

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

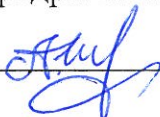
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему «Проект віртуалізованої серверної інфраструктури
корпоративної мережі на базі рішень ProxMox та Microsoft Windows»

Виконав: студент 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Олександр МАКАРОВ

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

 Олексій ШЕЛУХА

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

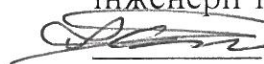
 Олена ГОЛОВНЯ

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
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Макаров Олександр Вікторович

Тема роботи: «Проект віртуалізованої серверної інфраструктури корпоративної мережі на базі рішень ProxMox та Microsoft Windows»

затверджена Наказом університету від 5 березня 2024 р. № 97

Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

Віртуальні середовища, сервер, віртуальні приватні мережі, процес віртуалізації серверної інфраструктури корпоративної мережі;

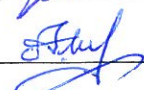
Обладнання та програмне забезпечення:

1. Віртуальні середовища VirtualBox та ProxMox;
2. Контролери домена Active Directory на базі Windows Server 2019,
клієнтські операційні системи Windows 10/11;

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І.Г.		

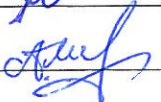
Студент  Олександр МАКАРОВ

Керівник  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.02.2024 – 10.03.2024	Вик.
2	Написання вступної частини кваліфікаційної роботи	10.03.2024 – 01.04.2024	Вик.
3	Аналіз теоретичних аспектів про сервер	01.04.2024 – 01.05.2024	Вик.
4	Проектування сервера та мережі	28.02.2024 – 10.03.2024	Вик.
5	Розгортання і налаштування віртуального середовища на сервері	02.05.2024 – 09.05.2024	Вик.
6	Створення і налаштування головного серверу	09.05.2024 – 16.05.2024	Вик.
7	Створення і налаштування термінального серверу	16.05.2024 – 21.05.2024	Вик.
8	Налаштування робочих станцій	21.05.2024 – 01.06.2024	Вик.
9	Налаштування OpenVPN	22.05.2024 – 01.06.2024	Вик.
10	Перевірка роботи розробленої системи	01.06.2024 – 05.06.2024	Вик.
10	Оформлення кваліфікаційної роботи	05.06.2024 – 09.06.2024	Вик.
11	Підготовка презентації до захисту	09.06.2024 – 29.06.2024	Вик.

Студент  Олександр МАКАРОВ

Керівник  Олексій ШЕЛУХА

АНОТАЦІЯ

Пояснювальна записка містить: 95 сторінки текстової частини, 107 рисунки, 1 таблиця та 21 літературних джерел.

Метою роботи є побудови віртуалізованої серверної інфраструктури корпоративної мережі на базі рішень Proxmox та Microsoft Windows.

В кваліфікаційній роботі розглядається процес розгортання віртуалізованої серверної інфраструктури для корпоративної мережі. В першому розділі розглянуто що з себе представляє сервер та його види, був проведений аналіз операційних систем для серверів, систем віртуалізації, проколів підключення VPN, а також визначено технічне завдання для теми “Проєкт віртуалізованої серверної інфраструктури корпоративної мережі на базі рішень Proxmox та Microsoft Windows”. В другому розділі, відповідно по поставлених завдань, проведено проектування топології для корпоративної мережі, налаштування серверної інфраструктури, яке включає віртуальне середовище, віртуальні машини, VPN-сервіс. В третьому розділі, згідно з проектування у другому розділі, висвітлено розгортання і налаштування середовища віртуалізації, розгортання і налаштування серверної частини, налаштування системи захищеного з’єднання за допомогою OpenVPN.

Ключові слова: СЕРВЕР, ВІРТУАЛЬНЕ СЕРЕДОВИЩЕ, WINDOWS SERVER 2019, OPENVPN, ACTIVE DIRECTORY, WINDOWS 10, WINDOWS 11, PROXMOX.

					ККІК.КР.Б – 123 – 14 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект віртуалізованої серверної інфраструктури корпоративної мережі на базі рішень ProxMox та Microsoft Windows	Літ.	Арк.	Аркушів	
Розроб.		Макаров О.В.		14.06					
Керівник		Шелуха О. О.		17.06			4	95	
Реценз.		Головня О.С.		17.06		ФІКТ, Гр. КІ-20-1			
Н. контр.		Шелуха О. О.		17.06					
Затверд.		Сфіменко А.А.		17.06					

ANNOTATION

The explanatory note contains: 95 pages of text, 107 figures, 1 table and 21 sources.

The purpose of the work is to build a virtualized server infrastructure for a corporate network based on Proxmox and Microsoft Windows solutions.

The qualification work examines the process of deploying a virtualized server infrastructure for a corporate network. The first section describes what a server is and its types, analyzes operating systems for servers, virtualization systems, VPN connection punctures, and defines the terms of reference for the topic “Project of virtualized server infrastructure for a corporate network based on Proxmox and Microsoft Windows solutions”. In the second section, in accordance with the tasks set, we designed topologies for the corporate network, configured the server infrastructure, which includes a virtual environment, virtual machines, and VPN service. The third section, in accordance with the design in the second section, covers the deployment and configuration of the virtualization environment, deployment and configuration of the server part, and setting up a secure connection system using OpenVPN.

Keywords: SERVER, VIRTUAL ENVIRONMENT, WINDOWS SERVER 2019, OPENVPN, ACTIVE DIRECTORY, WINDOWS 10, WINDOWS 11, PROXMOX.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД АРАТНО-ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ.....	9
1.1. Сучасний стан компонентів серверної інфраструктури	9
1.2. Аналіз серверних операційних систем	21
1.3. Огляд сучасних систем віртуалізації	25
1.4. Аналіз функціонування протоколів VPN	32
1.5. Постановка технічного завдання.....	41
Висновок до першого розділу:	42
РОЗДІЛ 2. ПРОЄКТУВАННЯ СЕРВЕРА ТА МЕРЕЖІ.....	43
2.1. Проєктування логічної та фізичної топології мережі	43
2.1.1. Фізична топологія.....	43
2.1.2. Логічна топологія	45
2.2. Розгортання серверу	46
2.3. Налаштування серверу	47
2.4. Налаштування VPN-сервісу.....	49
Висновок до другого розділу:	50
РОЗДІЛ 3. РОЗГОРТАННЯ СЕРВЕРУ І МЕРЕЖІ	51
3.1. Розгортання і налаштування прохтох на сервері.....	51
3.2. Розгортання і налаштування баскуп серверу прохтох	54
3.3. Створення і налаштування головного серверу	57
3.4. Створення і налаштування термінального серверу	75
3.5. Налаштування робочої станції	84
3.6. Налаштування OpenVPN.....	86
Висновок до третього розділу:	89
ВИСНОВКИ.....	91
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	93
ДОДАТКИ.....	96

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – Операційна Система

ПЗ – Програмне Забезпечення

VPN – Virtual Private Network

DNS – Domain Name System

IP – Internet Protocol

VE – Virtual Environment

BS – Backup Server

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

NTP – Network Time Protocol

DHCP – Dynamic Host Configuration Protocol

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. В сучасному інформаційному суспільстві, де велика кількість підприємств та організацій переходять до цифрового середовища, корпоративні мережі відіграють невід'ємну роль у забезпеченні ефективності та надійності обміну інформацією. Одним із ключових аспектів розробки та функціонування корпоративних мереж є правильне проєктування серверної частини, яка відповідає вимогам сучасного бізнесу.

Метою кваліфікаційної роботи є побудова віртуалізованої серверної інфраструктури корпоративної мережі з використанням Proxmox та Microsoft Windows.

Визначена мета обумовлює наступні завдання:

- Дослідити теоретичні відомості про сервер і віртуальні середовища.
- Спроектувати корпоративну мережу, розгортання і налаштування серверу.
- Розгортання і налаштування віртуального середовища на сервері.
- Розгортання і налаштування віртуальних машин на сервері.

Об'єктом дослідження є процес розгортання віртуалізованої серверної інфраструктури корпоративної мережі.

Предметом дослідження є віртуальне середовище Proxmox, операційна система Windows Server 2019, VPN-сервіс OpenVPN, служба Active Directory, протокол Remote Desktop.

У процесі виконання кваліфікаційної роботи було розгорнуто сервер для корпоративної мережі з Active directory, та можливістю віддаленого підключення до серверу у корпоративній мережі або через інтернет простір за допомогою OpenVPN.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД АРАТНО-ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ

1.1. Сучасний стан компонентів серверної інфраструктури

Сервер — це комп'ютер, який надсилає дані іншим комп'ютерам, підключеним до нього мережею, і керує мережевими ресурсами. Сервери з'єднують різні різні пристрої та дозволяють їм обмінюватися інформацією та доступом до програмного забезпечення. Ви можете використовувати сервер, щоб забезпечити потужність обробки, зберігання даних, послуги резервного копіювання даних або створити центральне розташування для керування даними. Сервери зазвичай мають великий об'єм пам'яті та потужні процесори. Вони призначені для цілодобової роботи та виняткової надійності, тому що вони необхідні для забезпечення доступності IT-послуг.

Часто вони розміщуються централізовано та обслуговуються системним адміністратором. На відміну від цього, на столах співробітників є простіші машини, які називаються клієнтами, за допомогою яких вони отримують доступ до віддалених даних, наприклад, для включення в електронні таблиці, які вони створюють. Клієнтська та серверна машини з'єднані мережею, як показано на рис.1.1. Зверніть увагу, що ми показали мережу у вигляді простого овалу без будь-яких деталей. Ми будемо використовувати цю форму, коли маємо на увазі мережу в найбільш абстрактному сенсі.

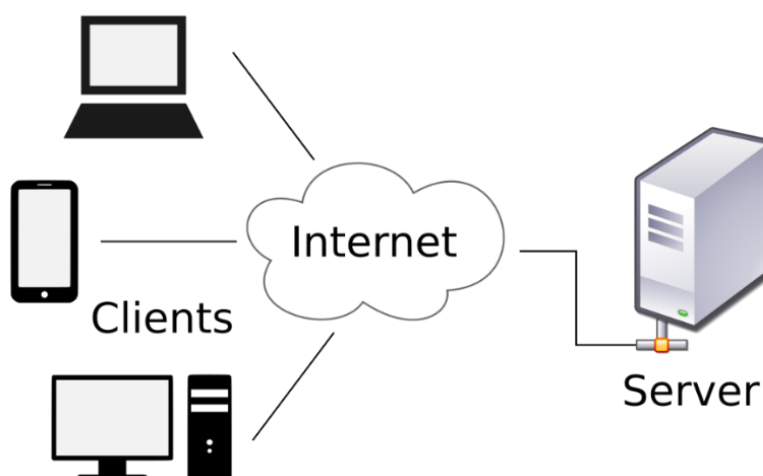


Рис. 1.1 – Мережа з трьома клієнтами та одним сервером

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

Вся ця система називається моделлю клієнт-сервер. Він широко використовується і є основою для широкого використання мережі. Найпопулярнішою реалізацією є веб-додаток, у якому сервер створює веб-сторінки на основі своєї бази даних у відповідь на запити клієнта, які можуть оновлювати базу даних. Модель клієнт-сервер застосовна, коли клієнт і сервер знаходяться в одній будівлі (і належать одній компанії), але також коли вони далеко один від одного. Наприклад, коли людина вдома отримує доступ до сторінки у Всесвітній павутині, використовується та сама модель, де віддалений веб-сервер є сервером, а персональний комп'ютер користувача – клієнтом. За більшості умов один сервер може обслуговувати велику кількість (сотні чи тисячі) клієнтів одночасно.

Якщо ми детально розглянемо клієнт-серверну модель, то побачимо, що задіяні два процеси: один на клієнтській машині, а інший на серверній. Комунікація приймає форму клієнтського процесу, який надсилає повідомлення через мережу серверному процесу. Потім процес клієнта чекає на повідомлення відповіді. Коли серверний процес отримує запит, він виконує потрібну роботу або шукає запитані дані та надсилає відповідь[1]. Ці повідомлення показано на рис.1.2.

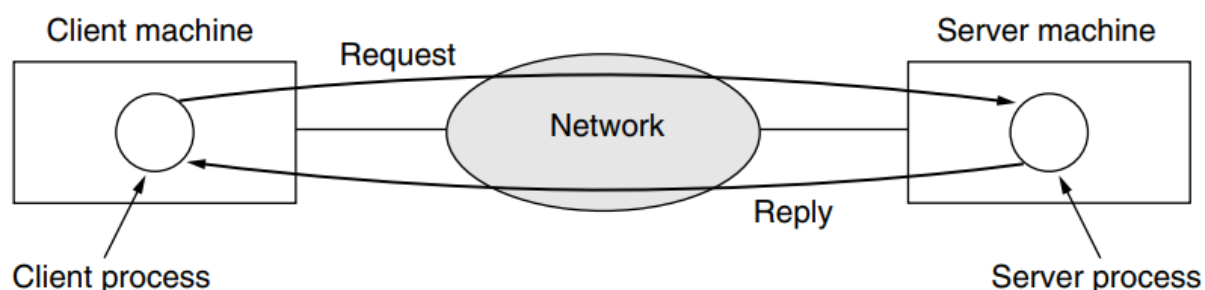


Рис. 1.2 – Модель клієнт-сервер, яка включає запити та відповіді

Доступ до більшої частини інформації у мережі здійснюється за допомогою моделі клієнт-сервер, але існує інша, популярна модель доступу до інформації, яка називається реєр-to-реєр зв'язком. У цій формі особи, які утворюють вільну групу, можуть спілкуватися з іншими в групі, як показано на рис.1.3. Кожна людина може спілкуватися з одним або кількома людьми. Сталого поділу на клієнтів і серверів немає.

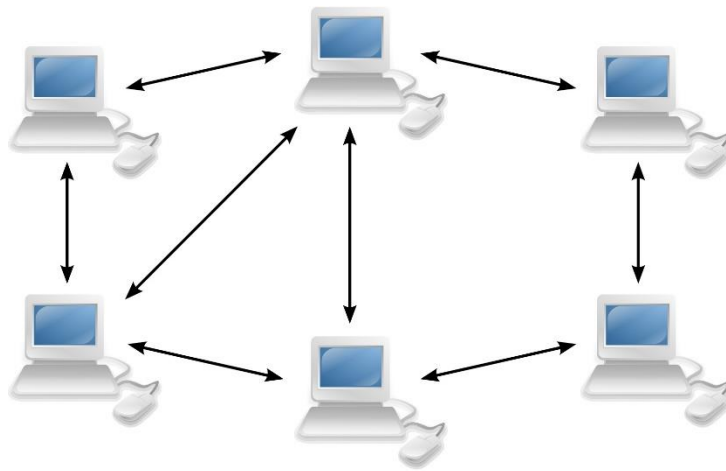


Рис. 1.3 – Модель peer-to-peer зв'язка

Багато peer-to-peer система, наприклад BitTorrent, не мають центральної бази даних вмісту. Замість цього кожен користувач підтримує власну базу даних локально та надає список інших людей поблизу, які є членами системи. Потім новий користувач може перейти до будь-якого існуючого учасника, щоб побачити, що він має, і отримати імена інших учасників для перевірки додаткового вмісту та інших імен. Цей процес пошуку можна повторювати нескінченно довго, щоб створити велику локальну базу даних про те, що існує. Це заняття, яке може стати втомливим для людей, але комп'ютери в цьому справляються.

Peer-to-peer зв'язок часто використовується для обміну музикою та відео. У 2000 році це стало справжнім успіхом із службою обміну музикою під назвою Napster, яку було закрито після, мабуть, найбільшої справи про порушення авторських прав за всю історію. Існують також легальні програми для однорангового спілкування. До них належать шанувальники, які діляться загальнодоступною музикою, або сім'ї, які діляться фотографіями та фільмами, а також користувачі, які завантажують публічні пакети програмного забезпечення. Фактично, одна з найпопулярніших інтернет-додатків, електронна пошта, за своєю суттю є peer-to-peer.

Існують багато видів серверів[2], но ми розглянемо тільки ті що можуть знадобитись для корпоративної, такі як:

1. Веб-сервер: Сервер, який відповідає за публікацію веб-сайту в Інтернеті, називається веб-сервером. Сервер, який надає хостинг, який також називається "хостинг", через Інтернет-протокол, називається веб-сервером. Оренда місця, необхідного для публікації веб-сторінок в Інтернеті, називається «хостинг». Хостинг означає розміщення сторінок, зображень або документів, призначених для веб-сайту, на комп'ютері, який користувачі Інтернету використовують для доступу до них. Apache, Microsoft Internet Information Server (IIS) і Nginx є найпопулярнішими веб-серверами в Інтернеті. Дані для кожного сайту, який ви бачите в Інтернеті, зберігаються на іншому хості та програмному забезпеченні під назвою Веб-сервер. Веб-сервер використовується для ефективного використання цього комп'ютера. Веб-сервери зазвичай складаються з численних програмних пакетів. Кожен із цих програмних пакетів допомагає керувати різними функціями. Наприклад, пакет протоколу передачі файлів (FTP), який постачається з програмним забезпеченням веб-сервера, допомагає серверу виконувати завдання FTP. Подібним чином доступні численні пакети для виконання різноманітних завдань, таких як обслуговування електронних листів, виконання запитів на завантаження та публікація веб-сторінок через HTTP.

Найпоширеніші веб-сервери:

- HTTP-сервер Apache: Apache Software Foundation створила найпопулярніший у світі веб-сервер. Apache — це веб-сервер із відкритим вихідним кодом, який можна встановити на Linux, Unix, Windows, FreeBSD, Mac OS X та багатьох інших операційних системах. Веб-сервер Apache використовується понад 60% комп'ютерів веб-серверів.
- Internet Information Server: інформаційний сервер Інтернету (IIS) від Microsoft — це високопродуктивний веб-сервер.
- Lighttpd: Lighttpd, вимовляється як легкий, — це безкоштовний веб-сервер, який постачається з операційною системою FreeBSD. Цей веб-сервер із відкритим вихідним кодом швидкий, безпечний і споживає набагато менше

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

потужності ЦП. Lighttpd також можна запускати в Windows, Mac OS X, Linux і Solaris.

- Nginx: веб-сервер Nginx є критично важливим компонентом обчислювального середовища клієнт-сервер, який надає клієнтським системам важливу для бізнесу інформацію. Як і Lighttpd, це веб-сервер із відкритим вихідним кодом, який відомий своєю швидкістю та потребує небагато ресурсів і часу для налаштування. Здебільшого він використовується для кешування, потокового мультимедіа, балансування навантаження, керування статичними файлами, автоматичного індексування та інших подібних завдань. Nginx обробляє запити в одному потоці, використовуючи асинхронну техніку, а не генеруючи нові процеси для кожного запиту, зробленого користувачем.
- Веб-сервер Sun Java System: веб-сервер Sun Microsystems призначений для середніх і великих веб-сайтів. Сервер є безкоштовним, але не має відкритого коду. З іншого боку, він працює на платформах Windows, Linux і Unix. Веб-сервер Sun Java System підтримує широкий спектр мов, сценаріїв і технологій Web 2.0, включаючи JSP, Java Servlets, PHP, Perl, Python, Ruby on Rails, ASP і Coldfusion.

2. Сервер бази даних: Сервер бази даних керує базою даних і надає послуги бази даних клієнтам. Сервер керує доступом до даних і пошуком, а також виконанням запитів клієнта. Сервер бази даних — це комп'ютер, на якому працює програмне забезпечення бази даних і призначений для надання послуг бази даних. Сервер бази даних складається з апаратного та програмного забезпечення, яке використовується для запуску бази даних.

Сервери баз даних мають різноманітні програми. Серед них:

- Регулярна робота з великими обсягами даних. Сервери баз даних сяють у клієнт-серверних архітектурах, де клієнти часто обробляють дані.
- Управління відновленням і безпекою СУБД (системи управління базами даних). Сервери баз даних забезпечують виконання обмежень, визначених у

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

СУБД. Сервер керує всіма підключеними до нього клієнтами, а також усіма запитамі доступу до бази даних і керування ними.

- Забезпечується одночасний контроль доступу. Сервери баз даних забезпечують багатокористувацьке середовище, в якому кілька користувачів можуть отримати доступ до бази даних одночасно, зберігаючи безпеку та приховуючи СУБД від клієнтів.
- Сховище файлів програм і не баз даних. Сервери баз даних є набагато ефективнішим рішенням для деяких організацій, ніж файлові сервери.

Більшість серверів баз даних використовують модель клієнт-сервер. Вони отримують запити від клієнтських пристроїв та їхніх користувачів, а потім надсилають відповідь, яку запитували. Сервери баз даних — це потужні машини, які можуть підключатися до кількох баз даних і обслуговувати ресурси клієнтам, іноді за допомогою серверів додатків і веб-серверів, які діють як посередники. Бази даних, наприклад, можуть надавати ресурси клієнтам за відсутності веб-сервера або сервера додатків.

Найпоширеніші сервери баз даних:

- Oracle: Oracle — це база даних, яка найчастіше використовується для адміністрування об'єктно-реляційної бази даних, а остання версія — 12c (12 Cloud Computing). Він підтримує різні версії Linux, Windows і UNIX.
- IBM DB2: IBM DB2 було розроблено на мовах C, C++ і Assembly та вперше було випущено в 1983 році. Його налаштування та процедури встановлення прості, як і доступ до даних. Як результат, це допомагає зберігати великі обсяги даних, аж до петабайт.
- Microsoft SQL Server: цей сервер вперше був представлений у 1989 році. Він написаний кількома мовами, зокрема асемблером, C, Linux і C++. Він може працювати з Linux і Windows. Це дозволяє кільком користувачам використовувати ту саму базу даних одночасно.
- MySQL: MySQL стає все більш популярним для багатьох веб-додатків. Вона доступна як безкоштовна, так і преміальна версія.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- SAP HANA: створено компанією SAP SE і може керувати даними як SAP, так і не SAP. Він здатний підтримувати OLTP, OLAP і SQL. Він може спілкуватися з широким спектром різних програм.
- MS Access: він сумісний лише з Microsoft Windows. Оскільки ця система керування базами даних є недорогою, її зазвичай використовують для веб-сайтів електронної комерції.

3. DNS-сервер: Система доменних імен (DNS) — це телефонний довідник Інтернету. DNS відповідає за пошук правильної IP-адреси для веб-сайтів, коли користувачі вводять свої доменні імена, наприклад «google.com» або «nytimes.com», у веб-браузерах.

Потім ці адреси використовуються браузерами для зв'язку з початковими серверами або крайовими серверами CDN для доступу до інформації веб-сайту. Усе це можливо завдяки DNS-серверам, які є спеціалізованими машинами для відповідей на запити DNS.

Для розпізнавання імен система DNS має системи розпізнавання. Резолвери імен використовуються для пошуку IP-адрес, пов'язаних із доменними іменами. DNS-клієнти — це люди, які використовують розпізнавальні пристрої. Система DNS може мати багато розпізнавачів імен. У результаті, якщо один з них стає недієздатним, інші беруться за це і забезпечують, щоб зв'язок не порушувався.

Коли ви вводите доменне ім'я у свій браузер і входите в систему, ваш браузер спочатку запитує вашу операційну систему про доменне ім'я, яка не відповідає. Потім він запитує ваш модем і продовжує запитувати, доки не досягне Інтернет-провайдера та основних серверів DNS.

Якщо відповідна база даних DNS-сервера містить еквівалент цього доменного імені, вона відповість на IP-адресу, і ваш браузер отримає цю відповідь за частки секунди та зв'яжеться з сервером, на якому розміщено відповідне доменне ім'я. Потім розпочнеться передача даних, і потрібна веб-сторінка відобразиться у вашому браузері.

4. Файловий сервер: Файловий сервер — це центральний сервер у комп’ютерній мережі, який обслуговує файлові системи або частини файлових систем для клієнтів, підключених до мережі. Як наслідок, файлові сервери надають користувачам центральне місце зберігання файлів на внутрішніх носіях даних, доступне всім авторизованим клієнтам. Адміністратор сервера встановлює суворі вказівки щодо того, які користувачі мають які права доступу: наприклад, конфігурація або авторизація файлів окремої файлової системи дозволяє адміністратору вказати, до яких файлів певний користувач або група користувачів може мати доступ і відкривати, а також чи дані можна лише побачити або додатково додати, змінити чи видалити.

Користувачі можуть отримувати доступ до файлів через локальну мережу, а також віддалено, якщо файлові сервери підключено до Інтернету та налаштовано належним чином. Це дозволяє користувачам переглядати та зберігати файли на файловому сервері, коли вони перебувають у русі. Усі поточні операційні системи, такі як Windows, Linux або macOS, можна використовувати на файловому сервері, але мережеві пристрої мають бути сумісні з операційною системою. Однак файлові сервери використовуються не тільки для зберігання та адміністрування файлів. Вони також часто використовуються як резервний сервер і як сховище для програм, які мають бути доступні численним учасникам мережі.

Клієнти можуть отримати доступ до віддаленої файлової системи лише через файлові сервери. Вони можуть зберігати будь-який матеріал, наприклад виконувати файли, документи, зображення або фільми. Вони зазвичай зберігають дані у вигляді двійкових блоків або файлів. Це означає, що вони не виконують подальшої індексації чи обробки файлів, які зберігають. Однак можуть існувати інші плагіни або серверні операції, які можуть надавати додаткові функції. Файловий сервер не має вбудованих методів для взаємодії з даними, і для цього покладається на клієнта. Оскільки бази даних обробляють лише структуровані дані, отримані за допомогою запиту, вони не вважаються файловими серверами.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Файлові сервери зазвичай містять додаткові можливості, які дозволяють кільком користувачам використовувати їх одночасно: Керування дозволами використовується для контролю того, хто має доступ до певних файлів і хто має повноваження змінювати або видаляти їх. Блокування файлу не дозволяє кільком людям одночасно редагувати той самий файл. Вирішення конфліктів; збереження цілісності даних у разі перезапису файлу. Дублюючи дані на численні сервери в різних місцях, розподілена файлова система може зробити дані надлишковими та доступними.

