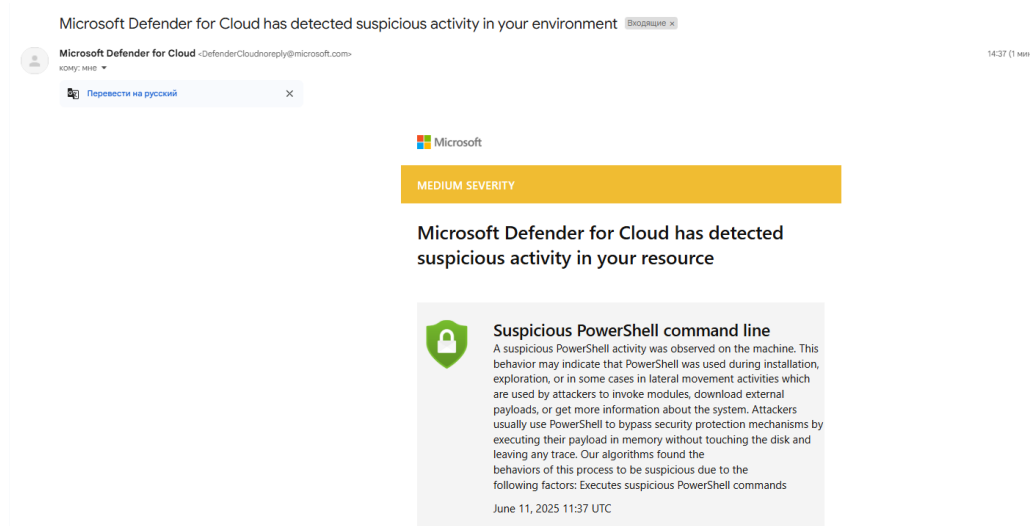


Рисунок 3.65. – Отримане сповіщення про небезпеку на пошту

Для резервного копіювання буде використовуватися Recovery Services vaults (рис. 3.66, рис. 3.67, рис. 3.68).

Recovery Services vaults — це об'єкт сховища в Azure, який містить дані. Дані зазвичай є копіями даних або інформацією про конфігурацію для віртуальних машин (ВМ), робочих навантажень, серверів або робочих станцій. Ви можете використовувати сховища служб відновлення для зберігання резервних даних для різних служб Azure, таких як віртуальні машини IaaS (Linux або Windows) та SQL Server у віртуальних машинах Azure. [21]

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

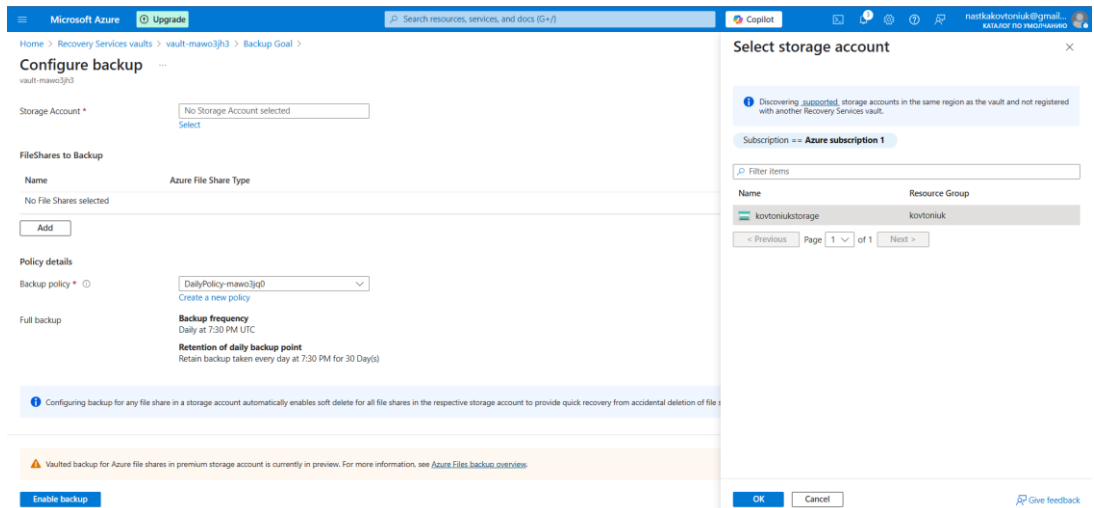


Рисунок 3.66.- Налаштування резервного копіювання

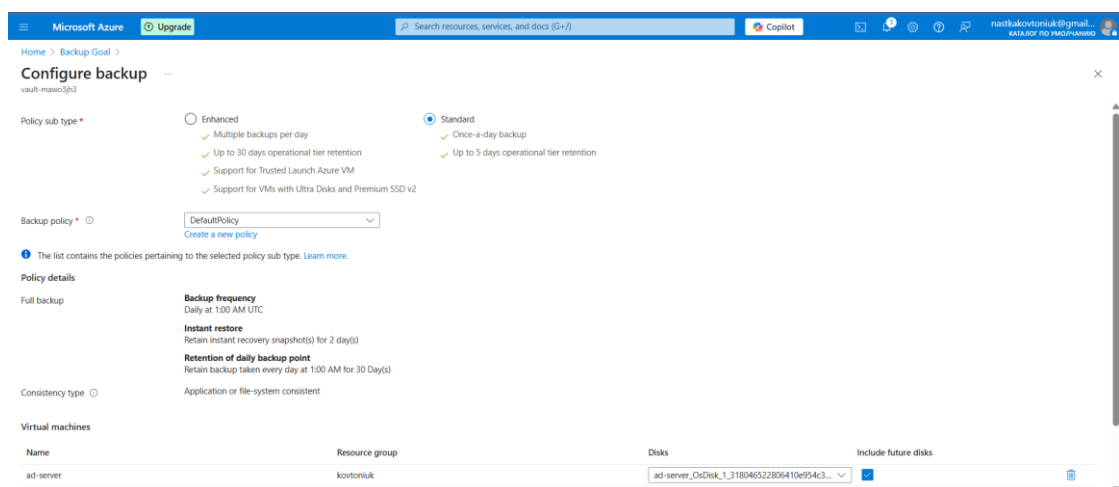


Рисунок 3.67. – Налаштування резервного копіювання

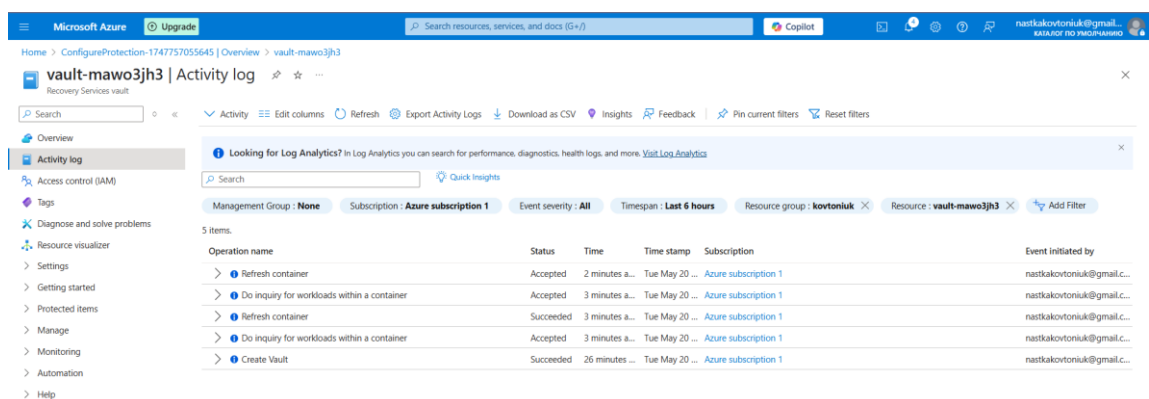


Рисунок 3.68. – Перевірка журналу аудиту

У рамках перевірки працездатності системи резервного копіювання було вручну запущено створення резервної копії віртуальної машини (рис. 3.69) через сервіс Azure Backup, а також спроба відновлення деяких файлів (рис. 3.71). Після завершення резервування в Recovery Vault з'явилася відповідна точка відновлення (рис. 3.70), а у звітах – підтвердження успішного виконання завдання, а після від-

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

новлення файлів був отриманий скрипт для підключення (рис. 3.72) та відповідні файли. Це доводить те, що Azure Backup функціонує коректно і забезпечує відновлення критичних даних за запитом.