Для багатьох підприємств використання файлового сервера є доцільним з різних причин. Першою перевагою є, очевидно, центральність, яка гарантує, що будь-який авторизований учасник мережі має доступ до збережених даних.

Це дає змогу спільно працювати над певними файлами. Конфлікти між кількома версіями документа можуть бути практично усунені, оскільки певні операції, наприклад редагування або видалення, недоступні для інших користувачів, щойно ви отримуєте доступ до файлу. Якщо користувачам доводиться ділитися необхідними файлами у своїй системі або надсилати їх через знімний носій, це займе значно більше часу та незручностей, і це майже напевно призведе до появи різних версій файлів.

Іншою значною перевагою використання файлових серверів є те, що це зменшує навантаження на клієнтські ресурси. За винятком особистих документів, майже всі корпоративні дані та резервні копії можна зберігати на файловому сервері, залежно від того, як організація збирається використовувати сховище файлів. А за належного розташування (каталоги, папки тощо) користувачі отримують набагато кращу перспективу повної інвентаризації файлів.

5. DHCP-сервер: Сервер DHCP — це мережевий сервер, який автоматично надає та призначає IP-адреси, шлюзи за замовчуванням та іншу мережеву інформацію клієнтським пристроям. Щоб відповісти на широкомовні запити клієнта, він використовує стандартний протокол, відомий як Dynamic Host Configuration Protocol або DHCP.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Сервер DHCP автоматично надсилає мережеві параметри, необхідні клієнтам для успішного спілкування в мережі. Без цього адміністратор мережі повинен вручну налаштувати кожного клієнта, який підключається до мережі, що може зайняти багато часу, особливо у великих мережах.

Сервери DHCP зазвичай призначають унікальну динамічну IP-адресу кожному клієнту, яка змінюється, коли закінчується термін оренди цієї IP-адреси.

Кожному пристрою, підключеному до Інтернету в IP-мережі, має бути призначена унікальна IP-адреса. DHCP дозволяє менеджерам мережі централізовано контролювати та призначати IP-адреси. Коли комп'ютер переміщується, він може автоматично надати йому нову IP-адресу. DHCP автоматизує процес розподілу IP-адрес, скорочуючи як час, необхідний для налаштування та розгортання пристрою, так і ймовірність помилок конфігурації. Сервер DHCP також може керувати налаштуваннями кількох сегментів мережі. Коли змінюється конфігурація сегмента мережі, адміністратору потрібно лише оновити відповідні параметри на сервері DHCP.

Конфігурація надійної IP-адреси. DHCP зменшує проблеми конфігурації IP-адреси вручну, наприклад друкарські помилки та конфлікти адрес, викликані призначенням IP-адреси декільком комп'ютерам одночасно. Адміністрування мережі спрощено. Щоб зменшити адміністрування мережі, DHCP підтримує такі функції:

- Конфігурація TCP/IP централізована та автоматизована. Можливість визначати налаштування TCP/IP з однієї точки контакту.
- Можливість використовувати DHCP для призначення різноманітних додаткових параметрів конфігурації TCP/IP. Ефективне керування змінами IP-адрес для клієнтів, які потрібно часто оновлювати, наприклад портативних пристроїв, які переміщуються по бездротовій мережі.

6. NTP-сервер: Протокол мережевого часу (NTP) — це Інтернет-протокол, який використовується для синхронізації з джерелами часу годинника комп'ютера в мережі. Він належить і є одним із найперших компонентів набору TCP/IP. Слово

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

NTP стосується як протоколу, так і клієнт-серверних програм, які працюють на комп'ютерах. Він призначений для надзвичайної відмовостійкості та масштабованості, а також дозволяє тимчасову синхронізацію.

Після синхронізації клієнт оновлює годинник приблизно кожні 10 хвилин, потребуючи лише одного обміну повідомленнями на додаток до синхронізації клієнт-сервер. Ця транзакція відбувається на порту 123 протоколу дейтаграм користувача (UDP). NTP також забезпечує синхронізацію трансляції годинника комп'ютера.

Точний час для всіх пристроїв у комп'ютерній мережі є критичним з кількох причин; навіть частка секунди може спричинити проблеми. Нижче наведено деякі приклади використання NTP:

- Для розподілених процедур потрібен скоординований час, щоб гарантувати дотримання належної послідовності.
- Послідовний відлік часу в мережі потрібен для процедур безпеки.
- Зміни файлової системи, які виконуються на кількох машинах, залежать від синхронізованого часу.
- Щоб контролювати продуктивність і виправляти проблеми, системи прискорення мережі та керування мережею покладаються на точність часових позначок.

7. Сервер Syslog: Протокол системного журналювання (Syslog) — це стандартний формат повідомлень, який використовується мережевими пристроями для підключення до сервера журналювання. Він був створений, перш за все, щоб зробити моніторинг мережеских пристроїв простим. Пристрої можуть використовувати агент Syslog для надсилання сповіщень за різними сценаріями.

Ці повідомлення журналу містять позначку часу, рейтинг серйозності, ідентифікатор пристрою (включно з IP-адресою) та інформацію про подію. Хоча він має недоліки, протокол Syslog широко використовується, оскільки він простий у створенні та дуже відкритий, що дозволяє використовувати різноманітні власні

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

реалізації та, отже, можливість контролювати практично будь-який підключений пристрій.

Стандарт Syslog визначає три рівні:

- Syslog Content Layer: це вміст повідомлення про подію. Він містить кілька елементів даних, таких як коди закладів і рейтинги серйозності.
- Syslog Application Layer: повідомлення генерується, інтерпретується, маршрутизується та зберігається на цьому рівні.
- Syslog Transport Layer: цей рівень відповідає за надсилання повідомлень через мережу.

Під час усунення труднощів інформація журналу є досить корисною. Наприклад, якщо деякі користувачі повідомляють про збій у роботі мережі, як-от нещодавні збої у роботі Facebook, WhatsApp та Instagram, ми можемо просто просканувати всі дані журналу, щоб перевірити, чи не було проблем. Зберігання даних є ще однією перевагою централізованого зберігання інформації журналу. Він може надати тимчасову інформацію, необхідну для відновлення попереднього стану системи після збою.

Повідомлення системного журналу передаються через порт 514 протоколу дейтаграм користувача (UDP). Оскільки UDP є протоколом без підключення, повідомлення не підтверджуються та не гарантуються, що вони надходять. Це може бути недоліком, але це також робить систему базовою та легкою в управлінні.

Повідомлення системного журналу часто мають формат, зрозумілий людині, але це не обов'язково. Кожне повідомлення має рівень пріоритету в заголовку, який є поєднанням коду для процесу створення пристроєм повідомлення та рівня серйозності. Коди процесу, відомі як "об'єкти", засновані на UNIX. Рівні серйозності варіюються від 0 (надзвичайна ситуація) до 1 (потрібна термінова допомога), а інформаційні та налагоджувальні повідомлення знаходяться десь посередині. У поєднанні ці два коди дозволяють швидко класифікувати повідомлення Syslog.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

8. Фізичний сервер: Деякі сервери використовуються виключно для певних функцій. Наприклад, сервер додатків просто розміщує веб-сторінку. Фізичні сервери легко використовувати для широкого спектру мережеских завдань завдяки їх програмному та апаратному забезпеченню. Деякі з цих операцій:

- Оновлення операційної системи
- Сервіси для брандмауерів
- Програмне забезпечення для захисту від спаму
- Антивірусне програмне забезпечення
- Захист від DDoS атак
- Хостинг DNS
- Виявлення вторгнень
- Управління SNMP
- Адміністрування бази даних
- Резервне копіювання та відновлення
- Процедури безпеки

1.2. Аналіз серверних операційних систем

Серверна операційна система (ОС) — це операційна система, яка встановлюється та використовується на серверах для керування апаратними та програмними ресурсами сервера та надання послуг багатьом програмам.

Серверні операційні системи оптимізовані для надання більш розширених можливостей і функцій для архітектур клієнт-сервер або корпоративних ІТ-середовищ. А серверні операційні системи націлені на мережу, а не на одного користувача, тому вони можуть працювати з декількома робочими столами та спрощують адміністрування та зменшують простой.

Більшість серверів можуть підтримувати широкий спектр операційних систем. Кожна серверна ОС має свої переваги і недоліки. Нижче наведено найпоширеніші серверні операційні системи на ринку[3]:

1. Windows Server: Microsoft розробила сімейство операційних систем Windows для повсякденного особистого використання та професійного

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

використання на серверах. ОС Windows Server підтримує керування на корпоративному рівні, зберігання даних і широкий спектр програм.

Windows Server підтримує керування віртуальною пам'яттю, повний графічний інтерфейс робочого столу, дозволяє багатозадачність і підтримує різні периферійні пристрої. Корпорація Майкрософт зазвичай надає 10 років підтримки Windows Server.

Перевагами серверної ОС Windows є інтуїтивно зрозумілий графічний інтерфейс користувача, підтримка симетричних багатопроцесорних систем, чудова підтримка програм сторонніх розробників і багато версій на вибір. Мінусами є потреба в ліцензуванні на основі користувачів і більше загроз безпеки від вірусів порівняно з іншими платформами.

2. Linux: Linux — це сімейство UNIX-подібних операційних систем, які мають усі функції UNIX. Це відкритий вихідний код, доступний безкоштовно, що полегшує багатокористувацькі, багатопроцесні та багатопотокові операції. Однак сервери Linux вимагають більше технічних знань - від установки до обслуговування та виправлення помилок.

Одна з найпоширеніших платформ для розміщення веб-сайтів, стек LAMP, базується на Linux (Linux, Apache, MariaDB/MySQL, Perl/PHP/Python).

Деякі з найпопулярніших серверних дистрибутивів Linux:

- Сервер Ubuntu.
- Сервер Debian.
- Fedora.
- OpenSUSE Leap.
- Корпоративний сервер SUSE Linux.
- Arch Linux.

Перевагами серверної ОС Linux є висока безпека, широкий вибір дистрибутивів, інтегроване програмне забезпечення з відкритим вихідним кодом,

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

включаючи компілятори мов високого рівня, і можливість керувати системою за допомогою графічного інтерфейсу користувача.

Мінусами є відсутність довгострокової підтримки деяких дистрибутивів і певних складних операцій, таких як оновлення системи.

3. Red Hat Enterprise Linux: RHEL — це платний дистрибутив Linux для робочого столу та сервера, створений Red Hat. Спочатку RHEL був випущений як Red Hat Linux Advanced Server, а пізніше перейменований на Red Hat Enterprise Linux AS, який включав два дистрибутиви - Red Hat Enterprise Linux ES і Red Hat Enterprise Linux WS.

Вихідний код RHEL є у вільному доступі, але Red Hat використовує суворі правила, які обмежують перерозподіл офіційної версії ОС Linux. Ці обмеження не застосовуються до похідних продуктів третіх сторін, які не містять невірних компонентів, таких як торгові марки Red Hat.

Перевагами RHEL є широка підтримка та доступні виправлення, оновлення та рішення для уразливих місць безпеки. Мінуси RHEL – дорогі навчальні курси та відсутність персоналізованих рішень.

4. UNIX: На початку UNIX була операційною системою з розподілом часу для невеликих комп'ютерів, а з часом вона стала однією з найпоширеніших операційних систем клієнт-серверного середовища. Мова програмування UNIX — C, що полегшило створення портів UNIX для багатьох машин.

Перевагами UNIX є багатокористувацьке середовище, вбудована підтримка TCP/IP і високий рівень стабільності та безпеки.

Недоліком є те, що він платний, а різні постачальники продають різні версії UNIX, тому стандартної версії UNIX немає.

5. NetWare: Novell NetWare — це серверна мережева операційна система, для роботи якої потрібен виділений сервер. Це була широко поширена ОС у ранніх локальних мережах.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Плюси NetWare полягають у підтримці мультипроцесорів і великої ємності управління фізичною пам'яттю, а також у першокласних функціях обміну файлами та друку в корпоративних мережах. ОС також пропонує широкий спектр інтерфейсів керування, включаючи веб-інтерфейс.

Мінуси: ціна, погана підтримка, складний процес встановлення та низька підтримка сторонніх програм.

6. MacOS Server: MacOS Server — це UNIX-подібна серверна операційна система на основі macOS, розроблена Apple. ОС створена на основі macOS і додає функції сервера та інструменти системного адміністрування, а також інструменти для керування пристроями macOS та iOS.

MacOS Server — чудовий вибір, якщо ви використовуєте клієнти Mac у своїй мережі, враховуючи його здатність легко створювати функції для клієнтів Mac.

Перевагами macOS Server є просте адміністрування, інтуїтивно зрозумілий графічний інтерфейс, чудова підтримка та простий розподіл робочого навантаження між кількома машинами. Таким чином, легко збільшити потужність обробки. ОС поставляється з необмеженою ліцензією користувача.

Мінуси полягають у тому, що macOS Server працює лише на апаратному забезпеченні Apple, яке може бути дорогим, а сторонніх програм не так багато. Крім того, незважаючи на те, що Apple використовує програмне забезпечення з відкритим кодом у своїй системі, є зміни, характерні для macOS, які вимагають вирішення деяких проблем, яких немає в Linux.

7. FreeBSD: FreeBSD — це безкоштовна Unix-подібна операційна система з відкритим кодом. ОС підтримує повну систему, надаючи ядро, драйвери, утиліти та документацію, а також містить велику колекцію програмного забезпечення, пов'язаного з сервером. Таким чином, FreeBSD легко налаштувати як поштовий сервер, веб-сервер, брандмауер тощо.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

FreeBSD має свою групу безпеки, яка перевіряє все програмне забезпечення, що постачається з базовим дистрибутивом, і дозволяє інсталювати програми сторонніх розробників із бінарних пакетів.

Плюси FreeBSD полягають у тому, що він швидкий, абсолютно безкоштовний, має хороший захист, який використовує брандмауер ipfw, і має багато доступних інструментів, які належать команді FreeBSD.

Мінуси FreeBSD полягають у тому, що її не дуже легко освоїти, оскільки вона має слабкішу підтримку спільноти, ніж Linux, і не має підтримки драйверів

1.3. Огляд сучасних систем віртуалізації

Віртуалізація — це процес, який дозволяє більш ефективно використовувати фізичне комп'ютерне обладнання та є основою хмарних обчислень.

Віртуалізація використовує програмне забезпечення для створення рівня абстракції над апаратним забезпеченням комп'ютера, що дозволяє розділити апаратні елементи одного комп'ютера — процесори, пам'ять, сховище тощо — на кілька віртуальних комп'ютерів, які зазвичай називають віртуальними машинами (ВМ). Кожна віртуальна машина працює під керуванням власної операційної системи (ОС) і поводить себе як незалежний комп'ютер, навіть якщо вона працює лише на частині базового комп'ютерного обладнання.

Звідси випливає, що віртуалізація дозволяє ефективніше використовувати фізичне комп'ютерне обладнання та забезпечує більшу віддачу від інвестицій організації в обладнання.

Контроль над віртуальними машинами проходить через гіпервізор. Гіпервізор (також відомий як монітор віртуальної машини) — це тип комп'ютерного програмного забезпечення, вбудованого або апаратного забезпечення, яке створює та запускає віртуальні машини. Комп'ютер, на якому гіпервізор запускає одну або декілька віртуальних машин, називається хост-машиною, а кожна віртуальна машина — гостьовою машиною. Гіпервізор надає гостьовим операційним системам віртуальну операційну платформу та керує виконанням гостьових операційних систем. На відміну від емулятора, гостьова

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

система виконує більшість інструкцій на рідному обладнанні. Кілька примірників різноманітних операційних систем можуть спільно використовувати віртуальні апаратні ресурси: наприклад, примірники Linux, Windows і macOS можуть працювати на одній фізичній машині x86.

Сьогодні віртуалізація є стандартною практикою в ІТ-архітектурі підприємства. Це також технологія, яка керує економікою хмарних обчислень. Віртуалізація дозволяє хмарним провайдерам обслуговувати користувачів за допомогою наявного фізичного комп'ютерного обладнання; це дозволяє користувачам хмари купувати лише ті обчислювальні ресурси, які їм потрібні, коли вони їм потрібні, і економічно масштабувати ці ресурси в міру зростання робочого навантаження.

Далі будуть розглядатися популярні системи віртуалізації[4]:

1. Hyper-V: Microsoft Hyper-V — це гіпервізор, який дає змогу користувачам створювати віртуальні машини (ВМ), що працюють на базі операційних систем Windows, і керувати ними, дозволяючи віртуалізувати різноманітні програми та служби Windows, а також широкий спектр гостьових операційних систем Windows.

Для керування кількома хостами Hyper-V, віртуальними машинами та розширеними функціями Microsoft надає Hyper-V Manager і System Center Virtual Machine Manager (SCVMM) як інструменти керування для моніторингу продуктивності та розподілу ресурсів (подібно до vCenter від vSphere).

Деякі ключові функції Microsoft Hyper-V:

- Інтеграція PowerShell: пропонує широкі можливості автоматизації за допомогою командлетів PowerShell, що дозволяє адміністраторам оптимізувати завдання керування та виконувати масові операції.
- Репліка Hyper-V: забезпечує асинхронну реплікацію віртуальних машин на вторинний сайт для чудових можливостей аварійного відновлення та захисту даних.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

- Служби інтеграції: набір оптимізованих драйверів і служб, які забезпечують плавний і ефективний зв'язок і роботу Hyper-V із гостьовими операційними системами Windows.

Microsoft Hyper-V особливо добре підходить для користувачів, які активно інвестують в екосистему Microsoft. Він повністю інтегрується з іншими продуктами та інструментами Microsoft, такими як Active Directory і пакет System Center, що забезпечує цілісне управління. Hyper-V може підтримувати значну кількість віртуальних машин у кластері хостів, а його функція живої міграції та можливості централізованого керування добре масштабуються.

2. VMware vSphere: VMware vSphere — це комплексна платформа віртуалізації та хмарних обчислень, розроблена VMware. vSphere дозволяє створювати та керувати віртуальними машинами; кожна віртуальна машина являє собою самодостатній ізольований екземпляр операційної системи та програм, що працює на одному фізичному сервері.

Деякі ключові особливості vSphere:

- vMotion: дозволяє здійснювати оперативну міграцію запущених віртуальних машин між хостами, забезпечуючи нульовий час простою та активуючи балансування навантаження.
- Висока доступність vSphere (HA): автоматично перезапускає віртуальні машини на різних хостах у разі збою хосту, мінімізуючи час простою.
- Розподілений планувальник ресурсів (DRS): динамічно балансує навантаження віртуальної машини між хостами, оптимізуючи розподіл ресурсів.
- Storage vMotion: дозволяє переміщувати віртуальні диски віртуальних машин між пристроями зберігання даних без перерви в роботі.
- Відмовостійкість (FT): забезпечує постійну доступність шляхом створення дзеркальної копії віртуальної машини в реальному часі на іншому хості.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

- Розподілений комутатор: спрощує керування мережею шляхом централізації конфігурації мережі на кількох хостах.

VMware vSphere потенційно може підтримувати тисячі віртуальних машин у кластері хостів. Він використовує такі функції, як Distributed Resource Scheduler (DRS) і Distributed Power Management (DPM), щоб оптимізувати використання ресурсів і енергоефективність.

3. KVM: Kernel-based Virtual Machine — це технологія віртуалізації з відкритим кодом, яка тісно інтегрована з ядром Linux. Він надає платформу для віртуалізації робочих навантажень на основі Linux, що робить його ідеальним вибором для користувачів, які працюють із програмами та службами Linux.

Що стосується керування, KVM пропонує кілька варіантів, включаючи інструменти командного рядка та графічні інтерфейси, такі як Virt-Manager. Хоча інтерфейс керування для KVM може бути не таким багатим на функції чи зручним для користувача, як деякі з інших у цьому списку, він надає основні можливості керування, наприклад створення, запуск, зупинку та моніторинг віртуальних машин.

Деякі основні функції KVM:

- Інтеграція з Linux: KVM використовує розширення віртуалізації, наявні в сучасних процесорах. Будучи «основаним на ядрі», означає, що KVM реалізовано як модуль у ядрі Linux, базовому компоненті операційної системи Linux (який безпосередньо взаємодіє з обладнанням і керує системними ресурсами). Інтеграція KVM з ядром Linux дозволяє забезпечувати ефективну та гнучку підтримку віртуалізації безпосередньо в самому ядрі, що забезпечує чудову продуктивність віртуальних машин Linux і широкого спектру гостьових операційних систем Linux.
- Розширюваність і налаштовуваність: KVM надає широкі можливості для адаптації середовищ віртуалізації до конкретних вимог щодо оптимізації апаратного забезпечення, налаштування робочого навантаження та конфігурації для конкретних програм. Ця гнучкість робить KVM чудовим

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

для різноманітних випадків використання та забезпечує ефективний розподіл ресурсів.

- Virtio: спеціалізований інтерфейс, який підвищує ефективність операцій введення/виведення, дозволяючи гостьовій операційній системі знати про гіпервізор 2.

KVM особливо популярний серед хмарних провайдерів і розгортань, орієнтованих на Linux, завдяки своїй продуктивності та міцній інтеграції з екосистемою Linux. Він пропонує чудову підтримку для віртуалізації робочих навантажень Linux і може вмістити велику кількість віртуальних машин на одному фізичному сервері. Загалом, це надійний і ефективний вибір для тих, хто хоче віртуалізувати робочі навантаження Linux, пропонуючи надійну безпеку, а також хорошу масштабованість та інтеграцію з екосистемою Linux.

4. Proxmox VE: Proxmox VE (віртуальне середовище) — це платформа віртуалізації з відкритим вихідним кодом, яка поєднує віртуалізацію, контейнеризацію і програмно-визначене сховище в одному рішенні. Він заснований на Debian GNU/Linux і використовує гіпервізор KVM і технологію LXC (Linux Containers), щоб забезпечити надійну платформу віртуалізації, а його інтеграція з файловою системою Zettabyte (ZFS) є великою перевагою для багатьох користувачів.

Proxmox VE пропонує веб-інтерфейс керування Proxmox GUI (графічний інтерфейс користувача), який дозволяє користувачам легко створювати, налаштовувати та керувати віртуальними машинами та контейнерами. На жаль, його графічний інтерфейс не має докерів, що ускладнює розгортання програм. Однак інтерфейс надає повний набір інструментів для моніторингу та керування ресурсами, резервного копіювання та відновлення, а також впровадження високої доступності та кластеризації.

Деякі ключові особливості Proxmox VE:

- Висока доступність: Proxmox VE містить вбудовані функції високої доступності, які забезпечують постійну доступність віртуальних машин і

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

контейнерів. Він використовує спільну інфраструктуру зберігання та автоматичні механізми відновлення після збою, щоб мінімізувати час простою та підтримувати доступність сервісу.

- Кластеризація: Proxmox VE підтримує кластеризацію, що дозволяє об'єднувати декілька хостів Proxmox у кластер для централізованого керування та балансування навантаження. Кластеризація забезпечує об'єднання ресурсів, оперативну міграцію та централізоване керування сховищами, підвищуючи масштабованість і відмовостійкість.
- Резервне копіювання та відновлення: Proxmox VE пропонує комплексні можливості резервного копіювання та відновлення для віртуальних машин і контейнерів, підтримуючи як повне, так і додаткове резервне копіювання, резервне копіювання на основі знімків і можливість відновлення окремих файлів або цілих віртуальних машин.
- Програмно-визначене сховище: Proxmox VE використовує Ceph, розподілену систему зберігання, щоб забезпечити гнучкі, програмно-визначені можливості зберігання, включаючи реплікацію та кодування видалення, забезпечуючи надлишковість даних і стійкість.
- Інтеграція з ZFS: Proxmox VE інтегрується з файловою системою ZFS, пропонуючи перевірку цілісності даних, створення знімків і стиснення даних. За допомогою ZFS дані перевіряються перед тим, як вони закріплюються на диску, це чудова функція, яка покращує захист даних. Пропонуючи такі функції, як копіювання під час запису, дедуплікація даних і ефективний розподіл пам'яті, ZFS підвищує ефективність у віртуалізованих середовищах.

Загалом Proxmox VE забезпечує міцну основу для віртуалізації. Що стосується платформ віртуалізації, Proxmox VE досить швидко запускається; поєднання відкритого вихідного коду та доступу, який платформа надає до надійного набору функцій, робить її особливо популярною серед освітніх і дослідницьких установ. (Що, у свою чергу, забезпечує чудову підтримку спільноти.) Його гнучка

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

архітектура дозволяє легко інтегрувати віртуальні машини та контейнери, забезпечуючи ефективне керування ресурсами, високу доступність і деяку першокласну масштабованість.

5. Oracle VirtualBox: Oracle VirtualBox — широко розповсюджена платформа віртуалізації з відкритим вихідним кодом, яка дозволяє користувачам запускати кілька операційних систем одночасно на одній фізичній машині. Гіпервізор забезпечує гнучке рішення для віртуалізації робочого столу, пропонуючи сумісність з різними операційними системами хоста, включаючи Windows, macOS, Linux і Oracle Solaris.

Oracle VirtualBox був призначений для індивідуального використання, тому, порівняно з іншими згаданими платформами, його інтерфейс керування має менше розширених функцій, необхідних для багатокористувацького середовища. Ви можете використовувати його для конфігурації параметрів віртуального обладнання, керування сховищем і мережевими конфігураціями, але, що стосується платформ віртуалізації, він не найскладніший. Якщо вам потрібне тимчасове середовище для тестування або запуску віддалених програм, VirtualBox може функціонувати як короткострокове рішення, але ми не рекомендуємо використовувати його довгостроково для більш масштабного організаційного використання.

Деякі ключові особливості VirtualBox:

- Запуск кількох операційних систем: за допомогою VirtualBox ви можете запускати декілька операційних систем одночасно на одному комп'ютері. Це корисно для таких завдань, як розробка програмного забезпечення, тестування різних налаштувань і використання старішого програмного забезпечення. Однак під час використання деяких інших операційних систем поза попередньо встановленим списком параметрів ви можете зіткнутися з проблемами сумісності.
- Підтримка USB-пристроїв: VirtualBox дозволяє використовувати USB-пристрої, підключені до вашого фізичного обладнання, під час роботи з

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

віртуальними машинами; це означає, що ви можете легко підключатися до пристроїв USB, таких як зовнішні накопичувачі, принтери та інші периферійні пристрої, працюючи в новому віртуальному середовищі.

- Мережеві можливості: Oracle VirtualBox пропонує низку мережевих опцій, включаючи трансляцію мережевих адрес (NAT), мостову мережу та внутрішню мережу. Користувачі можуть налаштувати свої мережеві конфігурації в VirtualBox, дозволяючи віртуальним машинам взаємодіяти з мережею та іншими пристроями за потреби.

Oracle VirtualBox віддають перевагу окремим особам, розробникам і невеликим середовищам завдяки своїй природі з відкритим вихідним кодом і сумісності між платформами. Це економічно ефективний варіант віртуалізації, який чудово підходить для тестування конфігурацій програмного забезпечення, запуску віртуалізованих середовищ або вивчення нових операційних систем.

1.4. Аналіз функціонування протоколів VPN

Протокол VPN (Virtual Private Network) використовується для забезпечення безпечного та приватного з'єднання між вузлами мережі через незахищену публічну мережу, таку як Інтернет. Він дозволяє створювати віртуальні приватні мережі, які забезпечують конфіденційність, цілісність та доступність передачі даних між вузлами мережі.

Принцип роботи та функціонування протоколу VPN може бути розподілений на наступні етапи:

- Аутентифікація та авторизація: Клієнт, який бажає підключитися до VPN, надає свої ідентифікаційні дані для аутентифікації. Сервер VPN перевіряє ці ідентифікаційні дані та приймає рішення про надання або відхилення доступу клієнта до VPN.
- Шифрування даних: Після успішної аутентифікації, клієнт та сервер VPN укладають угоду про спільний шифрувальний ключ. Цей ключ

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

використовується для шифрування даних, які передаються між клієнтом та сервером, забезпечуючи конфіденційність.

- Упаковка даних в тунелі: Для передачі даних між клієнтом та сервером VPN створюється віртуальний тунель. Дані, що передаються між клієнтом та сервером, упаковуються в пакети та шифруються, а потім розпаковуються та розшифровуються на другому кінці тунелю.
- Маршрутизація трафіку: Сервер VPN приймає упаковані дані від клієнта та розпаковує їх. Він маршрутизує розпаковані дані до відповідного місця призначення в мережі, забезпечуючи доставку даних.
- Забезпечення цілісності даних: Протокол VPN може включати механізми перевірки цілісності даних, такі як хеш-функції або контрольні суми. Ці механізми дозволяють перевіряти, чи були дані під час передачі змінені.

Існує кілька типів VPN:

- Віддалений доступ (Remote Access VPN): Це найпоширеніший тип VPN, який дозволяє користувачам з'єднуватися з корпоративною мережею з віддалених місць або домашніх офісів. Віддалений доступ VPN забезпечує безпечне тунельне з'єднання між пристроєм користувача та VPN-сервером у мережі підприємства.
- Сайт-до-сайту (Site-to-Site VPN): Цей тип VPN використовується для з'єднання двох або більше мереж на рівні мережі. Він дозволяє побудувати безпечне з'єднання між офісами, філіями або дата-центрами різних локацій.
- VPN-тунель (VPN Tunneling): Цей тип VPN використовується для з'єднання мережі або пристрою з VPN-сервером. Він створює захищений тунель для передачі даних через незахищену мережу, таку як Інтернет.
- SSL VPN: Це тип VPN, який використовує SSL або TLS протоколи для забезпечення безпеки. SSL VPN забезпечує захищений доступ до веб-додатків, файлів та інших ресурсів через стандартні веб-браузери без необхідності встановлювати додаткове програмне забезпечення.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Тепер розглянемо, які існують VPN протоколи[5]:

1. IPsec: Безпека Інтернет-протоколу (IPsec) — це набір безпечних мережових протоколів, який автентифікує та шифрує пакети даних, щоб забезпечити безпечний зашифрований зв'язок між двома комп'ютерами через мережу Інтернет-протоколу. Він використовується у віртуальних приватних мережах (VPN)[6].

IPsec включає протоколи для встановлення взаємної автентифікації між агентами на початку сеансу та узгодження криптографічних ключів для використання під час сеансу. IPsec може захищати потоки даних між парою хостів (хост-хост), між парою шлюзів безпеки (мережа-мережа) або між шлюзом безпеки та хостом (мережа-хост). IPsec використовує служби криптографічної безпеки для захисту зв'язку через мережі Інтернет-протоколу (IP). Він підтримує автентифікацію на рівні мережі, автентифікацію походження даних, цілісність даних, конфіденційність даних (шифрування) і захист від відтворення (захист від атак відтворення).

Початковий набір IPv4 був розроблений з незначною кількістю заходів безпеки. Як частина вдосконалення IPv4, IPsec є моделлю OSI рівня 3 або схемою наскрізної безпеки рівня Інтернету. У той час як деякі інші системи Інтернет-безпеки, які широко використовуються, працюють над мережовим рівнем, наприклад Transport Layer Security (TLS), яка працює над транспортним рівнем, і Secure Shell (SSH), яка працює на прикладному рівні, IPsec може автоматично захищати програми на рівні Інтернету.

IPsec пропонує два різні режими, які забезпечують різні рівні захисту для мережевого зв'язку:

- Режим тунелю: у цьому режимі всі дані, включаючи заголовок і корисне навантаження, шифруються, і додається новий заголовок. Він ідеально підходить для безпечної передачі даних через публічні мережі, оскільки забезпечує посилений захист від несанкціонованого доступу.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

- Транспортний режим: він шифрує лише корисне навантаження, а IP-заголовок залишається незмінним. Незашифрований заголовок дозволяє маршрутизаторам ідентифікувати адресу призначення кожного пакета, що робить його придатним для використання в надійній закритій мережі.

2. L2TP: Протокол тунелювання другого рівня (L2TP) — це протокол тунелювання на основі RFC, який є промисловим стандартом і вперше підтримувався в операційних системах клієнта та сервера Windows 2000. На відміну від PPTP, L2TP на серверах під керуванням Windows Server 2003 не використовує Microsoft Point-to-Point Encryption (MPPE) для шифрування датаграм протоколу Point-to-Point (PPP). L2TP покладається на безпеку Інтернет-протоколу (IPSec) для служб шифрування. Комбінація L2TP і IPSec відома як L2TP/IPSec. L2TP/IPSec надає послуги первинної віртуальної приватної мережі (VPN) для інкапсуляції та шифрування приватних даних[7-8].

Інкапсуляція для пакетів L2TP/IPSec складається з двох рівнів:

- Інкапсуляція L2TP: Кадр PPP (дейтаграма IP або дейтаграма IPX) обгортається заголовком L2TP і заголовком UDP.
- Інкапсуляція IPSec: Отримане повідомлення L2TP потім обгортається заголовком і трейлером IPSec Encapsulating Security Payload (ESP), трейлером автентифікації IPSec, який забезпечує цілісність повідомлення та автентифікацію, і остаточним IP-заголовком. У заголовку IP міститься IP-адреса джерела та призначення, яка відповідає VPN-клієнту та VPN-серверу.

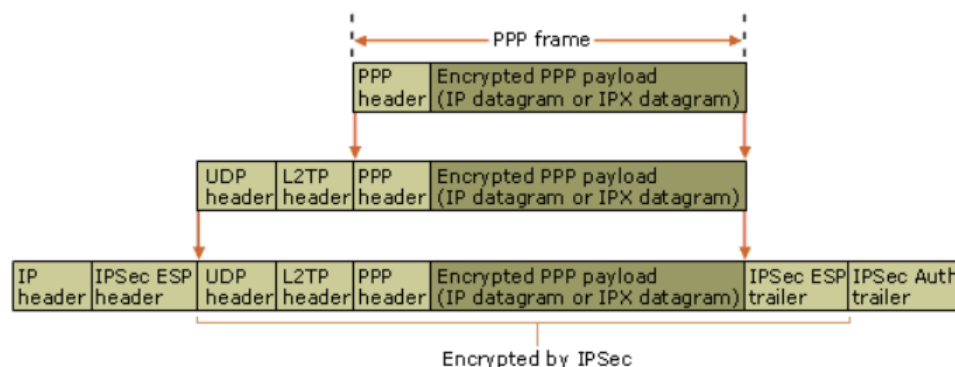


Рис. 1.4 – Інкапсуляція даних L2TP з IPSec

Повідомлення L2TP шифрується стандартом шифрування даних (DES) або потрійним DES (3DES) за допомогою ключів шифрування, створених у процесі узгодження обміну ключами в Інтернеті (IKE).

3. PPTP: Протокол тунелювання «точка-точка» (PPTP) — це мережевий протокол, який забезпечує безпечну передачу даних від віддаленого клієнта на сервер приватного підприємства шляхом створення віртуальної приватної мережі (VPN) у мережах передачі даних на основі TCP/IP. PPTP підтримує багатопроTOCOLьну віртуальну приватну мережу на вимогу через публічні мережі, такі як Інтернет[9].

Мережева технологія PPTP є розширенням протоколу віддаленого доступу Point-to-Point, визначеного в документі Інженерної робочої групи Інтернету (IETF) під назвою «Протокол точка-точка для передачі багатопроTOCOLьних дейтаграм через точку». -to-Point Links", відомий як RFC 1171. PPTP — це мережевий протокол, який інкапсулює пакети PPP в IP-дейтаграми для передачі через Інтернет або інші публічні мережі на основі TCP/IP. PPTP також можна використовувати в приватних мережах LAN-to-LAN.

Протокол PPTP входить до складу операційних систем Windows NT Server версії 4.0 і Windows NT Workstation версії 4.0. Комп'ютери, які працюють під керуванням цих операційних систем, можуть використовувати протокол PPTP для безпечного підключення до приватної мережі як клієнт віддаленого доступу за допомогою загальнодоступної мережі даних, як-от Інтернет. Іншими словами, протокол PPTP дозволяє створювати на вимогу віртуальні приватні мережі через Інтернет або інші загальнодоступні мережі передачі даних на основі TCP/IP. PPTP також може використовуватися комп'ютерами, підключеними до локальної мережі, для створення віртуальної приватної мережі в локальній мережі.

Важливою особливістю використання протоколу PPTP є його підтримка віртуальних приватних мереж за допомогою комутованих телефонних мереж загального користування (PSTN). PPTP спрощує та знижує витрати на розгортання рішення для віддаленого доступу на рівні підприємства для віддалених або

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

мобільних користувачів, оскільки забезпечує безпечний і зашифрований зв'язок через загальнодоступні телефонні лінії та Інтернет. PPTP усуває потребу в дорогих, виділених лініях або серверах зв'язку приватних підприємств, оскільки ви можете використовувати PPTP через лінії PSTN.

PPTP є старішим протоколом, ніж SSTP, і його легше налаштувати. PPTP також підтримується ширше, ніж SSTP. Однак PPTP може бути легко заблокований інтернет-провайдерами або адміністраторами. Оскільки SSTP використовує порт 443, його складніше заблокувати. PPTP має відомі вразливості безпеки та вважається менш безпечним порівняно з SSTP та іншими сучасними протоколами VPN.

4. SSTP: Secure Socket Tunneling Protocol — це протокол VPN, який створює тунель між клієнтським пристроєм і сервером. В першу чергу SSTP використовується для захисту віддаленого доступу до приватних мереж через Інтернет. Microsoft розробила SSTP, щоб замінити менш безпечні протоколи PPTP і L2TP/IPSec. SSTP зазвичай використовується для захисту внутрішніх VPN-з'єднань Windows.

SSTP встановлює зашифрований тунель між клієнтом VPN і сервером VPN. Дані, які проходять через тунель, захищені від зовнішнього перехоплення

SSTP є вдосконаленим протоколом PPTP (протокол тунелювання точка-точка), оскільки за замовчуванням він використовує SSL/TLS і TCP-порт 443. Ці функції дозволяють вважати SSTP кращим з точки зору безпеки та можливостей проходження брандмауера порівняно з PPTP.

SSTP також базує свої з'єднання на автентифікації користувача замість автентифікації пристрою чи комп'ютера.

SSTP вважається криптографічно безпечним протоколом. Він використовує шифри SSL/TLS і AES для встановлення безпечного з'єднання між клієнтом і сервером. SSTP забезпечує безпеку мережевого трафіку, охоплюючи його захисним каналом SSL/TLS.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

SSTP призначений лише для віддаленого клієнтського доступу, зазвичай він не підтримує VPN-тунелі типу «site-to-site». SSTP має ті ж обмеження продуктивності, що й будь-який інший тунель IP-over-TCP. Загалом продуктивність буде прийнятною лише до тих пір, поки є достатня надлишкова пропускна здатність на нетунельованому мережевому каналі, щоб гарантувати, що тунельовані таймери TCP не закінчатся. Якщо це стає неправдою, продуктивність різко падає.

5. IKEv2: Internet Key Exchange version 2 (IKEv2) — це протоколи vpn, які зазвичай поєднуються з IPSec і широко відомі як IKEv2/IPSec.

Протокол VPN широко реалізований у мобільних пристроях. Це можна пояснити високою швидкістю, стабільністю та високою надійністю під час перемикання між мережами.

IKEv2 — це протокол тунелювання в пакеті протоколів IPSec. Він відповідає за налаштування асоціації безпеки (SA) для безпечного зв'язку між клієнтами VPN і серверами VPN у межах IPSec. IKEv2 є наступником IKEv1 із покращеннями та оптимізацією, такими як висока швидкість, підвищена безпека та підвищена ефективність.

IKEV2 значною мірою покладається на IPSec для захисту зв'язку між клієнтом VPN і сервером VPN. IKEV2 встановлює асоціацію безпеки (SA), яка узгоджує ключі безпеки, які використовуються клієнтом VPN і сервером VPN. Після перевірки IKEv2 асоціації безпеки встановлюється безпечний тунель, який пропонує зашифрований зв'язок між двома вузлами. IKEv2/IPSec використовує більш надійне 256-бітне шифрування. Він може використовувати шифри шифрування VPN, такі як AES, ChaCha20 і Camellia.

IKEv2 підтримує всі основні платформи, включаючи Windows, macOS, Android, iOS, Linux і маршрутизатори. Це особливо швидко в macOS, що робить IKEv2 VPN чудовим вибором, якщо ви шукаєте Mac VPN. Протокол також сумісний із такими інтелектуальними пристроями, як Smart TV і деякими потоковими пристроями.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

6. OpenVPN: OpenVPN — це протокол VPN із відкритим кодом, який широко використовується окремими особами та організаціями для створення безпечних і зашифрованих з'єднань через Інтернет. Вперше він був випущений у 2001 році і з тих пір став одним із найпопулярніших протоколів VPN[10].

OpenVPN використовує шифрування SSL/TLS для захисту даних, що передаються через з'єднання VPN, і підтримує низку методів автентифікації, таких як цифрові сертифікати, попередньо надані ключі та комбінації імені користувача та пароля. Його розроблено з широкими можливостями налаштування, що робить його популярним вибором для провайдерів і адміністраторів VPN.

Протоколи SSL і TLS забезпечують безпеку зв'язку в Інтернеті та дозволяють програмам клієнт/сервер спілкуватися конфіденційно та надійно. Протоколи мають два рівні: протокол запису та протокол рукописання, і вони розташовані над транспортним протоколом, таким як TCP/IP. Вони обидва використовують асиметричні та симетричні методи криптографії.

Однією з ключових переваг OpenVPN є його гнучкість. Його можна використовувати в багатьох операційних системах, включаючи Windows, macOS, Linux, Android та iOS. Крім того, він підтримує різноманітні мережеві топології, такі як клієнт-сервер, сайт-сайт і багатоклієнт.

OpenVPN можна використовувати в режимі TCP або UDP, залежно від конкретних вимог VPN-з'єднання. TCP зазвичай використовується для з'єднань, які вимагають надійної та впорядкованої доставки пакетів, тоді як UDP використовується для з'єднань, які вимагають вищої пропускної здатності та меншої затримки.

Загалом, OpenVPN — це потужний і гнучкий протокол VPN, який пропонує високий рівень безпеки та можливості налаштування. Хоча для встановлення та конфігурації може знадобитися більше технічних знань порівняно з іншими протоколами VPN, його гнучкість і можливість налаштування роблять його популярним вибором для багатьох користувачів і провайдерів VPN.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

7. MPLS VPN: Протокол MPLS VPN (Multiprotocol Label Switching Virtual Private Network) є розширенням протоколу MPLS, яке дозволяє створювати захищені корпоративні мережі з використанням віртуальних приватних мереж (VPN). MPLS VPN забезпечує віртуальне розділення мережевого трафіку між різними клієнтами, забезпечуючи конфіденційність, цілісність та доступність даних.

Принцип роботи та функціонування протоколу MPLS VPN можна розподілити на наступні етапи:

- Розділення VPN: Мережа оператора, яка використовує MPLS, фізично розділяється на окремі віртуальні мережі (VPN). Кожна VPN володіє своїм власним вирізаним простором IP-адрес, топологією та політиками безпеки.
- Міткування пакетів: Кожен пакет, що надходить до мережі MPLS VPN, мітиться двома мітками: міткою VPN та міткою маршрутизації (label). Мітка VPN визначає до якої віртуальної мережі належить пакет. Мітка маршрутизації використовується для визначення шляху проходження пакета в мережі.
- Тунелювання даних: Пакети з мітками VPN та маршрутизації тунелюються через MPLS мережу від одного вузла до іншого. Вузли мережі, відомі як PE (Provider Edge), відповідають за вхід та вихід пакетів від VPN.
- Роутинг та пересилання пакетів: PE вузли використовують таблиці маршрутизації, щоб визначити, до якого іншого PE вузла переслати пакет. За допомогою міток маршрутизації, PE вузли визначають шляхи для кожного пакета в рамках мережі MPLS VPN.
- Безпека та ізоляція: MPLS VPN забезпечує конфіденційність даних між різними VPN шляхом використання віртуального розділення мережевого трафіку. Кожна VPN має свої політики безпеки, що встановлюються на PE вузлах та забезпечують контроль доступу до даних.
- QoS (Quality of Service): MPLS VPN підтримує механізми QoS, що дозволяють приділяти пріоритети різним типам трафіку. Це важливо для

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

забезпечення якості обслуговування для додатків, які вимагають низької затримки, високої пропускної спроможності або гарантованої якості передачі даних.

Протокол MPLS VPN дозволяє підприємствам побудувати безпечні та гнучкі корпоративні мережі, де дані клієнтів знаходяться в окремих віртуальних приватних мережах. Цей підхід дозволяє ефективно управляти трафіком, забезпечувати безпеку даних та забезпечувати високу якість обслуговування для корпоративних потреб.

1.5. Постановка технічного завдання

В сучасному інформаційному суспільстві, де велика кількість підприємств та організацій переходять до цифрового середовища, корпоративні мережі відіграють невід'ємну роль у забезпеченні ефективності та надійності обміну інформацією. Одним із ключових аспектів розробки та функціонування корпоративних мереж є правильне проєктування серверної частини, яка відповідає вимогам сучасного бізнесу, відповідно до цього в роботі визначаються наступні задачі:

1. Проєктування корпоративної мережі, та розгортання і налаштування серверу.

Для виконання цієї задачі потрібно визначити топологію та IP-адресацію корпоративної мережі, описати яке віртуальне середовище буде використовуватись, потім його розгортання і налаштування на сервері. Після цього розписати необхідно виконати розгортання і налаштування віртуальних машин, де буде описано визначити необхідні операційні системи, які будуть використовуватись, та їх ролі у корпоративної мережі. Також необхідно визначити вимоги до налаштування VPN-сервісу.

2. Розгортання і налаштування віртуального середовища.

Відповідно до цього завдання потрібно висвітлити процес встановлення віртуального середовища на сервері. Провести його налаштування, створити віртуальні машини і виділити їм ресурси сервера в залежності від ролей, визначених для цих компонентів.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

3. Розгортання і налаштування віртуальних машин.

В цьому завданні потрібно відобразити процес встановлення ОП на віртуальні машини, налаштування ір-адресації, та показати встановлення і налаштування служб та ролей, наприклад службу Active Directory для зручного контролю над робочими станціями, які підключені до домену в корпоративній мережі.

Висновок до першого розділу:

Протягом виконання даного розділу було дослідженню принцип роботи сервера і в чому заключається його ціль. Його основна ціль заключається в обміні інформації між ним і клієнтом. Існує декілька моделей серверу, наприклад сервер-клієнт або peer-to-peer, де нема централізованої бази даних і клієнти виступаю в якості серверів. Був проведений аналіз існуючих операційних систем для серверів, де були розглянуті різні дистрибутиви linux для серверів, windows server, та інші відносно популярні ОС. Було коротко описано самі ОС і для чого вони підходять. Був проведений аналіз існуючих систем віртуалізацій, так яку роль вони відіграють в роботі серверів. Вони дозволяють більш ефективно використовувати фізичне обладнання комп'ютера. Зазначено всі популярні системи віртуалізації та описано їхні особливості. Був проведений аналіз існуючих протоколів VPN, так як вони відіграють велику роль в безпеці мережі на сьогоднішній момент. Зазначено популярні VPN-протоколи і особливості їх роботи.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

РОЗДІЛ 2. ПРОЄКТУВАННЯ СЕРВЕРА ТА МЕРЕЖІ

2.1. Проєктування логічної та фізичної топології мережі

2.1.1. Фізична топологія

Топологія мережі - це спосіб, у який пристрої, такі як комп'ютери, принтери, маршрутизатори та комутатори, з'єднані та взаємодіють один з одним у мережі. Вибір правильної мережевої топології для вашого малого бізнесу може вплинути на продуктивність, надійність, безпеку та масштабованість вашої мережі. Нижче будуть перелічені мережеві топології та їх переваги та недоліки.

1. Шинна топологія: Шинна топологія - це найпростіша і найдешевша топологія мережі, де всі пристрої під'єднані до одного кабелю, який називається шиною або магістраллю. Цю топологію легко встановлювати і розширювати, оскільки вам потрібно лише додавати або видаляти пристрої з кабелю. Однак вона має деякі недоліки, такі як обмежена швидкість і пропускна здатність через довжину і якість кабелю. Крім того, мережа вразлива до збоїв і перешкод, що ускладнює усунення несправностей та управління нею. Крім того, вона не є безпечною, оскільки будь-який пристрій може отримати доступ до даних, що передаються по кабелю.

2. Топологія “зірка”: Топологія “зірка” - найпоширеніша і найпопулярніша мережева топологія, в якій всі пристрої підключаються до центрального пристрою, наприклад, концентратора, комутатора або маршрутизатора. Ця топологія є більш надійною та безпечною, ніж шинна, з вищою швидкістю та пропускною здатністю мережі, що залежить від потужності центрального пристрою. Крім того, вона стійка до збоїв і перешкод, проста в усуненні несправностей і управлінні, а також безпечна завдяки шифруванню і аутентифікації, що застосовуються з центрального пристрою. Однак топологія «зірка» також має певні недоліки: вона дорожча і складніша через додаткові кабелі та потужний центральний пристрій, а її продуктивність і доступність залежать від центрального пристрою.

3. Кільцева топологія: Кільцева топологія - це топологія мережі, в якій всі пристрої з'єднані по колу, причому кожен пристрій має пряме з'єднання з двома

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

іншими пристроями. Ця топологія є більш ефективною і стабільною, ніж шинна, оскільки швидкість і пропускна здатність мережі залишаються незмінними незалежно від кількості пристроїв, а в кабелі не виникають колізії або конфлікти. Крім того, її легко діагностувати і керувати, оскільки для регулювання передачі даних можна використовувати методи передачі маркерів або опитування. Однак кільцева топологія також має деякі обмеження, такі як вища вартість і складність мережі через потребу в більшій кількості кабелів і роз'ємів, вразливість до збоїв і перешкод, оскільки будь-який розрив або пошкодження одного з'єднання впливає на все кільце, а також відсутність безпеки, оскільки будь-який пристрій може отримати доступ до даних, що передаються по кільцю.

4. Комірчаста топологія: Комірчаста топологія - це топологія мережі, в якій всі пристрої повністю або частково з'єднані один з одним. Ця топологія є найбільш надійною і гнучкою мережевою топологією, оскільки вона забезпечує оптимальну швидкість і пропускну здатність, а також стійкість до збоїв і перешкод. Крім того, її легко усувати несправності та керувати за допомогою протоколів і алгоритмів маршрутизації, а також забезпечити безпеку за допомогою шифрування та автентифікації. Однак у цієї топології є й недоліки, такі як висока вартість і складність через необхідність використання великої кількості кабелів, роз'ємів і пристроїв, а також складне обслуговування та адміністрування, що вимагає координації та оновлення інформації про маршрутизацію між усіма пристроями.