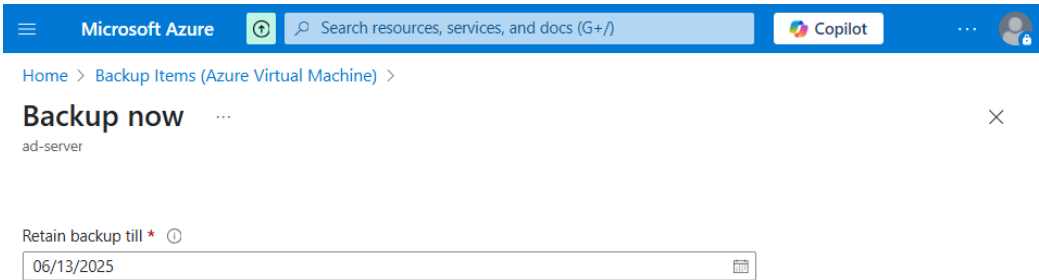


Рисунок 3.69. – Запуск резервного копіювання

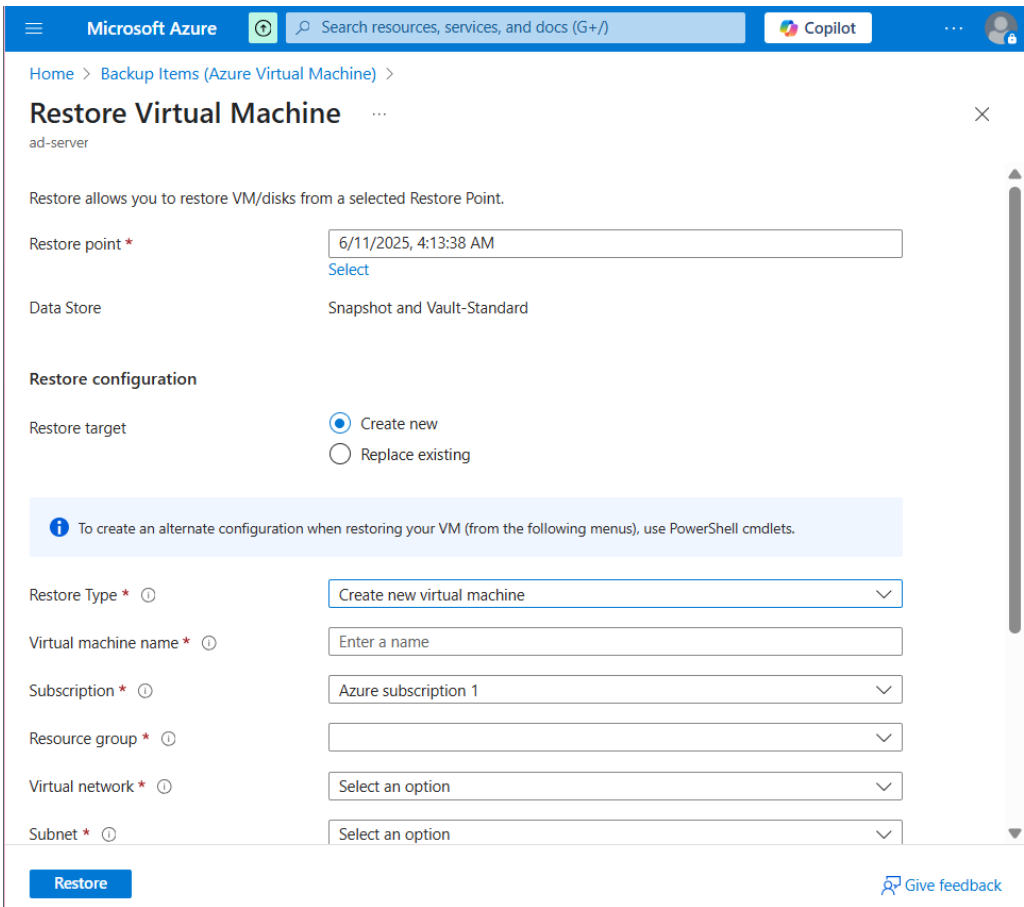


Рисунок 3.70. – Спроба відновлення віртуальної машини

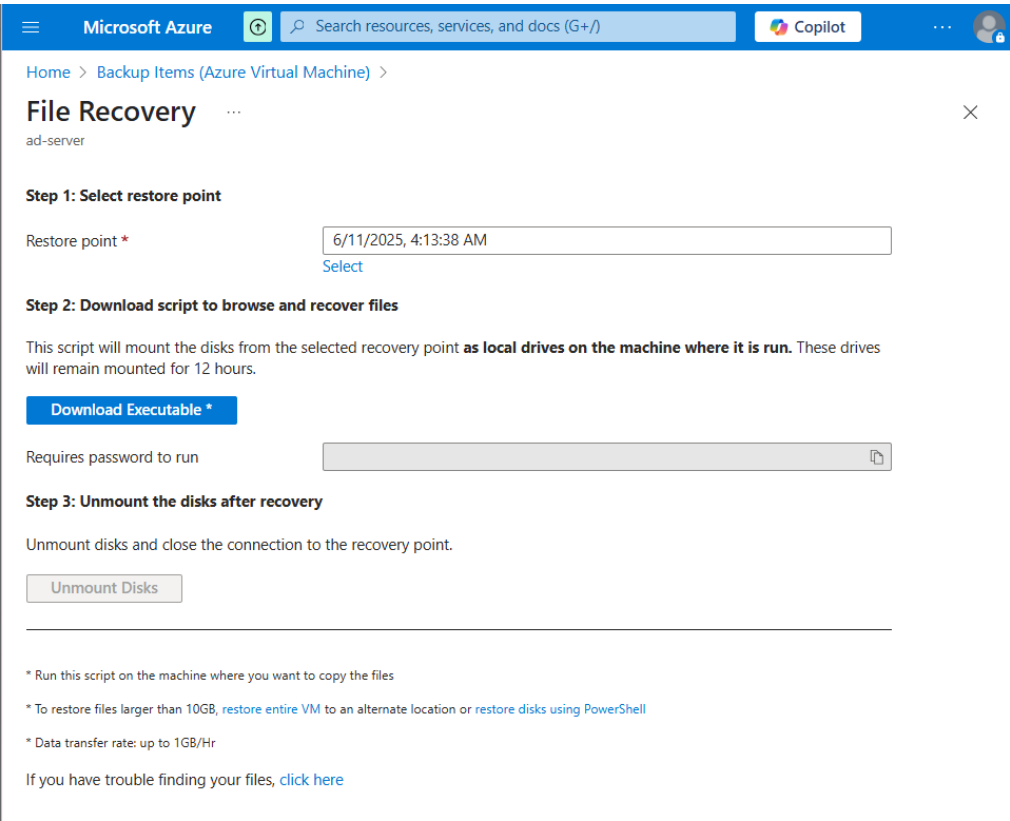


Рисунок 3.71. – Спроба відновлення окремих файлів

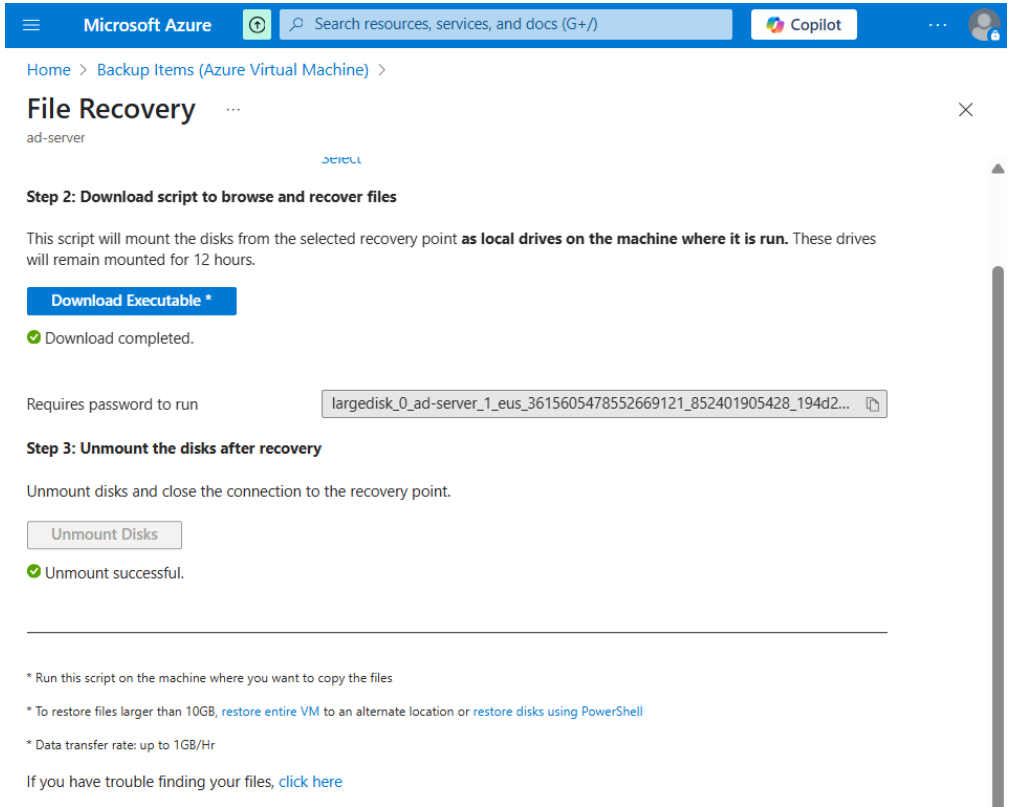


Рисунок 3.72. – Отримання скрипту для підключення диску до локальної машини

Ім'я	Дата змінення	Тип	Розмір
Сьогодні			
MicrosoftAzureBackupILRLogFile.log	11.06.2025 15:05	Текстовий докум...	4 КБ
SecureTCPTunnelLogFile.log	11.06.2025 15:05	Текстовий докум...	1 КБ
LegalNotice.txt	11.06.2025 15:05	Текстовий докум...	217 КБ
WindowsPowershellIISCSIScriptForILR.ps1	11.06.2025 15:05	Сценарій Window...	48 КБ
SecureTCPTunnel.exe	11.06.2025 15:03	Застосунок	305 КБ

Рисунок 3.73. – Отримані файли

В цьому підрозділі було налаштовано Microsoft Defender for Cloud та Azure Security Center для моніторингу та керування безпекою, після налаштування виконано тест на перевірку коректної роботи, який пройшов успішно. Для резервного копіювання було налаштовано Recovery Services vaults, після налаштування відбулася перевірка працездатності системи, де було створено резервну копію віртуальної машини та відновлено деякі файли.