Компанія буде мати окрему будівлю з відділами. В одному відділі будуть працювати звичайні працівники компанії, а на другому будуть працювати бухгалтери та менеджери проєктів. Перший відділ буде розрахований на 10 чоловік, а другий на 5. Також буде віділено окрему кімнату для серверів. Тому для такої невеличкої компанії підійде топологія “зірка”. Буде задіяно два сервери: основний та баскуп, на випадок виходу з ладу основного. В кожних відділеннях з працівниками буде встановлений як мінімум 1 комутатор. У випадку збільшення кількості працівників у відділенні, будуть встановлені додаткові комутатори. Усі

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

пристрої будуть мати можливість вийти в інтернет через маршрутизатор, до якого підключені всі комутатори.

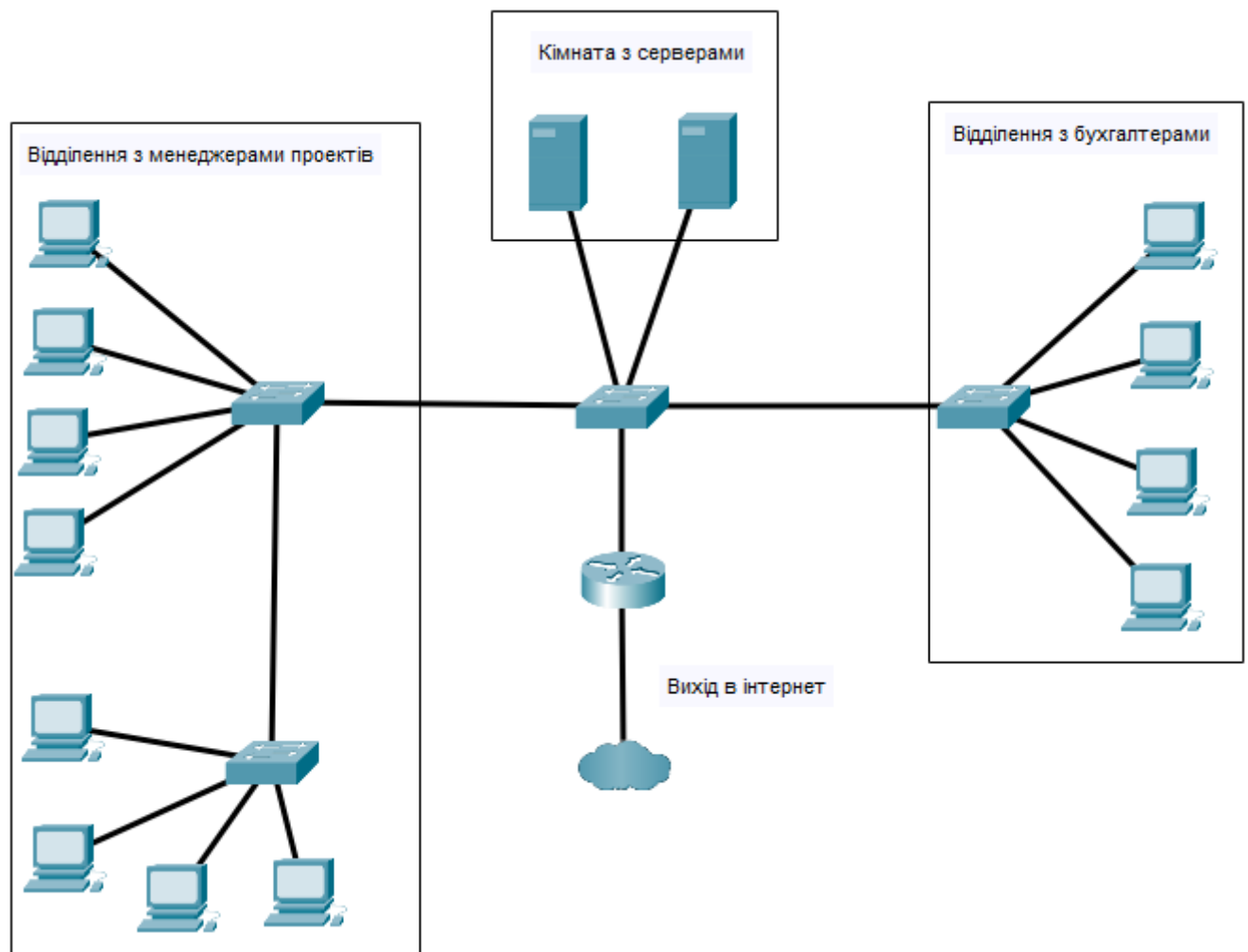


Рис. 2.1 – Схема мережі

2.1.2. Логічна топологія

Для передавання інформації між пристроями та мережами потрібно розробити схему адресації мережі. Мережа має бути розрахована як мінімум на 10 чоловік з можливістю розширення до 100 працівників. Тому будемо використовувати маску мережі 255.255.255.0, а ір мережі буде 192.168.1.0. Нижче буде показано адресація мережі у таблиці 2.1

Таблиця 2.1 – Адресація мережі

Призначення	ІР-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Широкомовна адреса	192.168.1.255
Шлюз по замовчуванню	192.168.1.1
Діапазон адрес комутаторів	192.168.1.121-192.168.1.140
Діапазон адрес ПК	192.168.1.1-192.168.1.100
Діапазон адрес серверів	192.168.1.101-192.168.1.120
Діапазон вільних адрес	192.168.1.141-192.168.1.253

2.2. Розгортання серверу

На сервері буде розгорнуто віртуальне середовище для економії коштів і гнучкості. Віртуальні машини є більш ефективними так як вони використовують менше ресурсів та їх можна швидко масштабувати вгору або вниз, щоб відповідати мінливим потребам у обчислювальних потужностях. Кожна віртуальна машина працює у власному віртуальному середовищі, що може допомогти ізолювати програми та дані одна від одної. Віртуальні машини займають менше фізичного простору, ніж фізичні сервери, що може бути важливо для компаній з обмеженим простором. Вибір віртуального середовища впав на Proxmox. Для невеликої компанії до 100 працівників Proxmox VE є чудовим вибором з наступних причин:

- Безкоштовність: Це дозволяє економити кошти на програмному забезпеченні віртуалізації.
- Простота використання: Це полегшує адміністраторам керувати віртуальними машинами, навіть якщо вони не мають багато досвіду.
- Гнучкість: Це дозволяє використовувати різні операційні системи для віртуальних машин, що може бути корисно для компаній з різними потребами.

- Масштабованість: Це дозволяє компанії рости, не турбуючись про те, що їй доведеться оновлювати програмне забезпечення віртуалізації.
- Безпека: Це допомагає захистити віртуальні машини від загроз безпеки.

Тому, на першому сервері буде встановлено віртуальне середовище Proxmox VE. У ньому будуть знаходитись і працювати всі віртуальні машини. На другому сервері буде встановлено Proxmox Backup Server для того щоб він резервно копіював та відновлював віртуальні машини, контейнерів та фізичних хостів у випадку неполадок. Завдяки підтримці інкрементного, повністю дедуплікованого резервного копіювання, Proxmox BS значно знижує навантаження на мережу і економить цінний простір для зберігання даних. Завдяки надійному шифруванню і методам забезпечення цілісності даних, ви можете почувати себе в безпеці при резервному копіюванні даних, навіть на об'єкти, яким не можна повністю довіряти.

Для першого серверу потрібно підібрати обладнання. Було підібрано подібне обладнання:

- Процесор: Intel Xeon E3-1230 v5 (3.4 GHz)
- Пам'ять: 8 GB DDR4
- Накопичувач: 2000 GB HDD

Для другого серверу:

- Процесор: Intel Xeon E3-1230 v5 (3.4 GHz)
- Пам'ять: 2 GB DDR4
- Накопичувач: 100 GB HDD

2.3. Налаштування серверу

В цьому пункті будуть описані основні налаштування на серверах. На першому сервері будуть дві віртуальні машини на яких буду встановлена операційна система Windows Server 2019. Він був вибраний із-за того, що він має зручний графічний інтерфейс (GUI) та інструменти PowerShell, які полегшують адміністрування сервера, та має доступні численні навчальні матеріали та ресурси для допомоги адміністраторам у роботі з нею.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Перша віртуальна машина буде головним сервером, а друга термінальним сервером. Використання одного головного та термінального сервера на віртуальному середовищі може значно покращити адміністрування копоративної мережі.

Головний сервер потрібний для зберігання і контролю користувачів, даних важлив для компанії. На ньому будуть налаштований Active directory, який автентифікує та авторизує всіх користувачів і комп'ютери в мережі доменного типу Windows, призначає і застосовує політики безпеки для всіх комп'ютерів, а також встановлює або оновлює програмне забезпечення. Наприклад, коли користувач входить до комп'ютера, який є частиною домену Windows, Active Directory перевіряє введені ім'я користувача та пароль і визначає чи є користувач системним адміністратором, чи ні. Крім того, вона дозволяє керувати та зберігати інформацію, забезпечує механізми автентифікації та авторизації, а також створює основу для розгортання інших супутніх служб: Служб сертифікації, служб федерації Active Directory, полегшених служб каталогів і служб керування правами. Також в ньому можна буде налаштувати dhcp і інші сервіси, які можуть бути необхідними в процесі налаштування головного серверу.

Термінальний сервер забезпечує віддалений доступ до графічного інтерфейсу додатків та операційної системи. На ньому також буде налаштований Active Directory, щоб потім під'єднатися до головного серверу. За допомогою термінального сервера користувачі можуть працювати з додатками та даними на сервері так, ніби вони знаходяться на локальному комп'ютері. При цьому всі дані та програми зберігаються на сервері, що робить роботу з ними більш ефективною та безпечною. Технічно термінальний сервер працює на операційній системі Windows Server і використовує протоколи Remote Desktop Protocol (RDP) або Independent Computing Architecture (ICA) для надання віддаленого доступу користувачам. Він також може використовувати різні механізми автентифікації та авторизації, щоб забезпечити безпечний доступ до даних та додатків. Термінальний сервер може бути налаштований для різних цілей, наприклад, для забезпечення

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

віддаленого доступу до програм, спільної роботи над документами, віртуалізації робочих станцій та багатьох інших завдань. Він також може бути інтегрований з іншими системами керування та безпеки, такими як Active Directory, щоб забезпечити централізоване керування користувачами та доступ до ресурсів.

2.4. Налаштування VPN-сервісу

Щоб адміністратор домену зміг підключитися до серверів через інтернет мережу, потрібно створити між ними VPN з'єднання, а для цього підійде OpenVPN. Як було зазначено в теоретичній частині, він повністю безплатний та дозволяє детально налаштовувати його серверну і клієнтську частину.

Почнемо з налаштування серверної частини OpenVPN. Він буде розташований на головному сервері. Після встановлення OpenVPN, потрібно згенерувати сертифікат CA (Certificate Authority), параметри DH (Diffie Hellman), а потім сертифікат і приватний ключ для серверу[11]. Також наперед можна створити сертифікат і приватний ключ для клієнту, но для кожного клієнта потрібно створювати свій. В папці з програмою є зразок налаштування конфігураційного файлу для серверу і клієнта з детальним описом кожної команди. В ній, через команди, потрібно зазначити щоб сервер використовував певний порт і протокол, наприклад tcp або udp, потім треба зазначити шлях до створених ключів і сертифікатів для серверу. Потім зазначити, щоб він створював маршрутизований IP-тунель, через команду “dev tun”. Обов'язково потрібно налаштувати мережу VPN через команду “server”, в ній прописуємо ip мережі і маску мережі, наприклад 10.8.0.0 та 255.255.255.0. Щоб клієнт міг підключитися до іншого серверу в приватній мережі, який стоїть за межею VPN-серверу, потрібно вписати команду “push”, тоді клієнт зможе мати зв'язок не тільки з VPN-сервером, а й з іншими машинами в корпоративній мережі. Після налаштування конфіг файлу, потрібно зберегти його в папку config-auto. Це всі налаштування, які потрібно для працювання VPN-серверу.

Для того щоб клієнт зміг з'єднатися з VPN-сервером потрібно згенерувати для нього сертифікат і ключ клієнта. Після цього їх та CA сертифікат, який був

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

створений до цього на сервері, потрібно відправити до клієнта в папку config. По зразку в папки, створюємо конфігураційний файл для клієнта. Позначаємо що він є клієнтом командою “client”. Як і на конфігураційному файлі сервера потрібно буде вписати команду “dev tun” та зазначити щоб клієнт використовував tcp протокол. Через команду “remote” вказуємо статичну адресу серверу і порт для підключення. Ще для безпеки стоїть додати команду “remote-cert-rlc” і назву серверу, яку вибирали при генерації сертифікатів і ключів, щоб перевірялись сертифікат сервера, переконавшись, що сертифікат має правильний набір ключів. Після цього зберегти конфігураційний файл в папці “config”.

Після налаштувань на обох кінцях серверу і клієнта, потрібно перезавантажити сервіси OpenVPN щоб налаштування були задіяними. На цьому етапі можна підключатись до VPN-серверу і пробувати підключатись через RDC до робочого стола головного і термінального серверу.

Висновок до другого розділу:

Протягом виконання даного розділу було розглянуто проектування логічної і фізичної топології мережі. Розглянуто основні види фізичних і логічних топологій, де було вибрано оптимальний варіант для корпоративної мережі. Спроектовано розгортання серверу, де зазначено яка там буде віртуальне середовище і віртуальні машини в ньому, також було обрано оптимальні характеристики серверу для його роботи. Показано які будуть основні налаштування серверу, тобто його віртуальних машин, де кожна відіграє свою роль в корпоративній мережі. Був обраний оптимальний VPN-сервіс і розписано дії при його налаштуванні, щоб клієнт ззовні корпоративної мережі міг підключитися до серверу.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

РОЗДІЛ 3. РОЗГОРТАННЯ СЕРВЕРУ І МЕРЕЖІ

3.1. Розгортання і налаштування прохмох на сервері

Так як не було доступного сервера, було вирішено створити його у VirtualBox і встановити туди Proxmox для наглядності.



Рис. 3.1 – Встановлення Proxmox

При встановленні Proxmox, нам пропунують це зробити через зручний графічний інтерфейс або звичайний термінал. Я вибрав зручний інтерфейс.

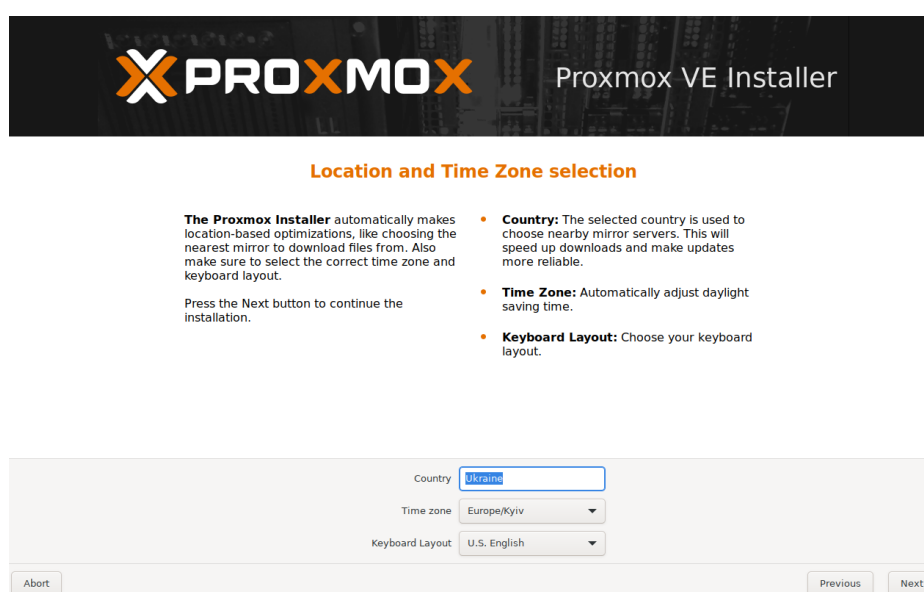


Рис. 3.2 – Встановлення Proxmox

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

Налаштовуємо часовий пояс і мову введення. В моєму випадку, як показано в рис.3.2., було встановлено автоматично часовий пояс український і мову введення англійський.

PROXMOX Proxmox VE Installer

Administration Password and Email Address

Proxmox Virtual Environment is a full featured, highly secure GNU/Linux system, based on Debian.

In this step, please provide the **root** password.

- Password:** Please use a strong password. It should be at least 8 characters long, and contain a combination of letters, numbers, and symbols.
- Email:** Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events, etc.).

Press the Next button to continue the installation.

Password:
 Confirm:
 Email:

Abort Previous Next

Рис. 3.3 – Встановлення Proxmox

Вводимо пароль, за допомогою якого нам дозволять керувати прохтох, та пошту, на яку будуть приходити важливі повідомлення.

PROXMOX Proxmox VE Installer

Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installing.

IP address (CIDR): Set the main IP address and netmask for your server in CIDR notation.

After you have finished the configuration, you will be shown a summary screen where you can choose during the installation.

Management Interface:
 Hostname (FQDN):
 IP Address (CIDR): /
 Gateway:
 DNS Server:

Abort Previous Next

Рис. 3.4 – Встановлення Proxmox

Тут потрібно ввести ір-адресу, маску мережі та шлюз по замовчуванням. При встановленні, вона може сама отримати ір-адресу за допомогою dhcp. Також тут можна ще ввести хостнейм та ір-адресу.



Рис. 3.5 – Встановлення Proxmox

У рис.3.5. можна побачити перелік налаштувань, які будуть виконані при встановленні Proxmox.

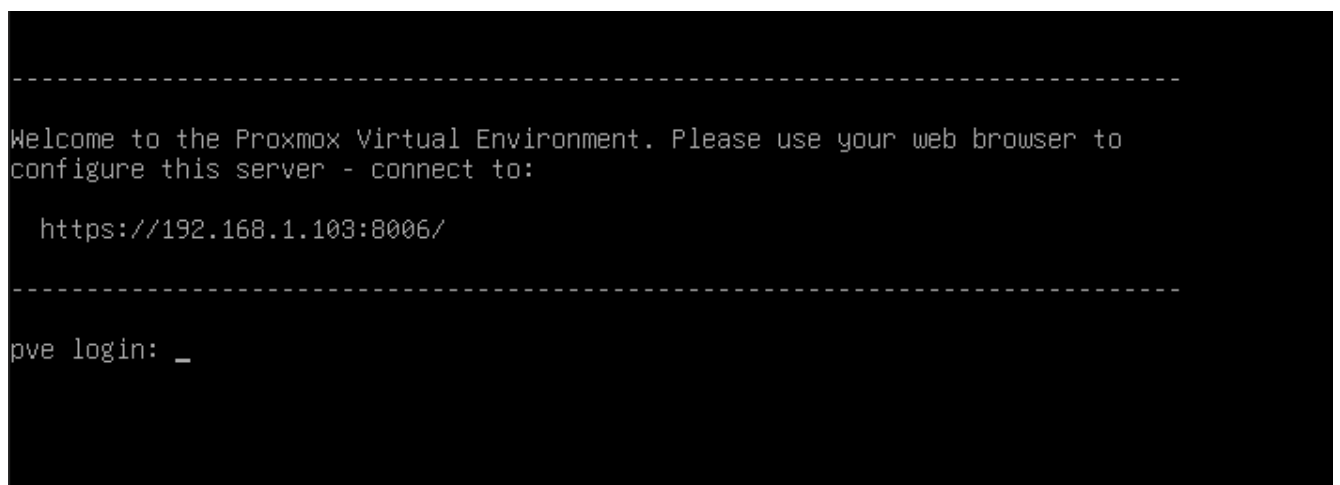


Рис. 3.6 – Успішне встановлення і запуск Proxmox

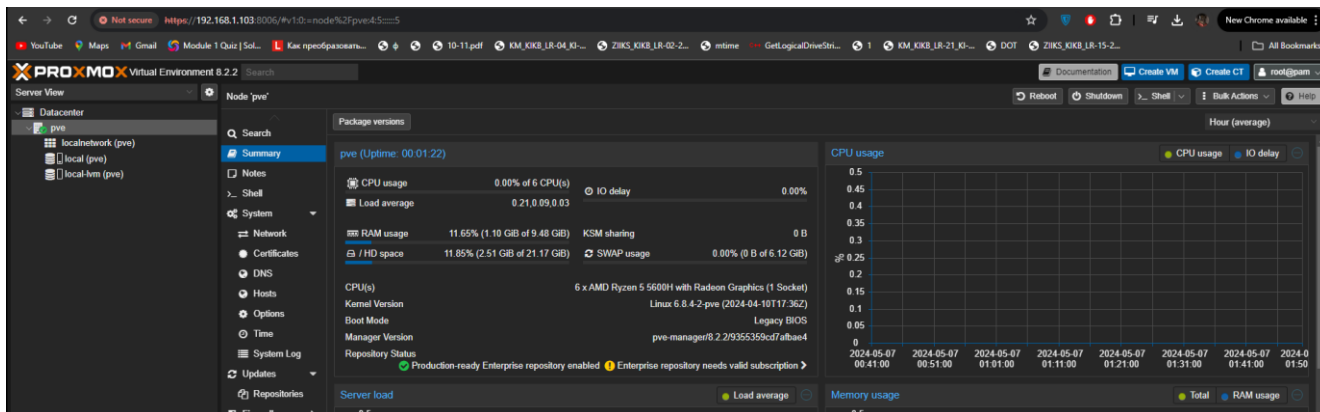


Рис. 3.7 – Перехід до графічного інтерфейсу Proxmox

Після встановлення прохтох на віртуальну машину та запуску його, на екрані повинно показати ір-адресу і порту. Їх можна ввести в браузері і тим самим отримати доступ до графічного інтерфейсу Proxmox. Звісно при цьому треба ввести логін і пароль.

3.2. Розгортання і налаштування backup серверу proxmox

Для того, щоб у випадку поломки віртуальної машини можна було її відновити, потрібно на другий сервер встановити Proxmox Backup Server. Він записує снапшоти віртуальних машин. Можна зробити записувати їх на backup сервер вручну або автоматично по розкладу. Встановлення Proxmox BS ідентичний до Proxmox VE.

Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installing.

After you have finished, press the Next button. You will be shown a list of the options that you chose during the previous steps.

- IP address (CIDR):** Set the main IP address and netmask for your server in CIDR notation.
- Gateway:** IP address of your gateway or firewall.
- DNS Server:** IP address of your DNS server.

Management Interface: enp0s3 - 08:00:27:8b:c4:87 (e1000)

Hostname (FQDN): pbs.server.backup

IP Address (CIDR): 192.168.1.102 / 24

Gateway: 192.168.1.1

DNS Server: 192.168.1.104

Рис. 3.9 – Встановлення Proxmox

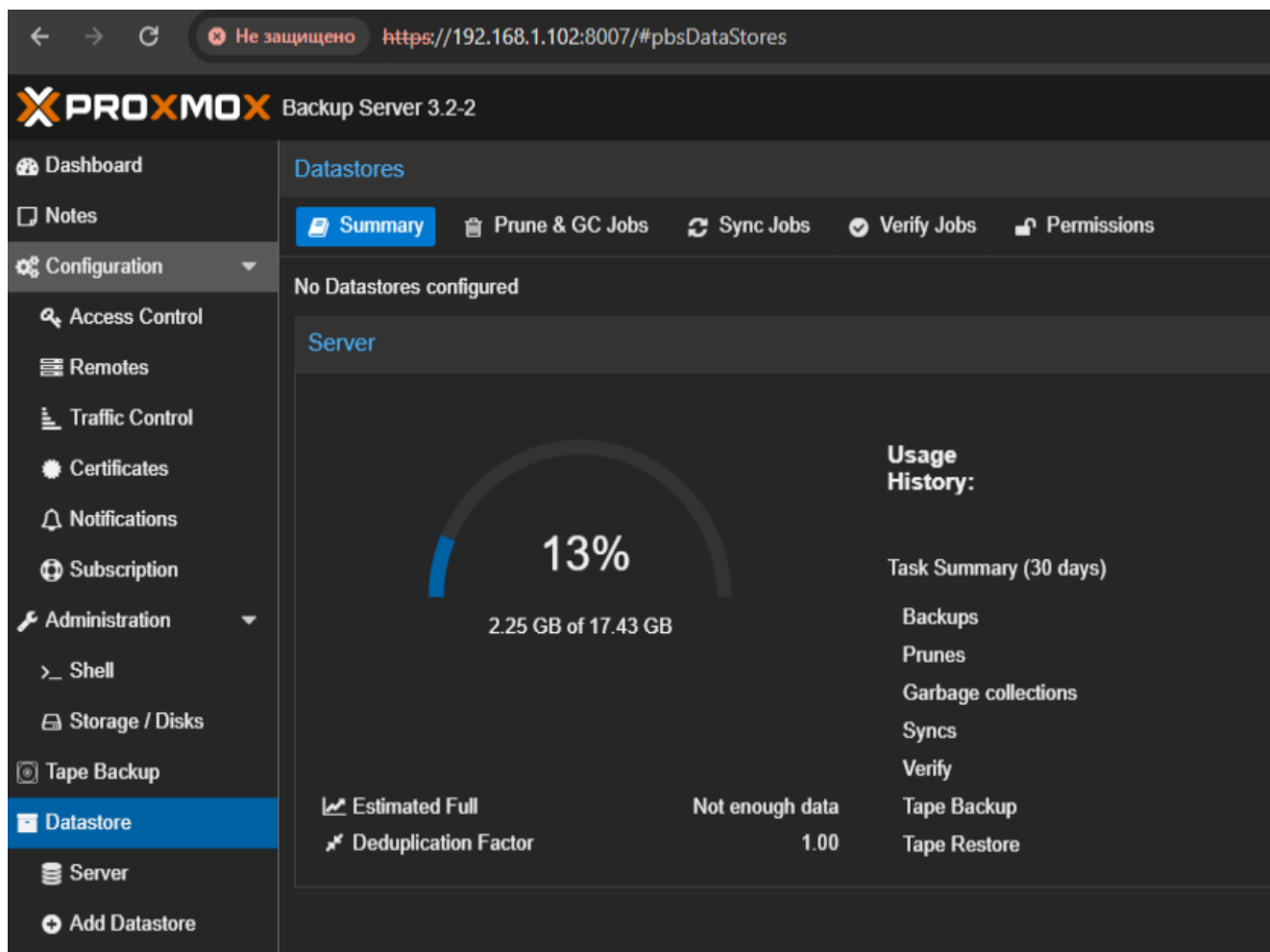


Рис. 3.10 – Графічний інтерфейс Прохмох BS

Add: Proxmox Backup Server

General
Backup Retention
Encryption

ID:BackupVM

Nodes:All (No restrictions)

Server:192.168.1.102

Enable:☒

Username:root@pam

Content:backup

Password:.....

Datastore:Server

Namespace:Root

Fingerprint:50c:f1:8e:18:21:09:32:6f:47:d1:ad:f6:c8:e8:14:73:b2:97:ba:3e:83:ed:d1:aa:0f:e3

Help

Add

Рис. 3.10 – Додавання Прохмох BS до Прохмох VE



Рис. 3.11 – Додавання Proxmox BS до Proxmox VE

Backup VM 102

Storage:

BackupVM

Mode:

Snapshot

Protected:

☐

Compression:

ZSTD (fast and good)

Notification mode:

Auto

Send email to:

none

Notes:

{{guestname}}

Possible template variables are:

{{cluster}}, {{guestname}}, {{node}}, {{vmid}}

Help

Backup

Рис. 3.12 – Спроба зберегти снапшот віртуальної машини на Proxmox VE

Virtual Machine 102 (TerminalServer) on node 'pve'		No Tags	
Summary	Backup now	Restore	File Restore
Console	Show Configuration	Edit Notes	Change Protection
Hardware	Remove	Storage	
Cloud-Init	Name		Notes
Options	vm/102/2024-06-10T13:55:25Z		TerminalServer
Task History			
Monitor			
Backup			

Рис. 3.13 – Список снапшотів віртуальної машини на Proxmox VE

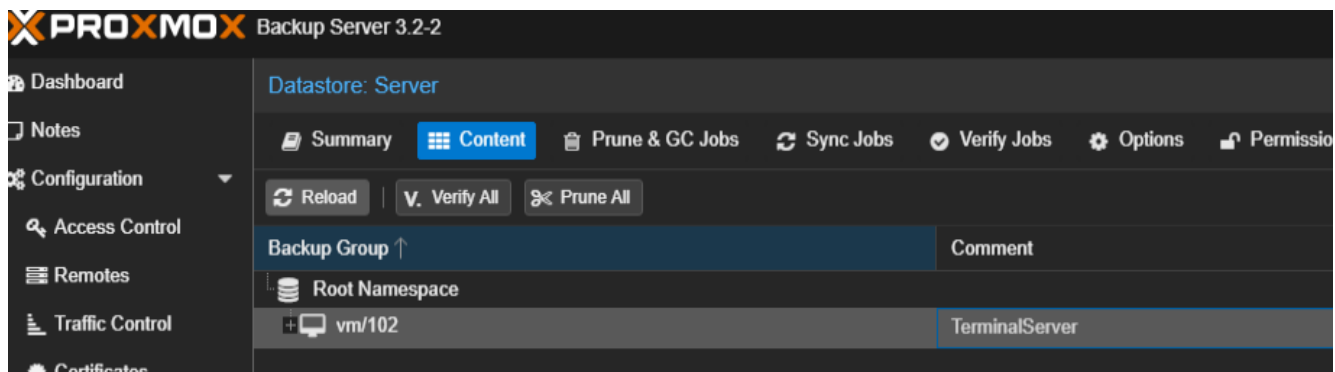


Рис. 3.14 – Список снапшотів віртуальної машини на Proxmox BS

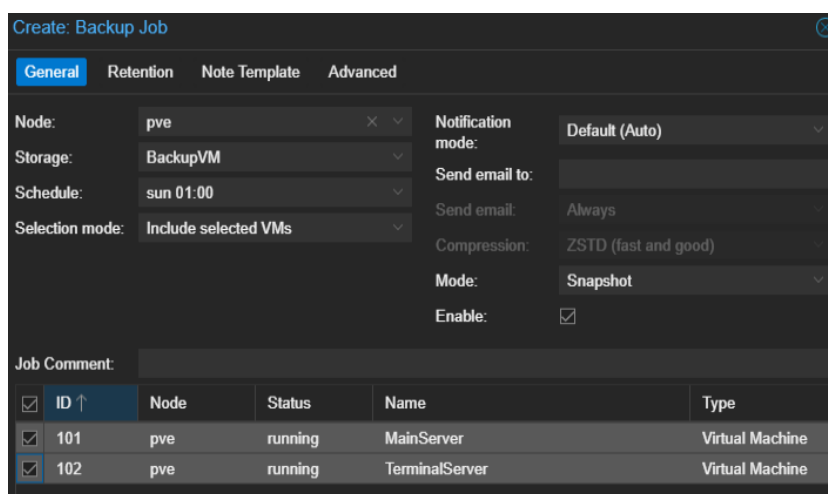


Рис. 3.14 – Налаштування збереження снапшотів по розкладу на Proxmox VE

3.3. Створення і налаштування головного серверу

Тепер нам потрібно створити головний сервер на Proxmox. Все починається з того, що потрібно задати iso-файл образу операційної системи та потрібні характеристики для серверу.

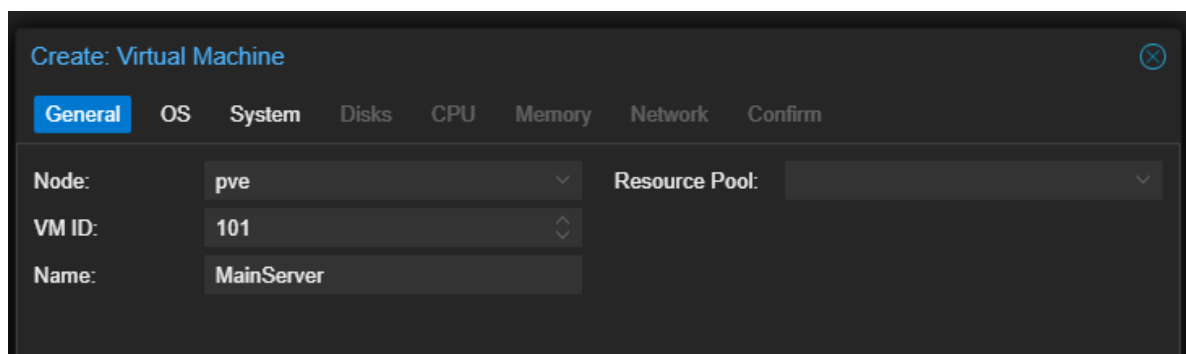


Рис. 3.15 – Створення головного серверу

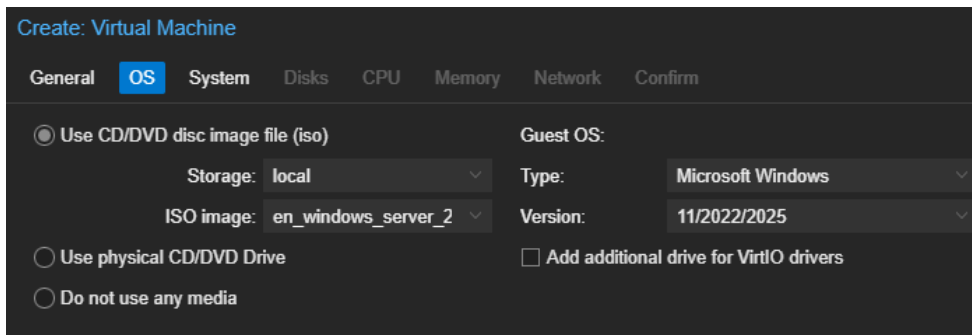


Рис. 3.16 – Створення головного серверу

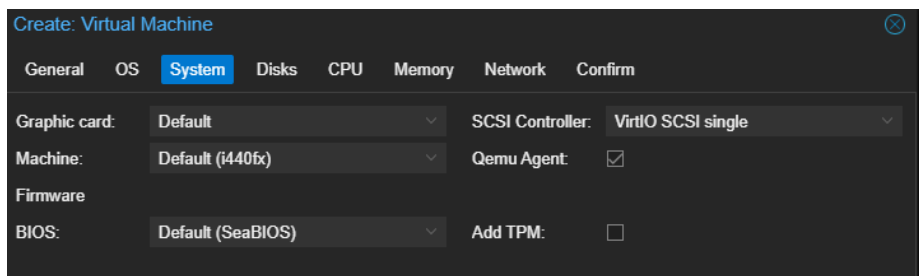


Рис. 3.17 – Створення головного серверу

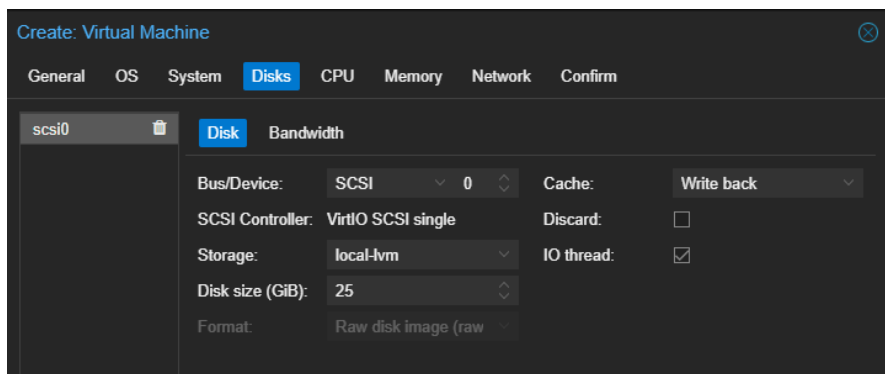


Рис. 3.18 – Створення головного серверу

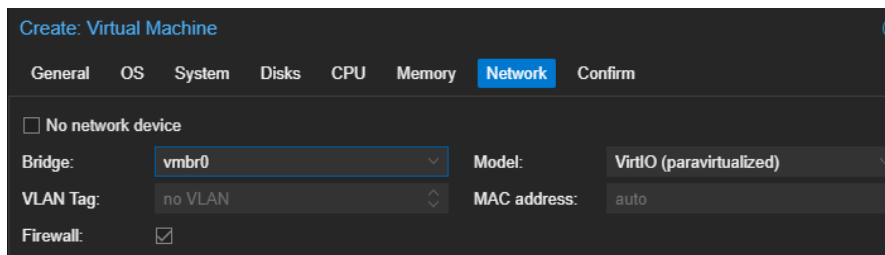


Рис. 3.19 – Створення головного серверу

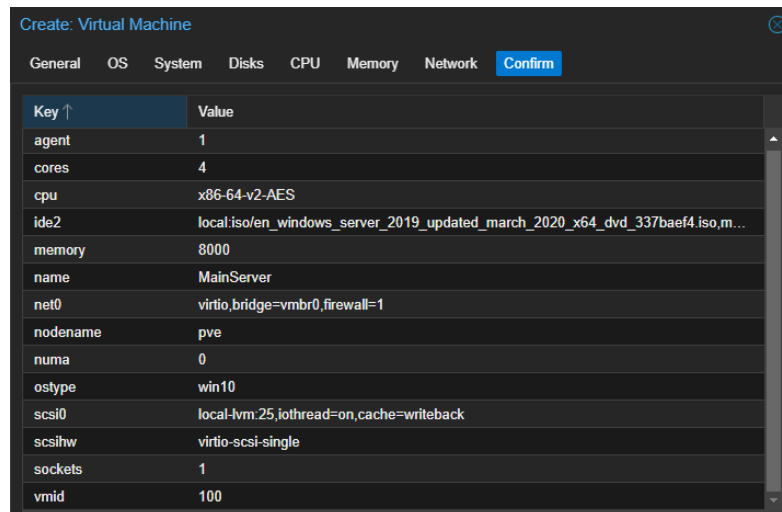


Рис. 3.21 – Створення головного серверу

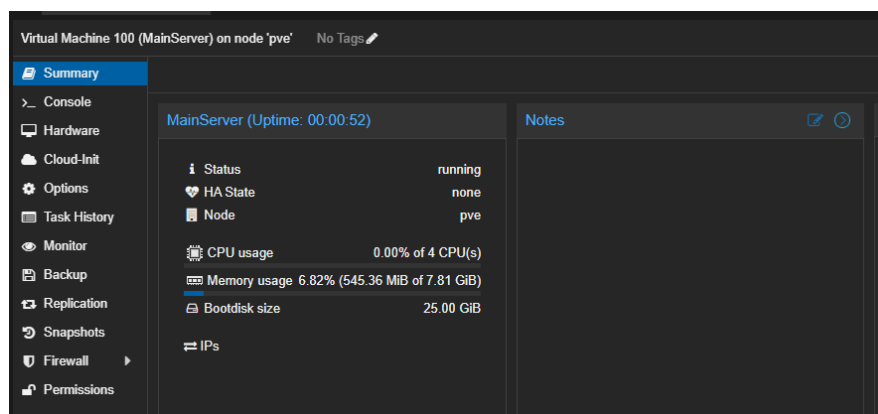


Рис. 3.22 – Моніторинг над віртуальною машиною в Proxmox

Далі буде показано встановлення операційної системи Microsoft Server.

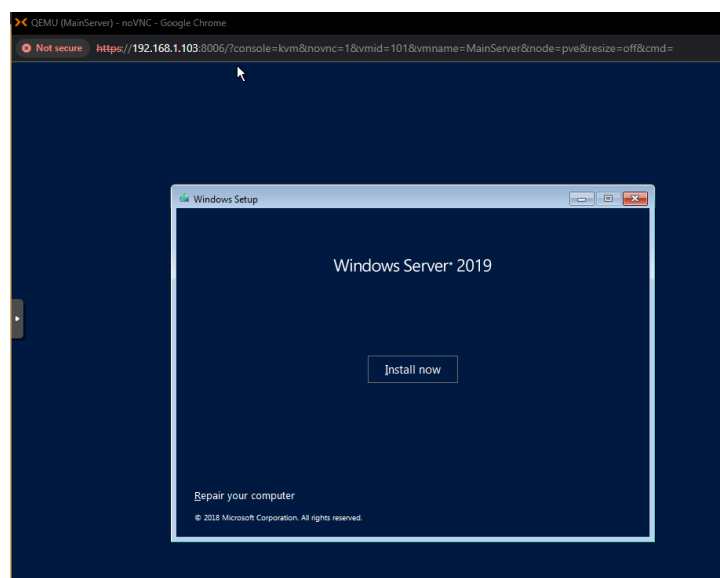


Рис. 3.23 – Встановлення операційної системи для головного серверу

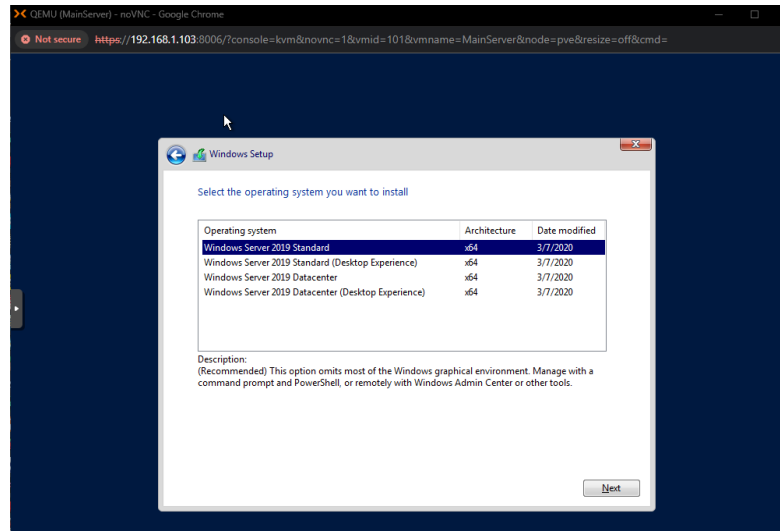


Рис. 3.24 – Встановлення операційної системи для головного серверу

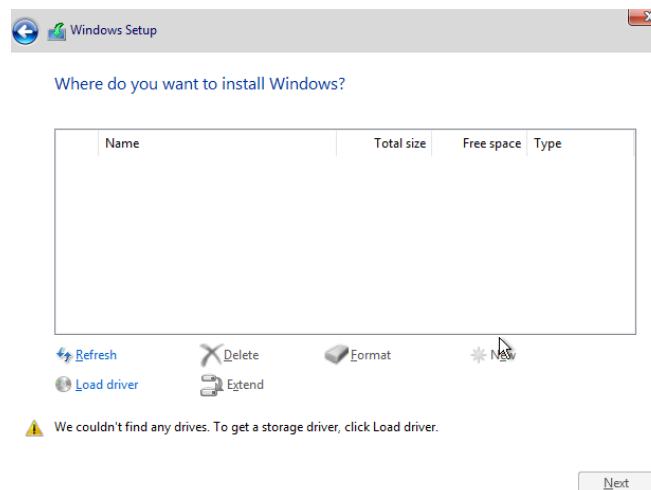


Рис. 3.25 – Встановлення операційної системи для головного серверу

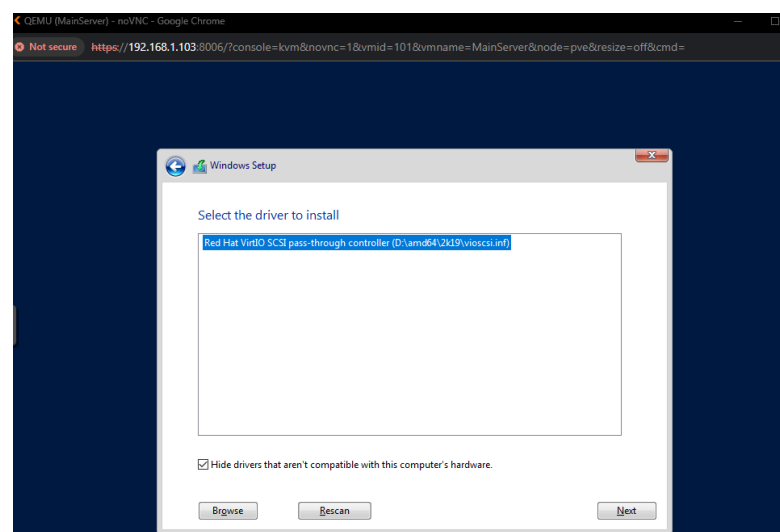


Рис. 3.26 – Встановлення операційної системи для головного серверу

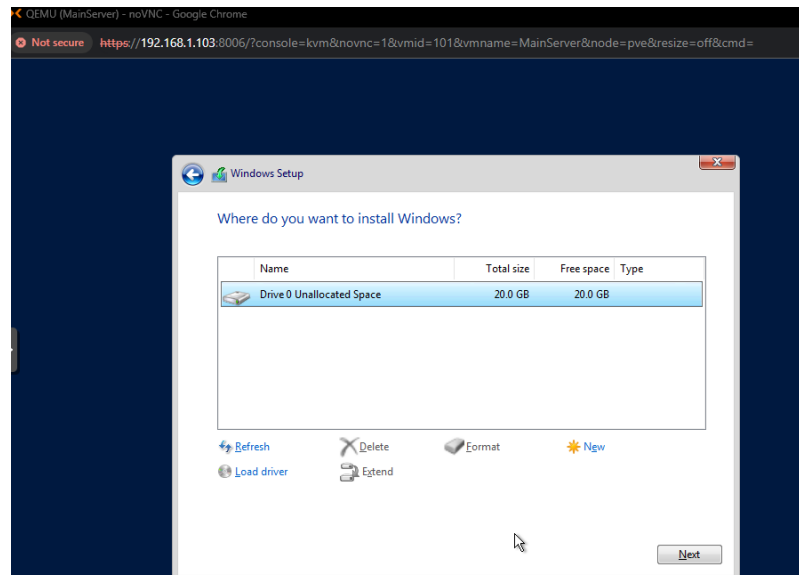


Рис. 3.27 – Встановлення операційної системи для головного серверу

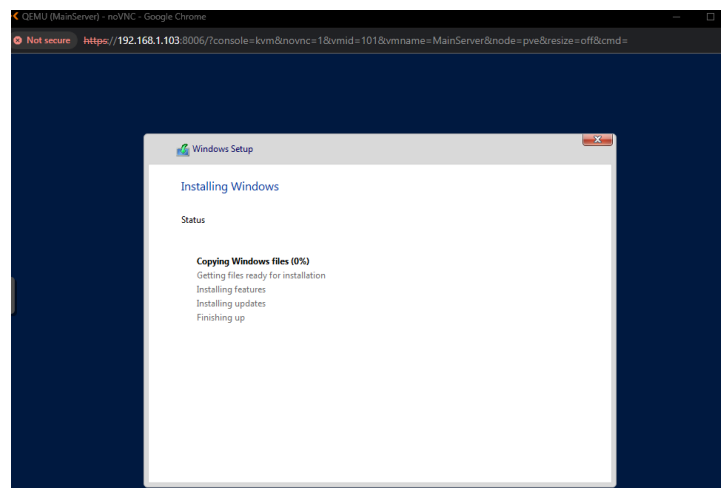


Рис. 3.28 – Встановлення операційної системи для головного серверу

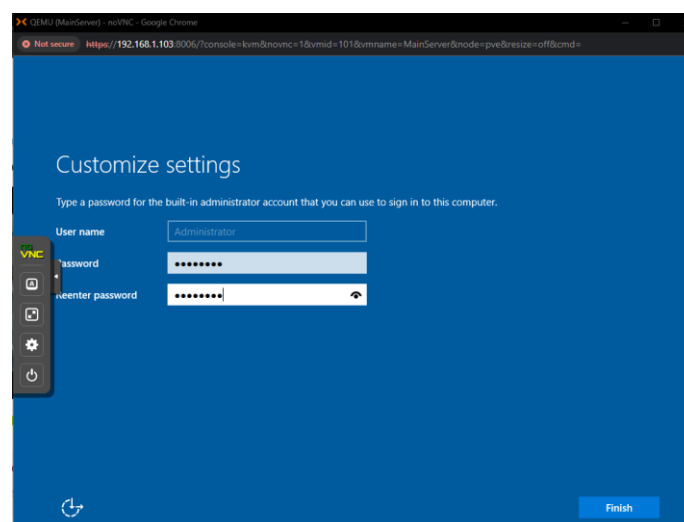


Рис. 3.29 – Налаштування паролю для головного серверу

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

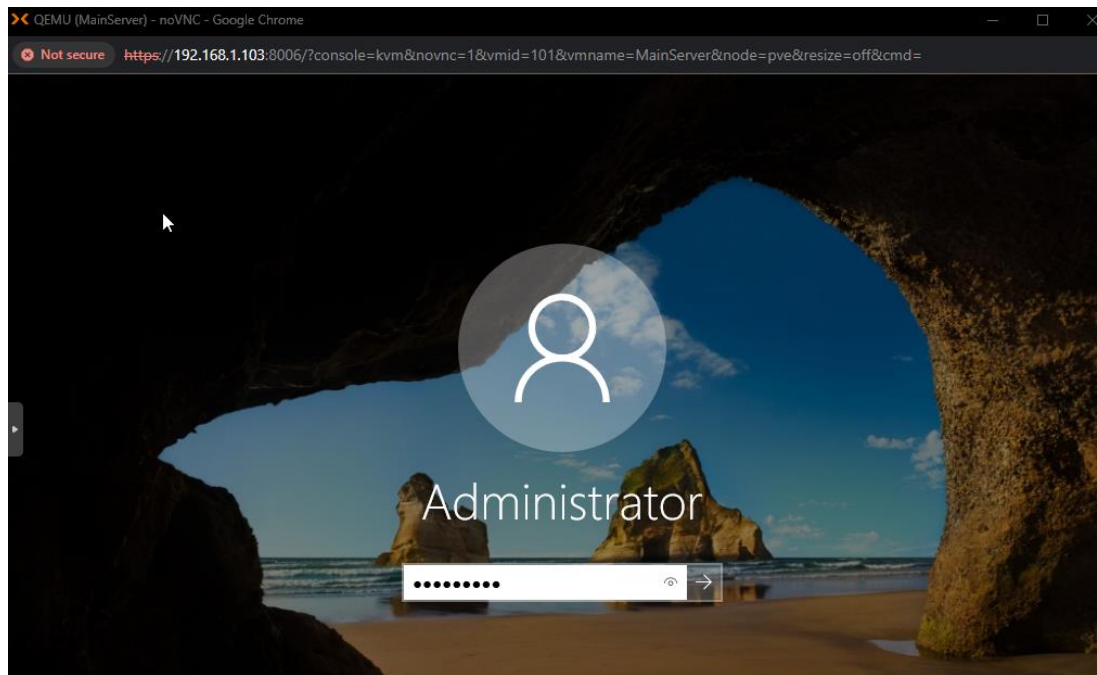


Рис. 3.30 – Успішне встановлення операційної системи на головний сервер

Після встановлення операційної системи на головний сервер, потрібно в ньому ір-адресацію та Active Directory, після чого створює домен для компанії.