Висновок до третього розділу

Третій розділ присвячений практичному аспекту – налаштуванню та тестуванню гібридної IT-інфраструктури на базі продуктів Microsoft. Основним етапом було налаштування та розгортання віртуальних машин в хмарному та локальному середовищі, а також створення тенанту (tenant) в Microsoft Azure. На віртуальних машинах (локальній та хмарній) було налаштовано AD DS, створено домени, організаційні одиниці та користувачів. Детально показано створення та додавання користувачів та груп в тенант (tenant), налаштовано віртуальну мережу. Ще одним важливим етапом було налаштування синхронізації між локальним та хмарним сервером за допомогою Microsoft Entra ID Connect Sync. Для передачі та обміну даних було налаштовано Azure File Share та перевірено його працездатність. Microsoft Defender for Cloud налаштовано для моніторингу та керування безпекою, після налаштування виконано тест на перевірку коректної роботи, який пройшов успішно. Для резервного копіювання використано Recovery Service vaults за допомогою якого було створено резервну копію віртуальної машини та відновлено деякі файли.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було спроектовано та розроблено гібридну IT-інфраструктуру організації на базі продуктів Microsoft, яка поєднує можливості локального середовища та функціоналу хмарної платформи Microsoft Azure. Теоретична частина базується на огляді основних понять про хмарні та гібридні IT-інфраструктури, а також їх переваги та недоліки. Розглянуто основні сервіси Microsoft, які забезпечують взаємодію між локальним і хмарним середовищем: Microsoft Entra ID, Active Directory, Azure File Share, Microsoft Entra Connect Sync, Microsoft Defender for Cloud та Azure Backup.

У практичній частині було реалізовано розгортання локального середовища на базі Windows Server 2019 Evaluation Edition із налаштуванням служб Active Directory, налаштування хмарного середовища Azure із створенням Microsoft Entra ID та віртуальної машини з Active Directory. Після чого було виконано синхронізацію облікових записів локального середовища з хмарним за допомогою Microsoft Entra Connect Sync. Організовано централізоване файлове сховище (Azure File Shares) в Azure та забезпечено доступ до нього з локальних машин. Налаштовано моніторинг безпеки та резервне копіювання. Проведено тестування окремих компонентів – синхронізації, доступу до ресурсів, сповіщень від Microsoft Defender for Cloud та виконання резервного копіювання.

Загалом, результати роботи підтверджують доцільність впровадження гібридної моделі на основі продуктів Microsoft у малих та середніх організаціях. Це рішення може бути використане як основа для побудови корпоративних інформаційних систем із сучасним рівнем безпеки та функціональності.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Інтеграція хмарних рішень з існуючими системами компанії [Електронний ресурс]. – Режим доступу: <https://wezom.com.ua/ua/blog/integratsiya-hmarnih-rishen-z-isnuyuchimi-sistemami-kompaniyi>
2. Типи хмарних обчислень – публічні, приватні, гібридні та спільноти [Електронний ресурс]. – Режим доступу: <https://www.guru99.com/uk/types-of-cloud-computing.html>
3. Хмарні технології: що це та які переваги надають людям для бізнесу [Електронний ресурс]. – Режим доступу: <https://gigacloud.ua/articles/hmarni-tehnologiyi-shho-cze-ta-yaki-perevagy-nadayut-lyudyam-ta-biznesu/>
4. AWS vs Azure vs Google Cloud [Електронний ресурс]. – Режим доступу: <https://cloudfresh.com/ua/cloud-blog/aws-vs-azure-vs-google-cloud/>
5. Що таке Microsoft Azure? [Електронний ресурс]. – Режим доступу: <https://simpla.com.ua/blog/shcho-take-microsoft-azure>
6. Що таке віртуалізація серверів і чому вона корисна? [Електронний ресурс]. – Режим доступу: <https://hyperhost.ua/info/uk/shho-take-virtualizaciya-serveriv-i-comu-vona-korisna>
7. Що таке віртуалізація сервера? [Електронний ресурс]. – Режим доступу: <https://introserv.com/ua/blog/shho-take-virtualizacziya-servera/>
8. Офіційний сайт VirtualBox [Електронний ресурс]. – Режим доступу: <https://www.virtualbox.org/>
9. Що таке віртуалізація? [Електронний ресурс]. – Режим доступу: <https://wiseit.com.ua/shho-take-virtualizacziya/>
10. Платформа Microsoft Azure [Електронний ресурс]. – Режим доступу: <https://techexpert.ua/it-products/platforma-microsoft-azure/>
11. Ubuntu – опис ОС: актуальні версії, плюси, мінуси [Електронний ресурс]. – Режим доступу: <https://hyperhost.ua/info/uk/ubuntu-opis-os-aktualni-versii-plyusi-minusi>
12. Переваги та недоліки OS Windows Server для виділеного сервера [Електронний ресурс]. – Режим доступу:

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

<https://fotocvetov.com/allinnews/wol&org&uu/blog/uk/vindovs-perevagi-ta-nedoliki-os-windows-server-dla-vidilenogo-servera-data-centr-unit-is>

13. Linux Server проти Windows Server: Вихідна продуктивність [Електронний ресурс]. – Режим доступу: <https://introserv.com/ua/blog/linux-server-proti-windows-server-vixidna-produktivnist/>

14. Що таке доменні служби Active Directory? [Електронний ресурс]. - Режим доступу: <https://mix.mak.v.ua/ukraincyam/shho-take-domenni-sluzhbi-active-directory.html>

15. Active Directory Domain Services (AD DS) [Електронний ресурс]. – Режим доступу: <https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Active-Directory-Domain-Services-AD-DS>

16. Ідентифікатор Microsoft Entra [Електронний ресурс]. – Режим доступу: <https://en.wikipedia.org/wiki/Microsoft Entra ID>

17. Що таке Azure AD Connect? [Електронний ресурс]. – Режим доступу: <https://pathlock.com/learn/azure-ad-connect-features-architecture-and-best-practices-2/>

18. Azure File Shares: A Beginner's Guide [Електронний ресурс]. – Режим доступу: <https://www.smikar.com/azure-file-shares-a-beginners-guide/>

19. Огляд Microsoft Defender для хмари [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>

20. Azure Security Center [Електронний ресурс]. – Режим доступу: <https://azuremarketplace.microsoft.com/en-us/marketplace/apps/microsoft.azuresecuritycenter?tab=overview>

21. Recovery Services vaults overview [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview>

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

Ідентифікація та автентифікація

Автентифікація та ідентифікація – це два важливих поняття в комп’ютерній безпеці.

Автентифікація – це процес перевірки особи користувача, що дає змогу отримати авторизований доступ до приватної інформації або системи.

Процес автентифікації – це комплексна процедура, яка включає кілька етапів захисту. Спочатку система запитує логін або e-mail користувача. Далі відбувається перевірка першого фактора автентифікації – це пароль. За підвищеного рівня безпеки система може запитати додаткові фактори автентифікації.

Існують різні методи автентифікації для забезпечення безпечного доступу:

1. Парольна автентифікація

Підтвердження входу за допомогою паролю залишається найпоширенішим методом захисту системи. Сучасні системи парольної автентифікації використовують складні алгоритми хешування для захисту паролів у базі даних.

2. Голосова автентифікація

Метод використовує унікальні характеристики голосу для ідентифікації особи. Користувач записує свій голос для зразку під час реєстрації, і за спроби входу система порівнює їх.

3. Біометрична автентифікація

Метод використовує унікальні біологічні характеристики людини для підтвердження особи. Сучасні системи використовують для цього відбитки пальців, риси обличчя або голос.

4. Двофакторна автентифікація (2FA)

Двофакторна автентифікація – це надійний метод захисту, який підвищує безпеку облікового запису. Принцип роботи 2FA базується на використанні паролю та телефону для отримання SMS або зчитування біометричних даних.

5. Токен-автентифікація

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

Це сучасний та надійний метод автентифікації, під час якого використовуються спеціальні пристрої або застосунки для генерації одноразових кодів доступу.

6. Автентифікація за сертифікатом

Метод використовує цифрові сертифікати. Документ містить відкритий ключ, ім'я власника та підпис центру сертифікації.

Ідентифікація – це процедура розпізнавання суб'єкта за його ідентифікатором (визначення імені, логіна або номера).

Вона виконується при спробі увійти в будь-яку систему. Мета ідентифікації – перевірити чи відомий індивід системі. Ідентифікатором може бути: номер телефону, номер паспорта, email та інше.

		Ковтонюк А.Д.			ККІКБ.КР.Б – 123 – 05 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		92