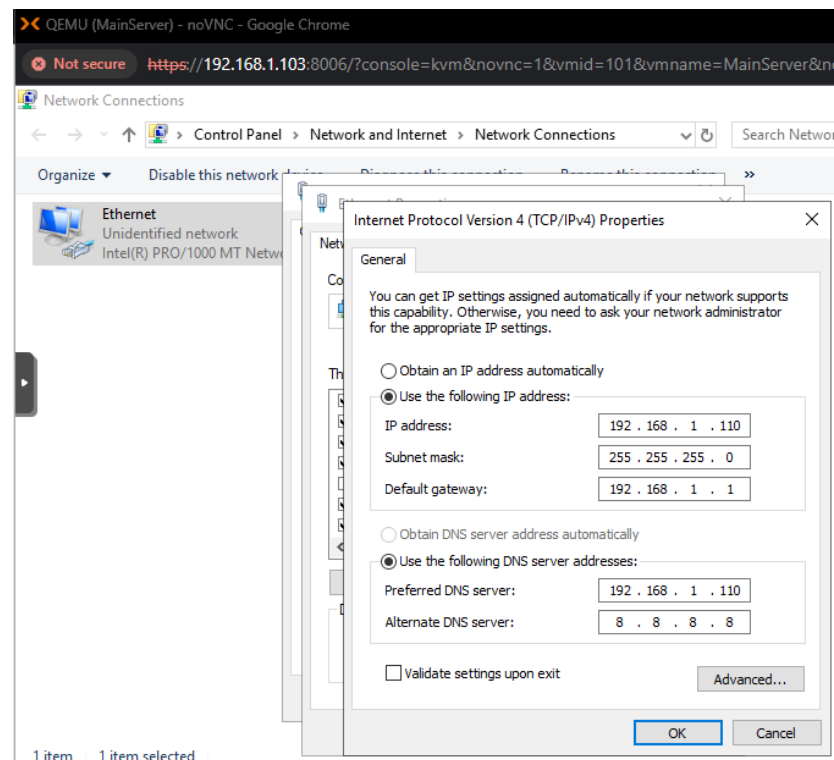


Рис. 3.31 – Налаштувати ір-адресації

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

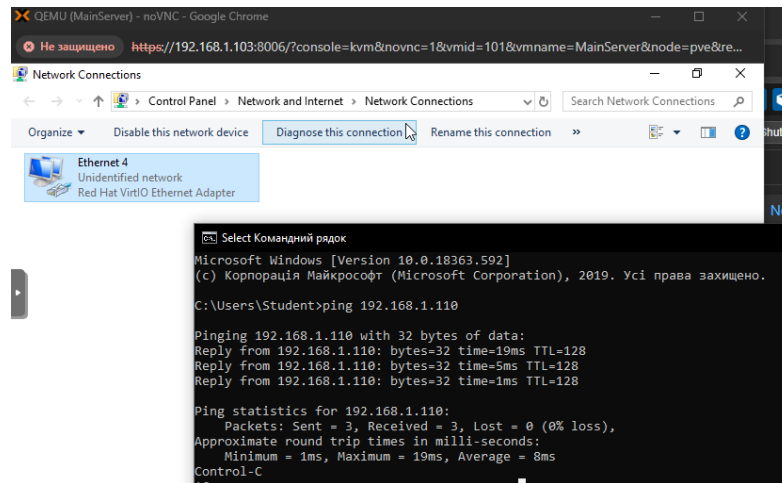


Рис. 3.32 – Перевірка зв'язку між головним сервером та комп'ютером підключеного до мережі

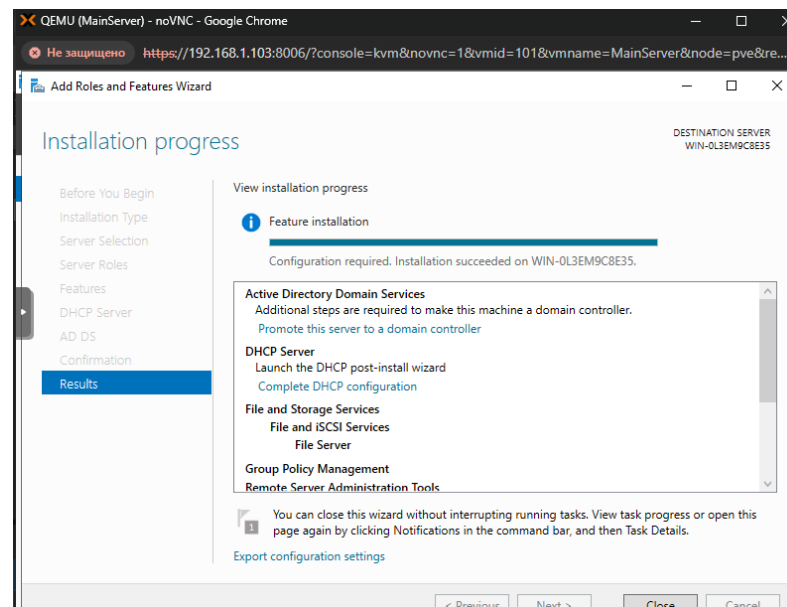


Рис. 3.33 – Налаштування Active Directory на головному сервері

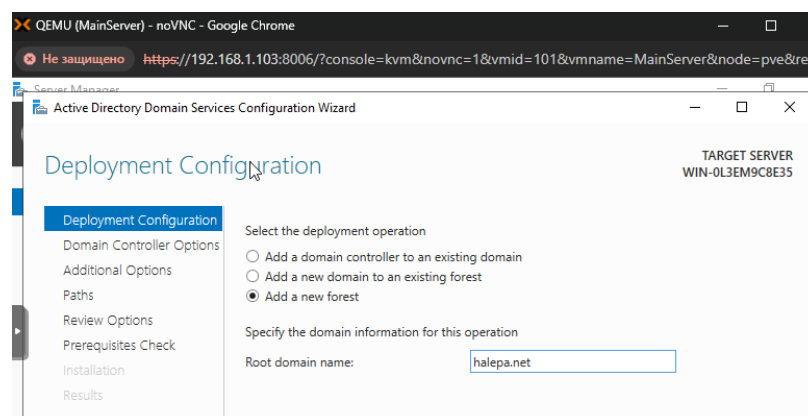


Рис. 3.34 – Налаштування Active Directory на головному сервері

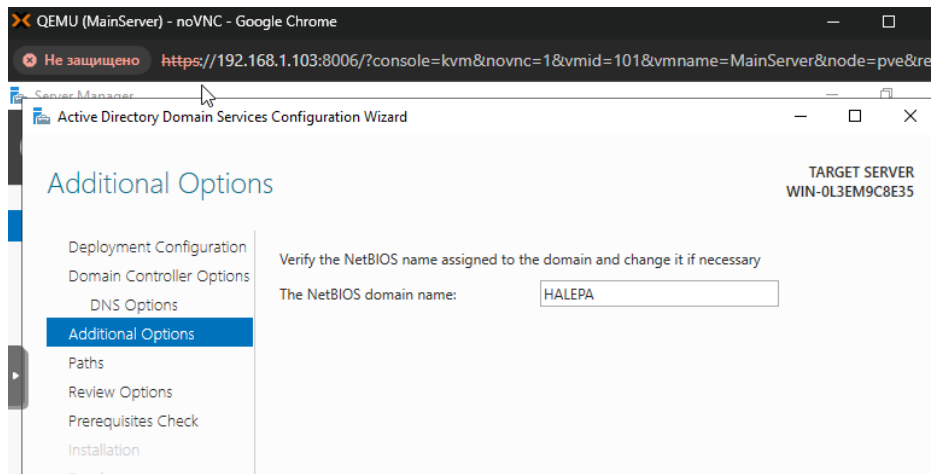


Рис. 3.35 – Налаштування Active Directory на головному сервері

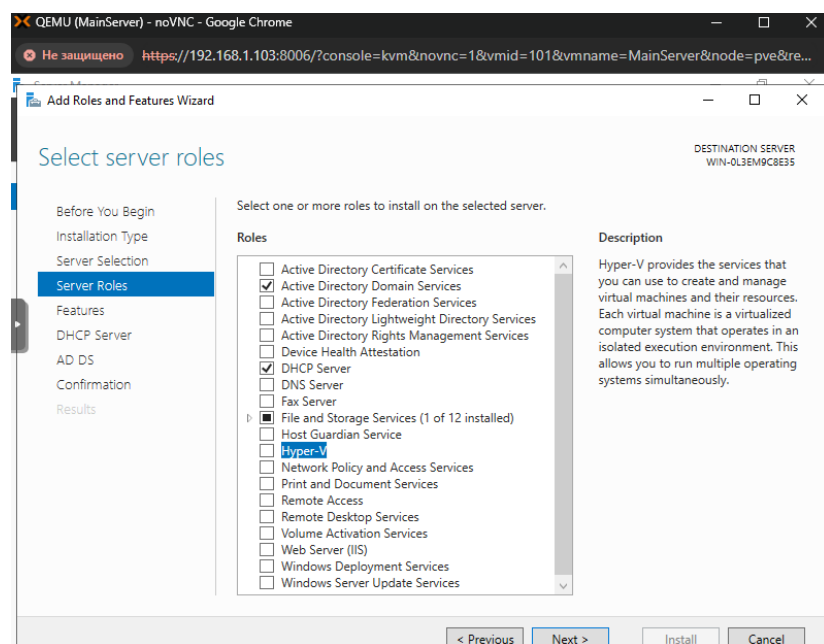


Рис. 3.36 – Налаштування Active Directory на головному сервері

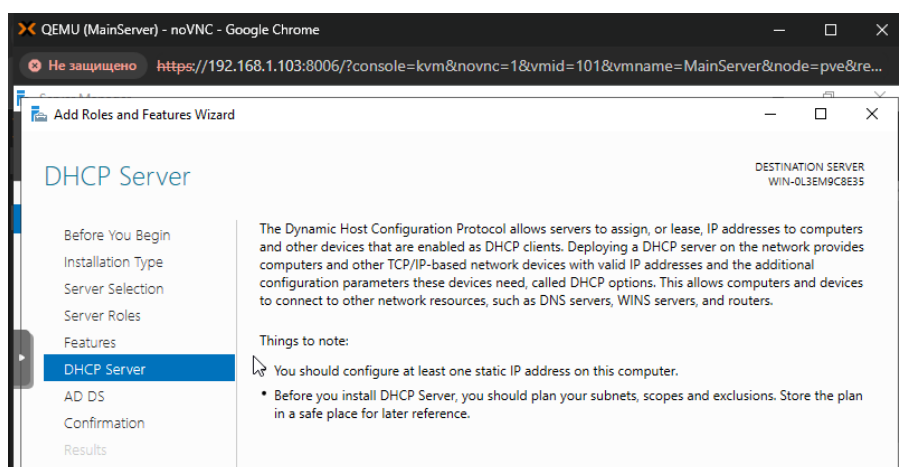


Рис. 3.37 – Налаштування Active Directory на головному сервері

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк. 64
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		

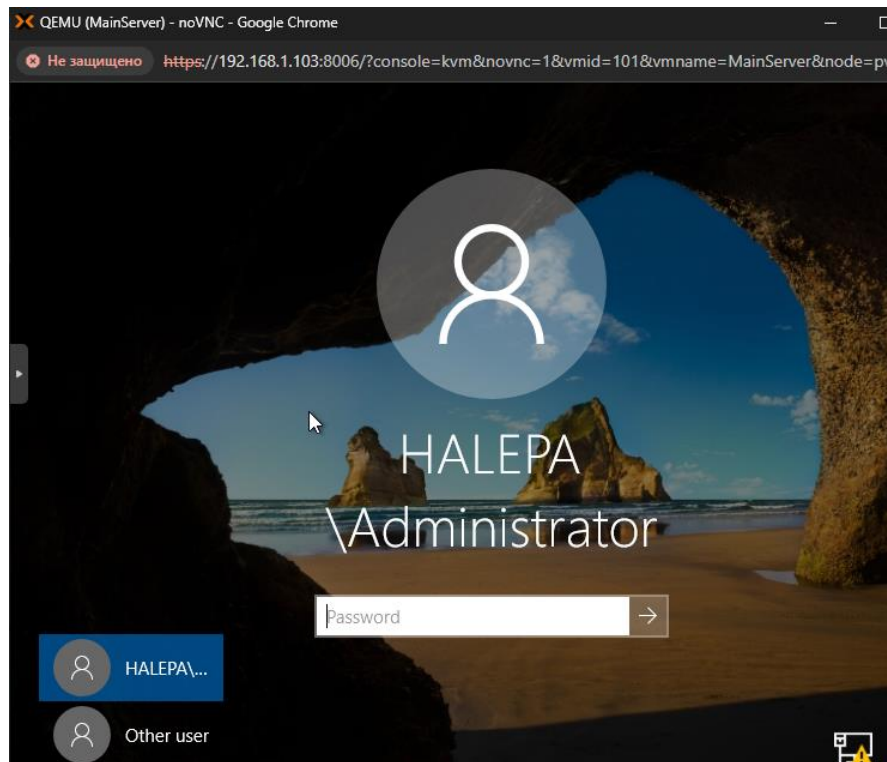


Рис. 3.38 – Налаштування Active Directory на головному сервері

Як можна побачити по рис.3.28. було успішно налаштовано домен на головному сервері. Тепер потрібно налаштувати доступ до папки, в яку будуть відправляти звіти і файли робітники компанії.

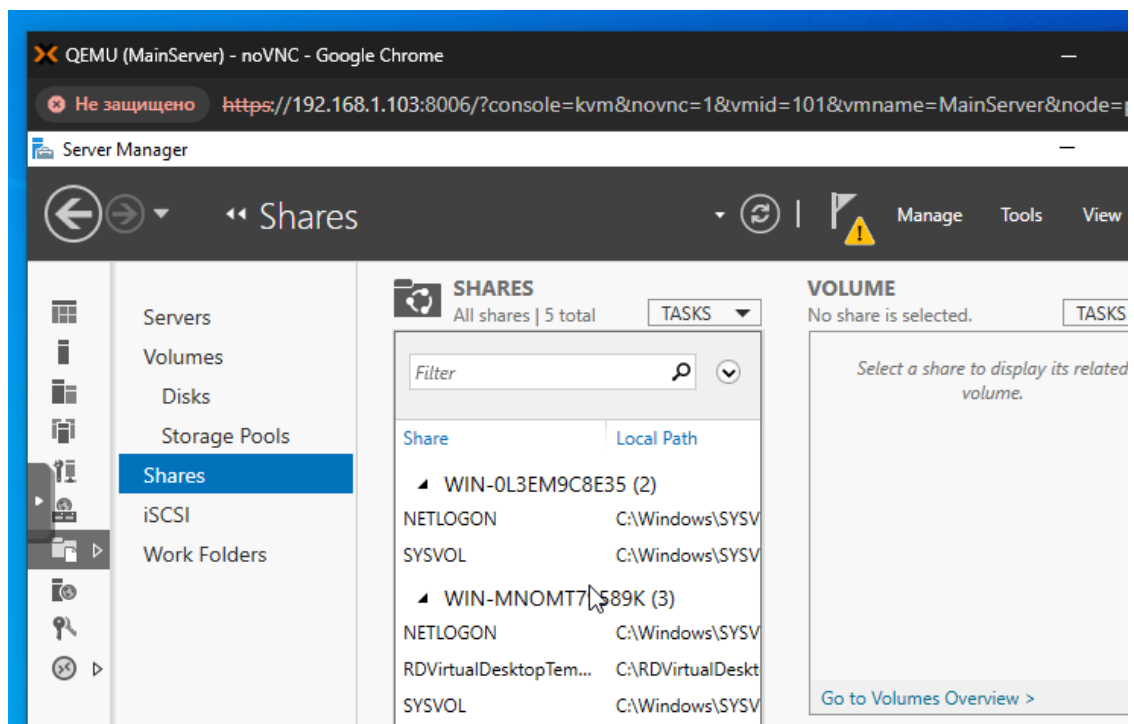


Рис. 3.39 – Налаштування доступу до папки на головному сервері

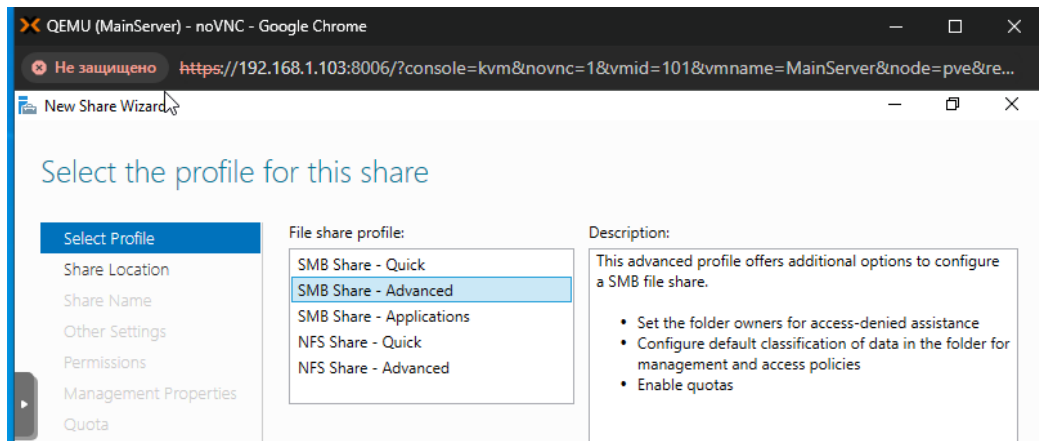


Рис. 3.40 – Налаштування доступу до папки на головному сервері

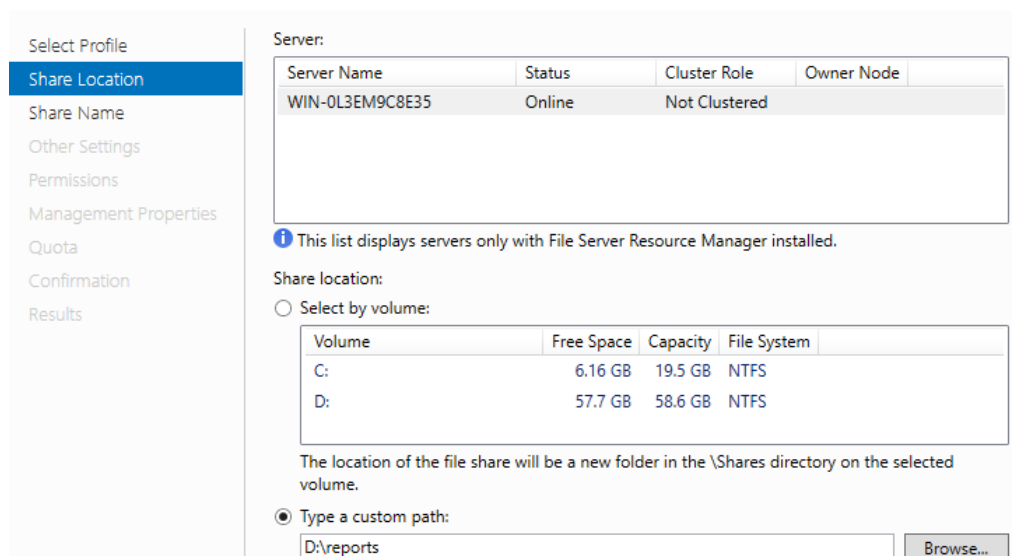


Рис. 3.41 – Налаштування доступу до папки на головному сервері

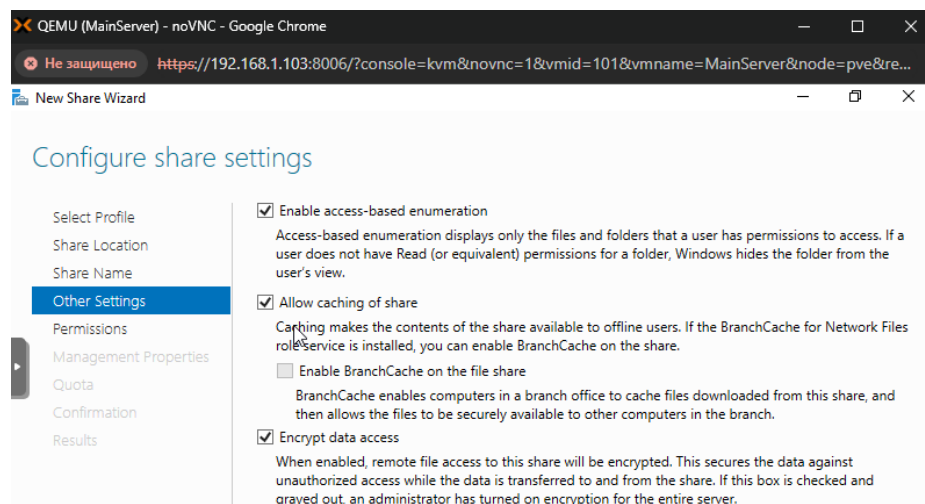


Рис. 3.42 – Налаштування доступу до папки на головному сервері

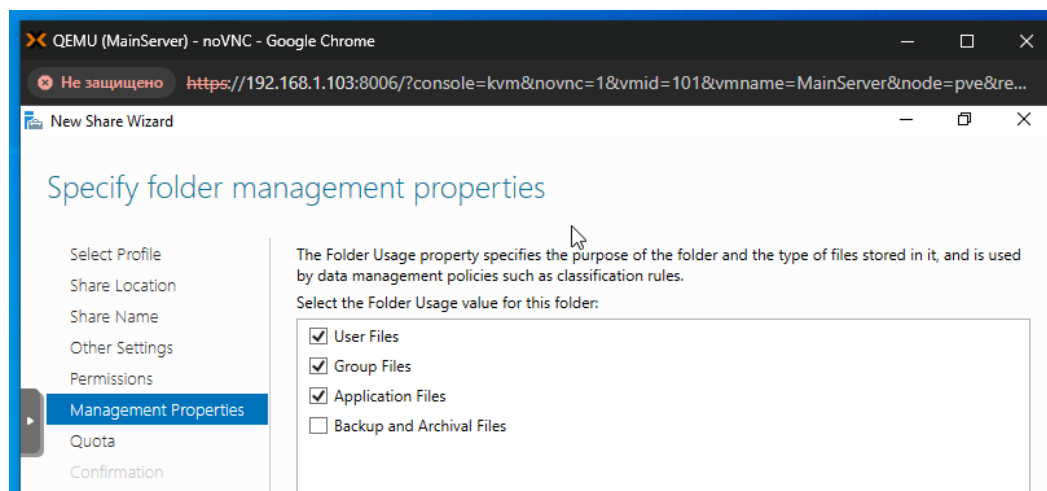


Рис. 3.43 – Налаштування доступу до папки на головному сервері

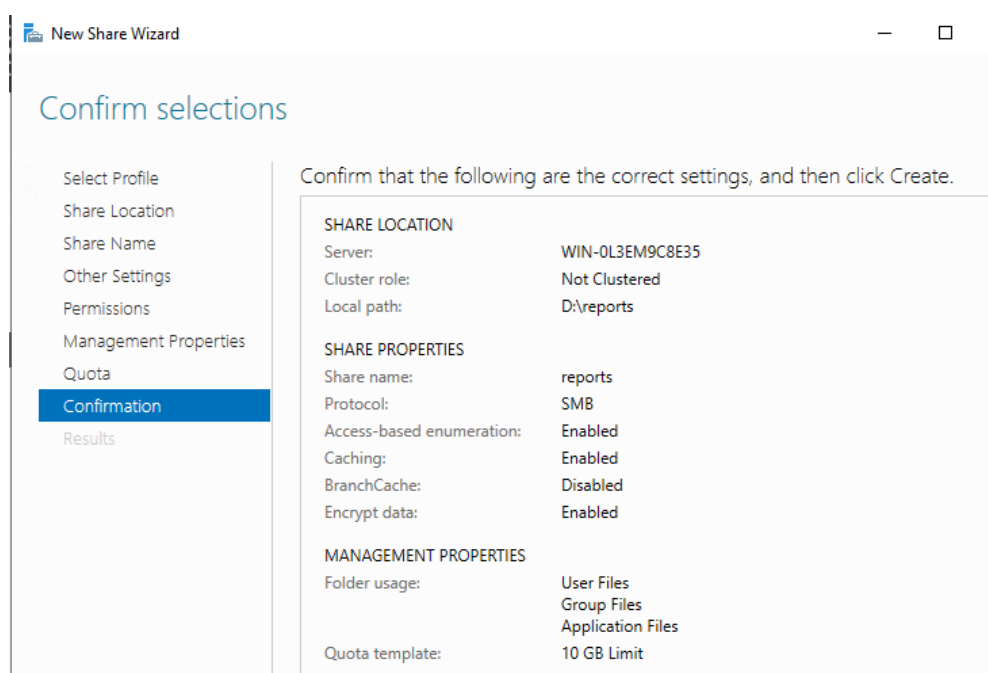


Рис. 3.44 – Налаштування доступу до папки на головному сервері

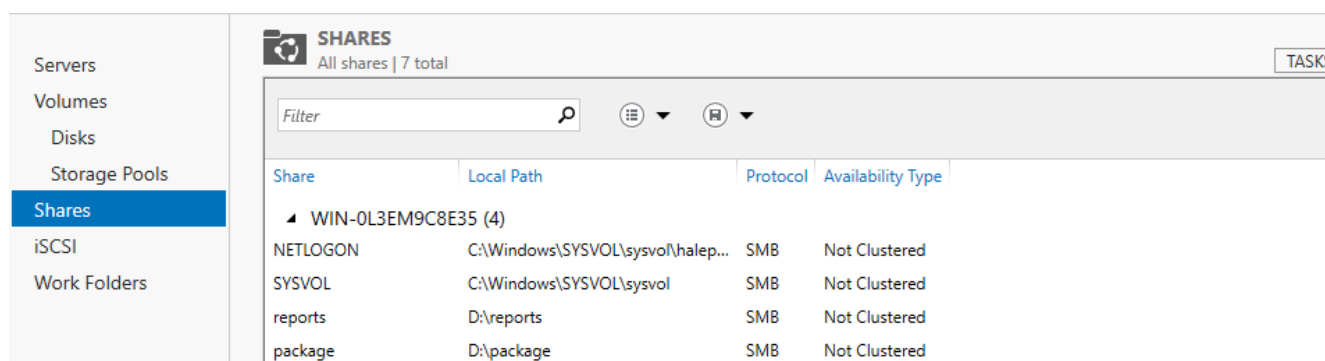


Рис. 3.45 – Налаштування доступу до папки на головному сервері

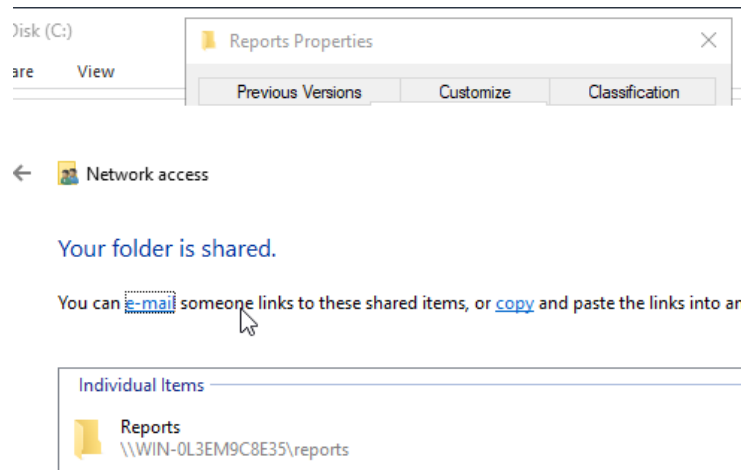


Рис. 3.46 – Перевірка доступу до папки на домені

Дальше потрібно створити групу користувачів і самих користувачів. Групи буде 3 – це адміни, керівники проєкту, бухгалтери.

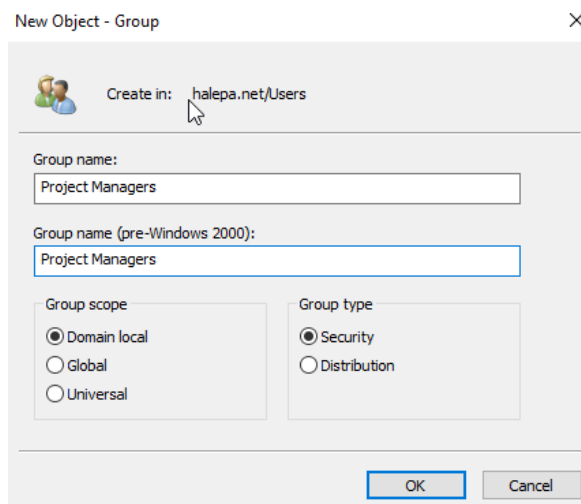


Рис. 3.47 – Створення груп користувачів

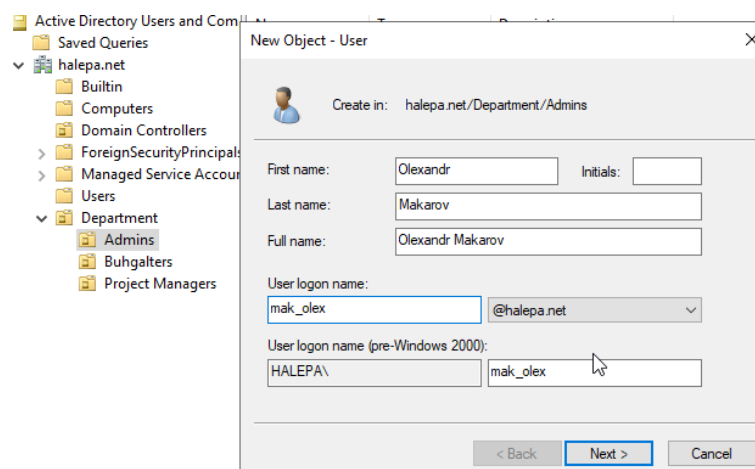


Рис. 3.48 – Створення користувачів

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

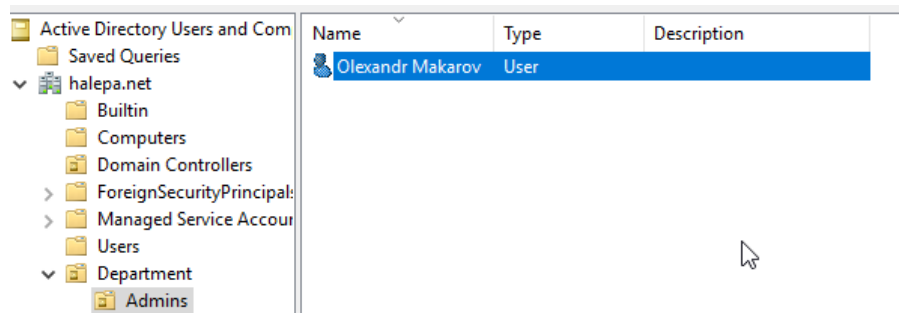


Рис. 3.49 – Створення користувачів

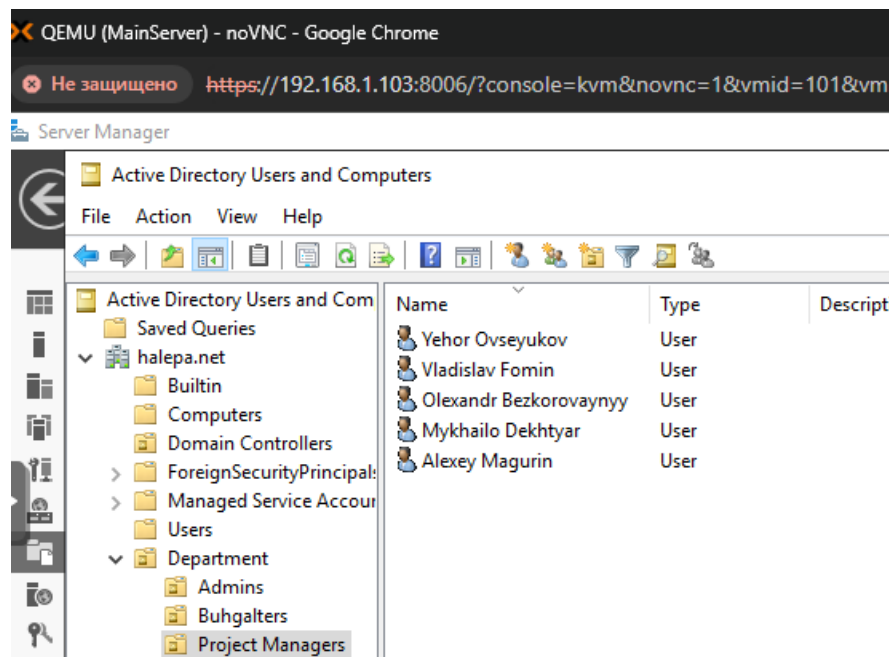


Рис. 3.50 – Створені користувачі

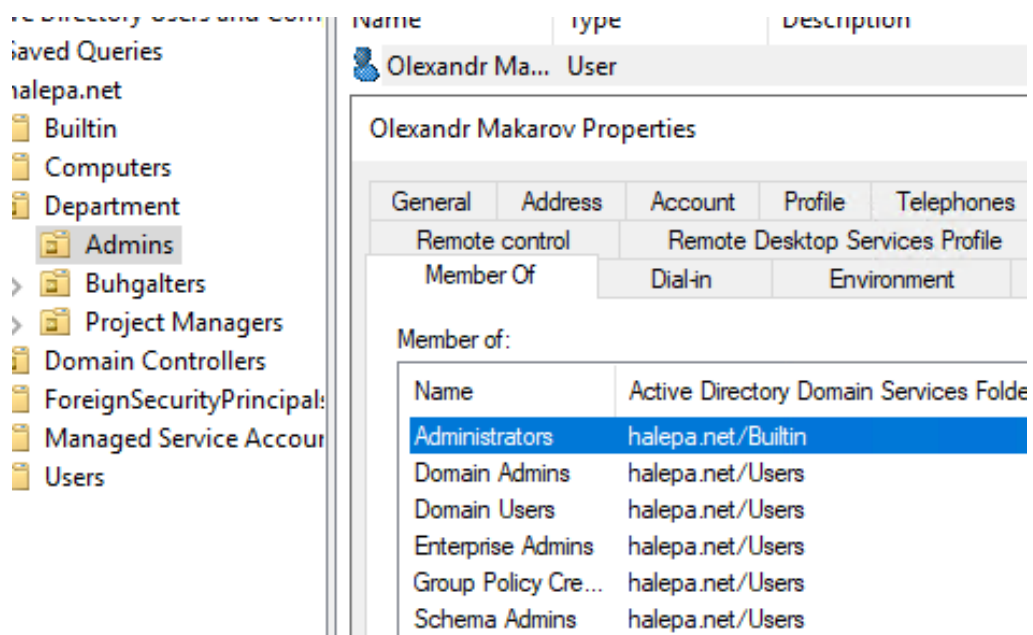


Рис. 3.51 – Групи адміна членом якого він являється

Тепер потрібно налаштувати доступ папок на сервері груп для користувачів. Група бухгалтери будуть мати право у папці Buhgalters створювати, копіювати, виконувати файли і папки, но при цьому вони можуть у папці Project Managers вставляти і копіювати файли в ній. Група керівників проєктів будуть мати ті самі права тільки навпаки.

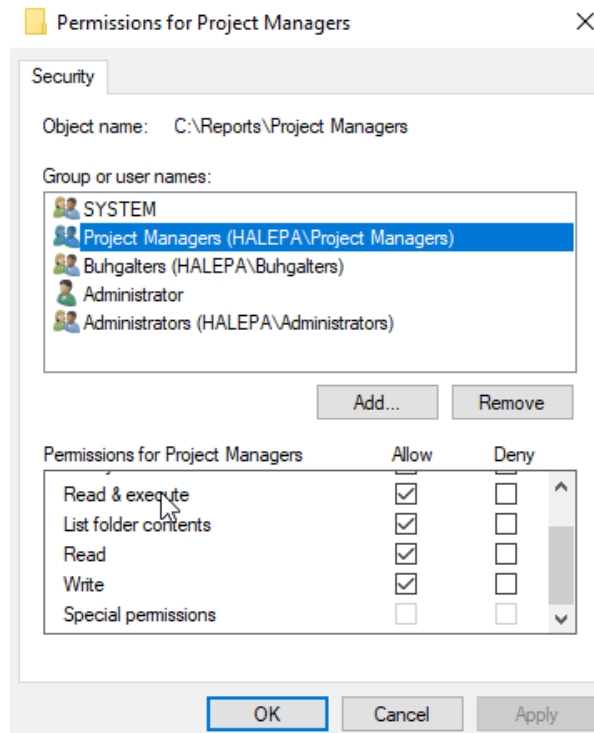


Рис. 3.52 – Налаштування прав

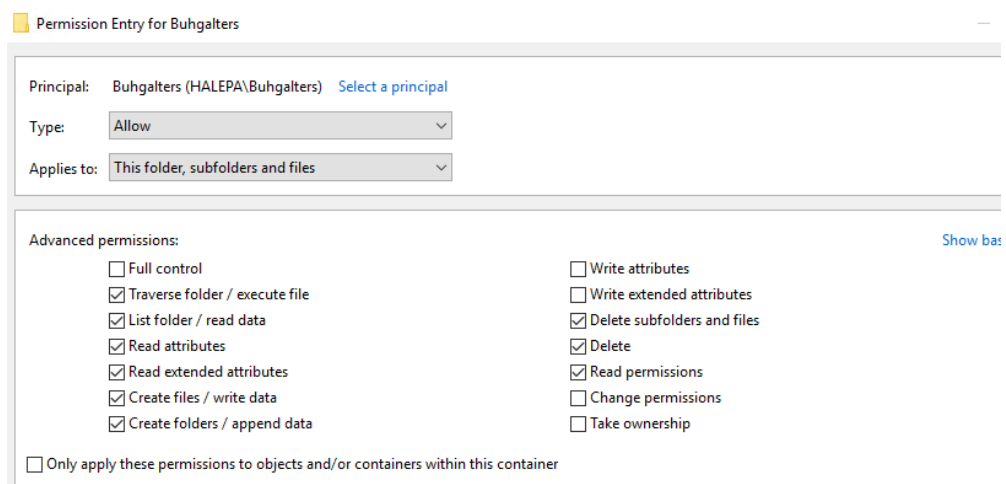


Рис. 3.53 – Налаштування прав

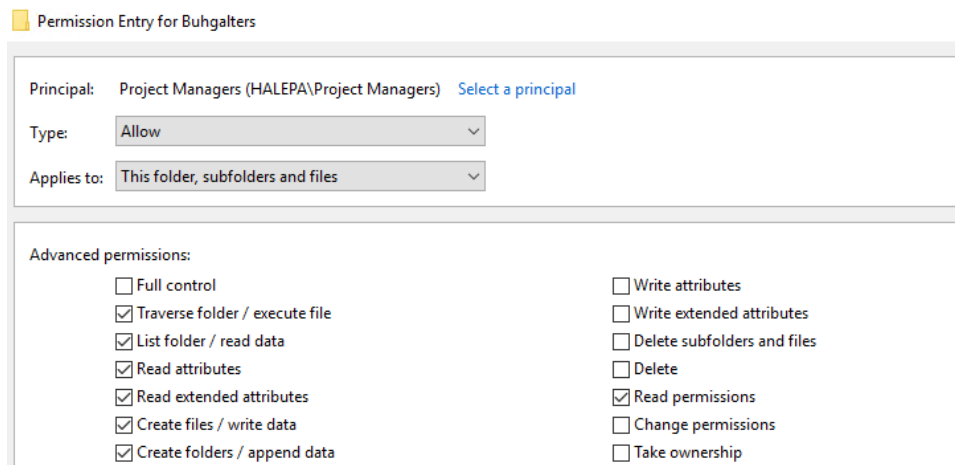


Рис. 3.54 – Налаштування прав

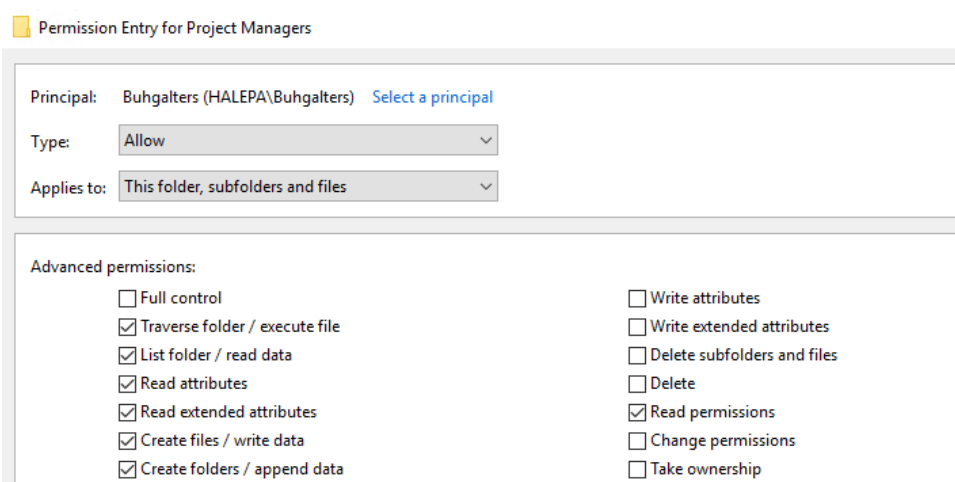


Рис. 3.55 – Налаштування прав

Тепер, після налаштування прав на папки, потрібно щоб користувачі автоматично підключалися до папок на сервері зі своєї робочої станції. Для цього потрібно налаштувати шлях до папок в менеджері групових політик.

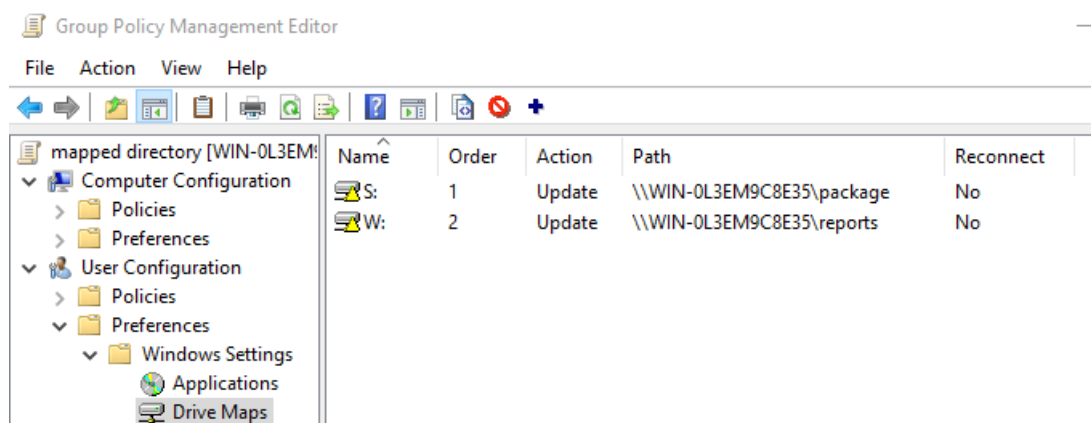


Рис. 3.56 – Налаштування доступу до папок для робочих станцій

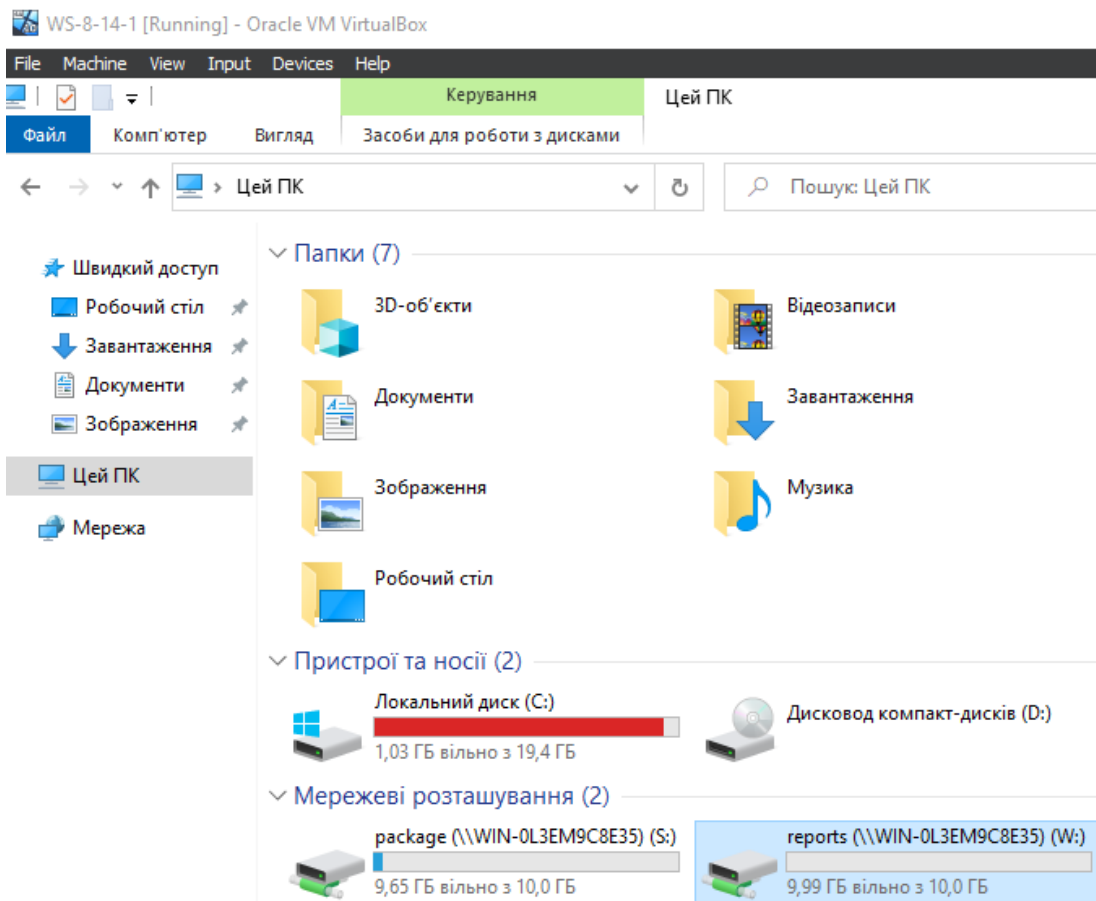


Рис. 3.57 – Перевірка доступу до папки на робочій станції

Для того щоб звичайні працівники могли працювати потрібно встановити ПЗ подібний до Microsoft Office. Для цього підійде його безплатний аналог LibreOffice, в ньому є весь потрібний інструментарій подібний до word, excel, powerpoint. Через менеджера групових полік можна налаштувати встановлення ПЗ.

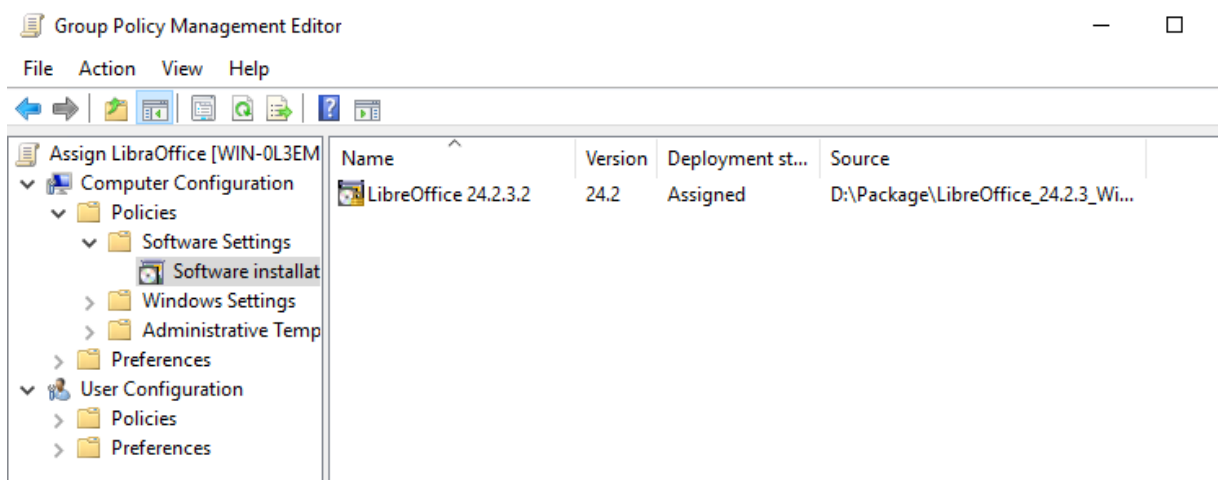


Рис. 3.58 – Налаштування встановлення ПЗ через GPM

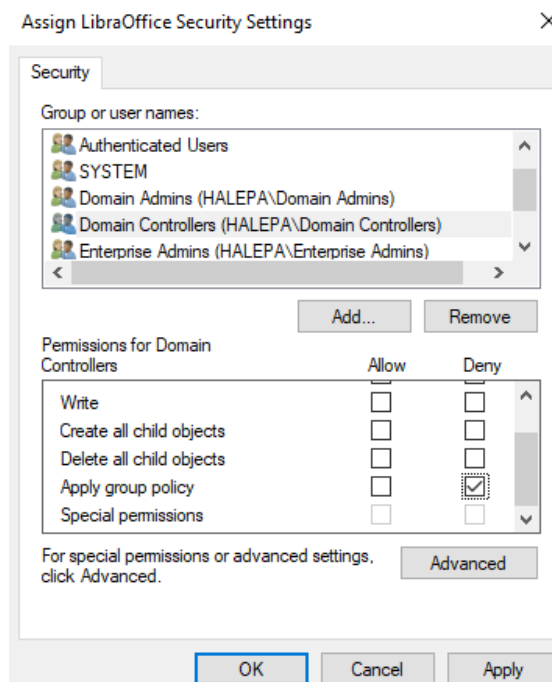


Рис. 3.59 – Заборона на встановлення ПЗ на контролери домену

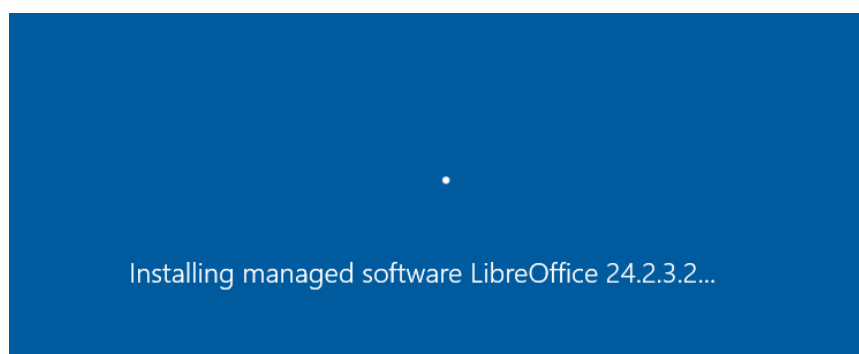


Рис. 3.60 – Встановлення ПЗ при запуску

Тепер потрібно налаштувати створення ярликів для працівників, щоб вони мали доступ до потрібного їм інструментарію на робочому столі.

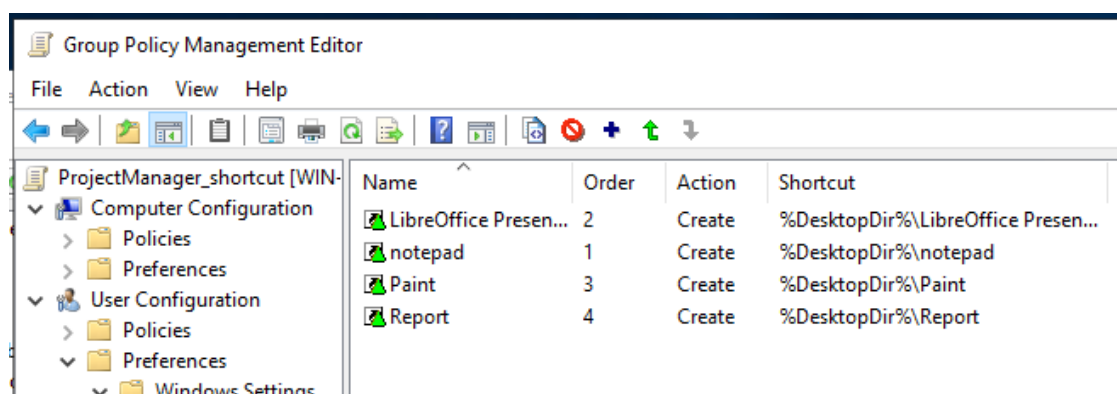


Рис. 3.61 – Налаштування створення ярликів для менеджерів проекту

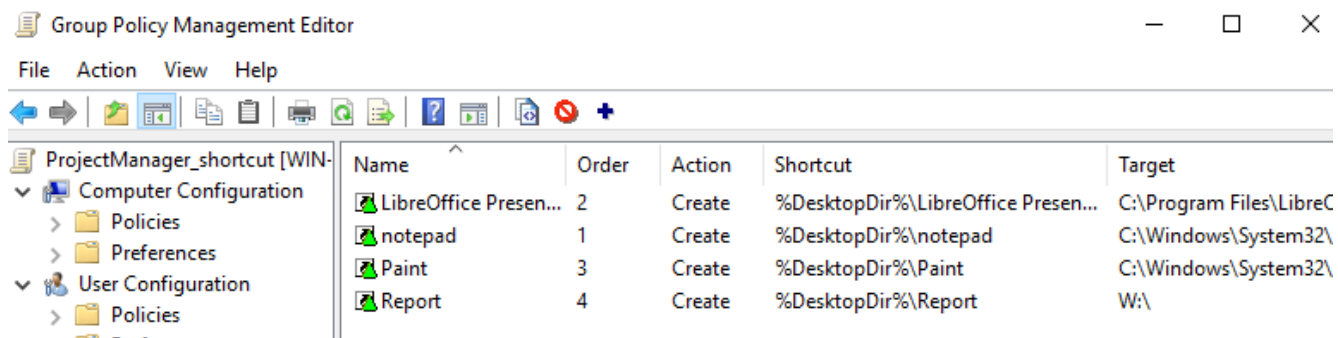


Рис. 3.62 – Налаштування створення ярликів для менеджерів проекту

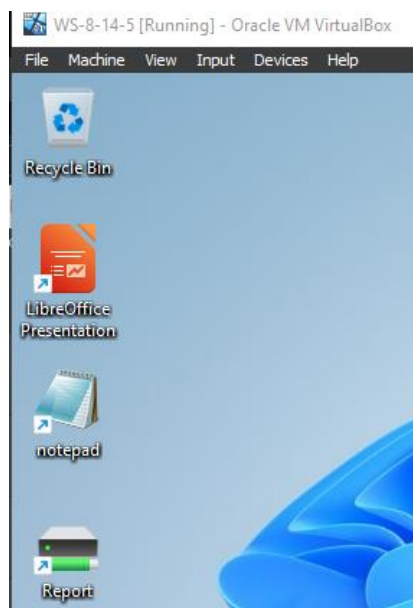


Рис. 3.63 – Перевірка створення ярликів на робочій станції

Тепер потрібно налаштувати DHCP-сервер, щоб звичайні користувачі могли підключитися до мережі при під'єднанні до нього.

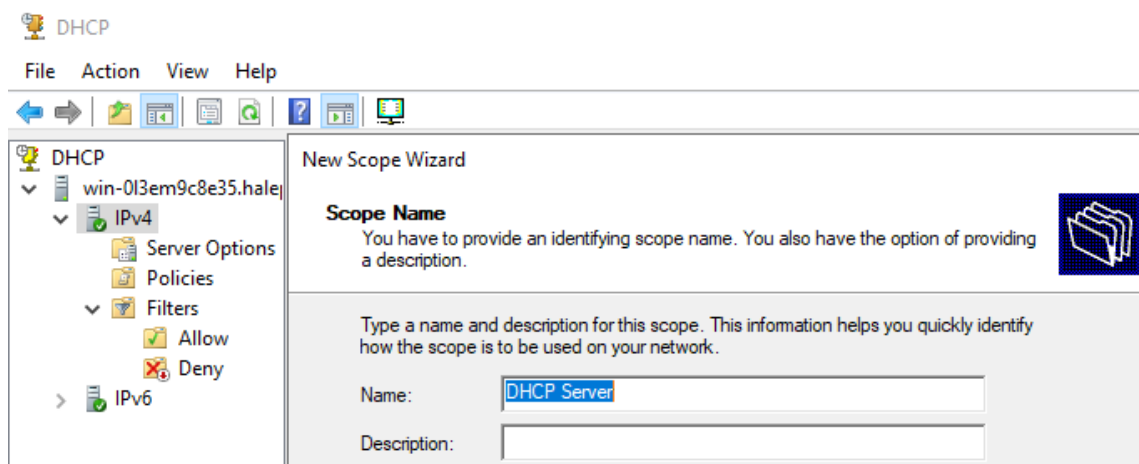


Рис. 3.64 – Налаштування DHCP-сервера

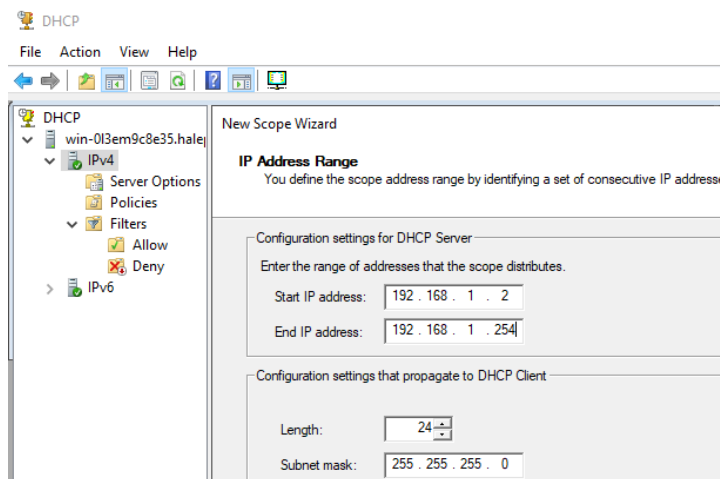


Рис. 3.65 – Налаштування DHCP-сервера

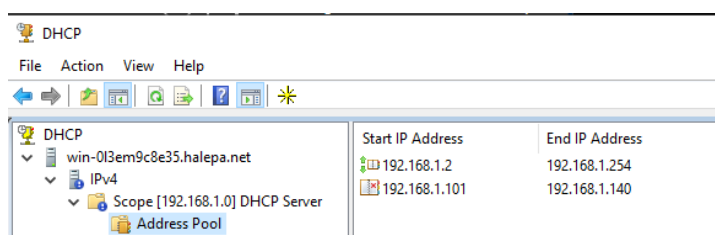


Рис. 3.66 – Налаштування DHCP-сервера

На цьому етапі завершено налаштування головного серверу.

3.4. Створення і налаштування термінального серверу

В цьому пункті будуть показано створення, налаштування термінального серверу. В налаштування входить Remote Desktop Protocol та підключення вже до існуючого домену. Буде пропущений момент з встановлення операційної системи, так як він не буде відрізнятися від того, що було показано на головному сервері.

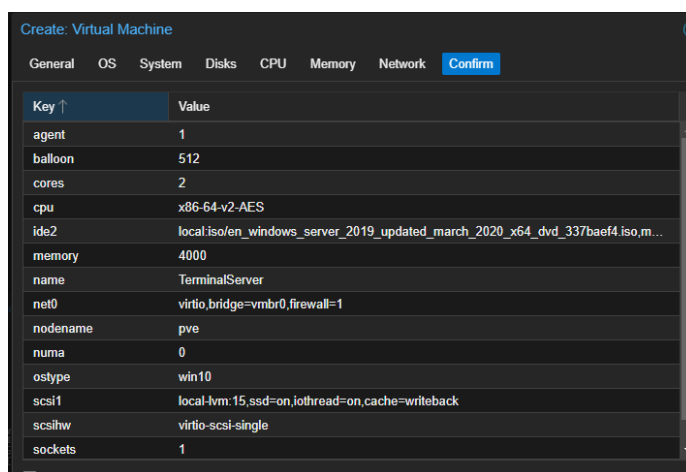


Рис. 3.67 – Створення термінального серверу

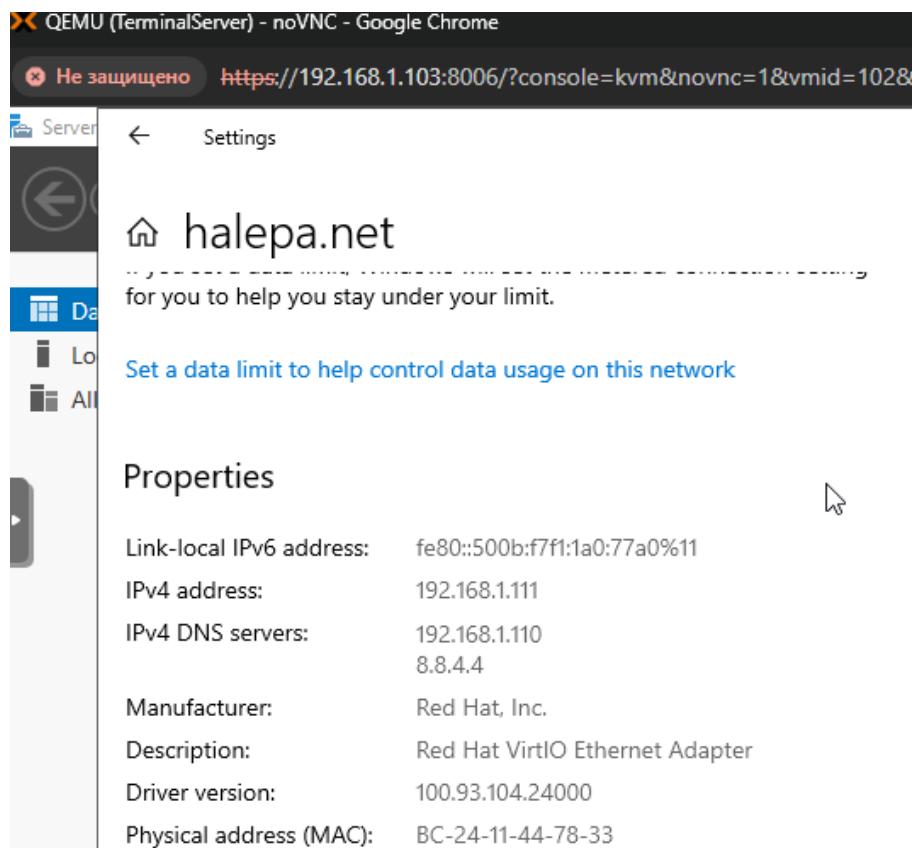


Рис. 3.68 – Налаштування ір-адресації

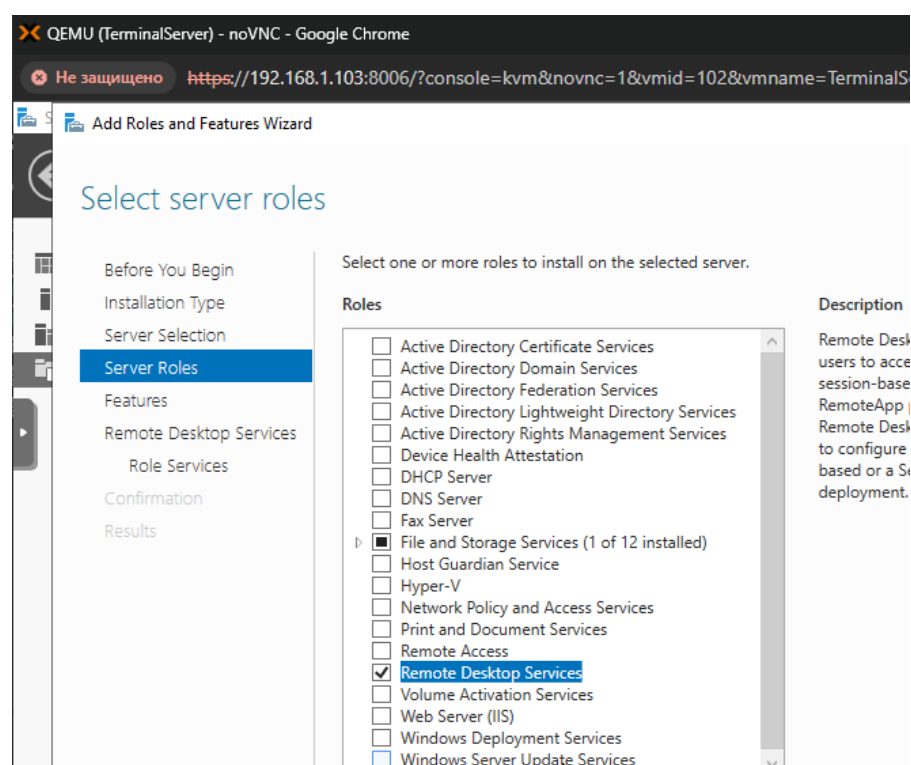


Рис. 3.69 – Налаштування RDP на термінальному сервері

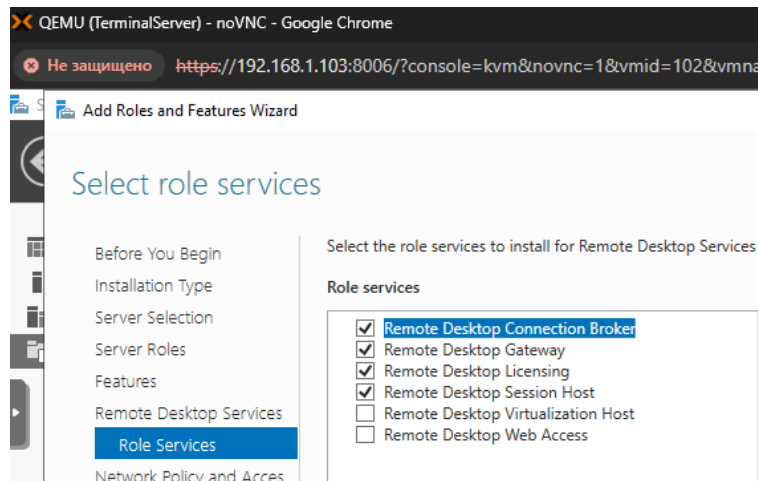


Рис. 3.70 – Налаштування RDP на термінальному сервері

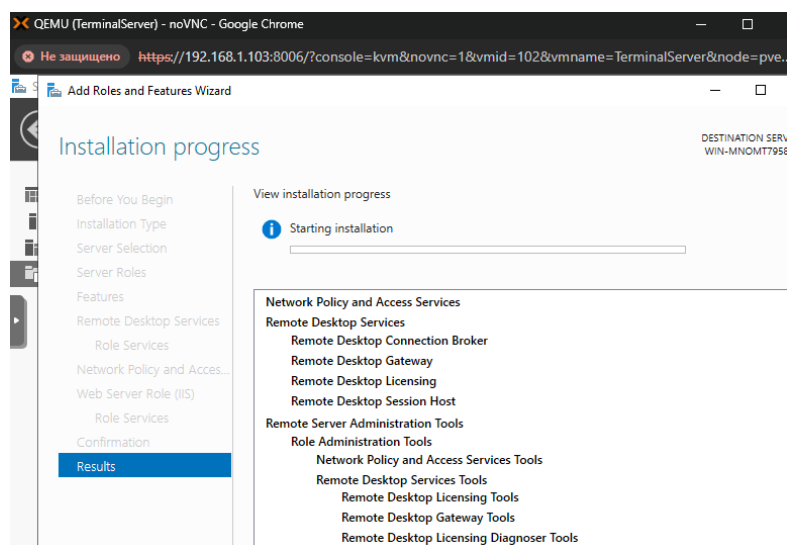


Рис. 3.71 – Налаштування RDP на термінальному сервері

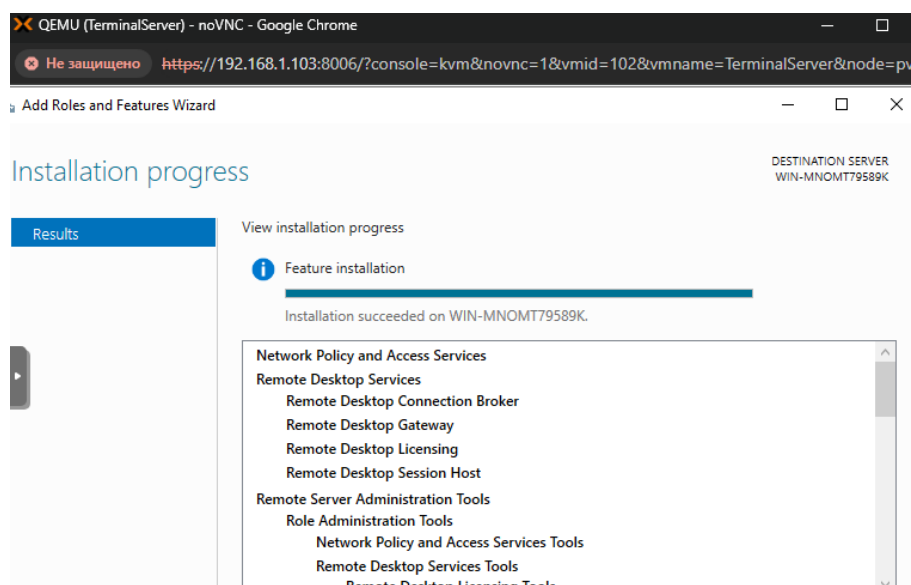


Рис. 3.72 – Налаштування RDP на термінальному сервері

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

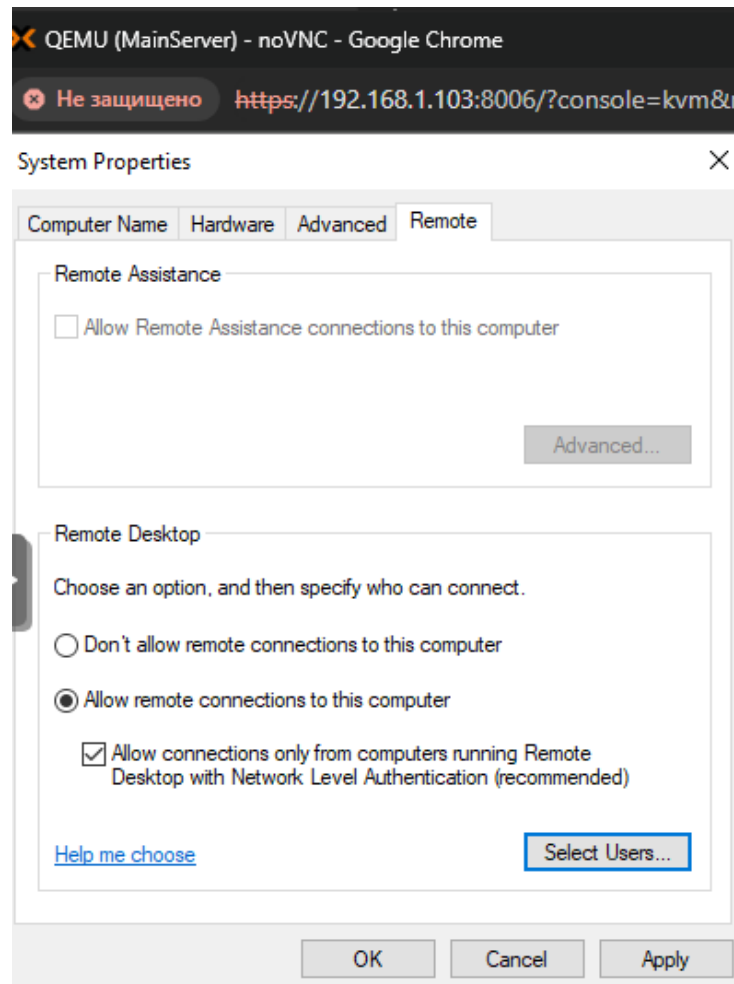


Рис. 3.73 – Надання дозвілу на підключення до головного сервера

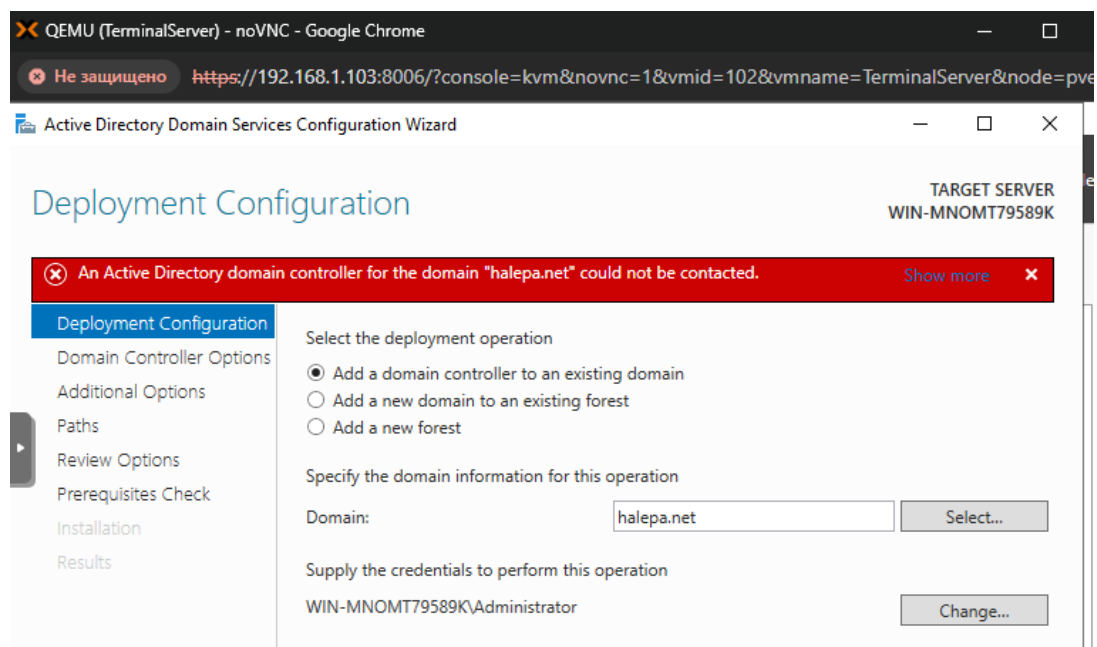


Рис. 3.74 – Підключення до домену на термінальному сервері

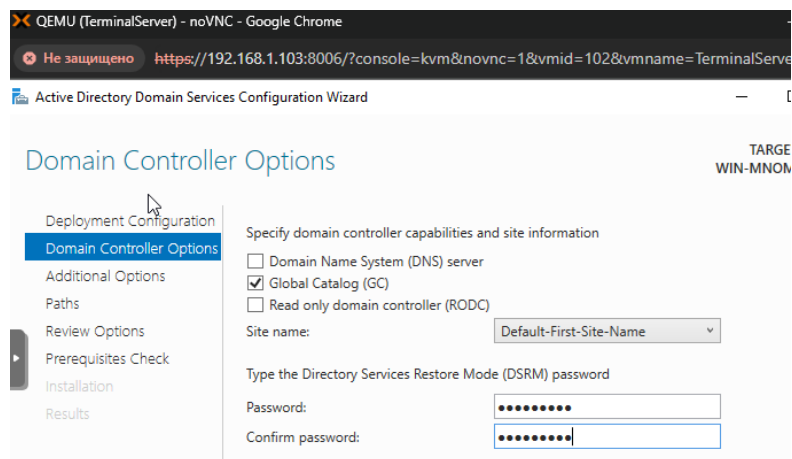


Рис. 3.75 – Підключення до домену на термінальному сервері

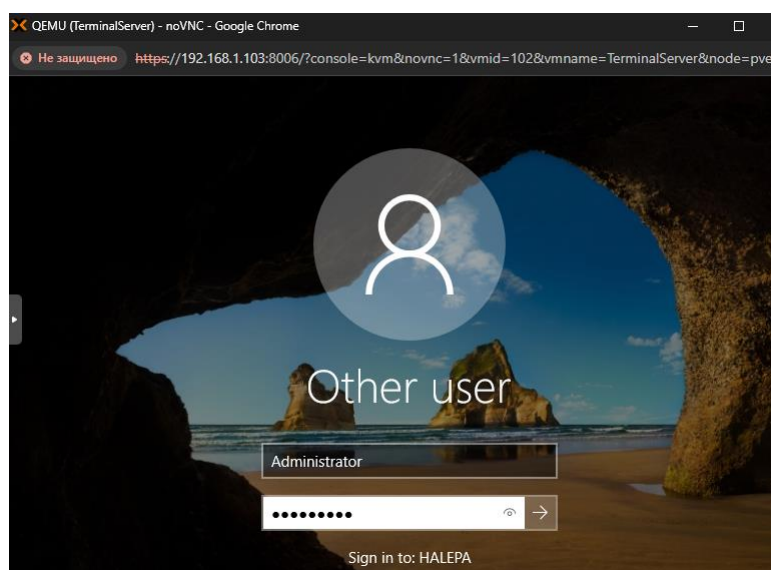


Рис. 3.76 – Підключення до домену на термінальному сервері

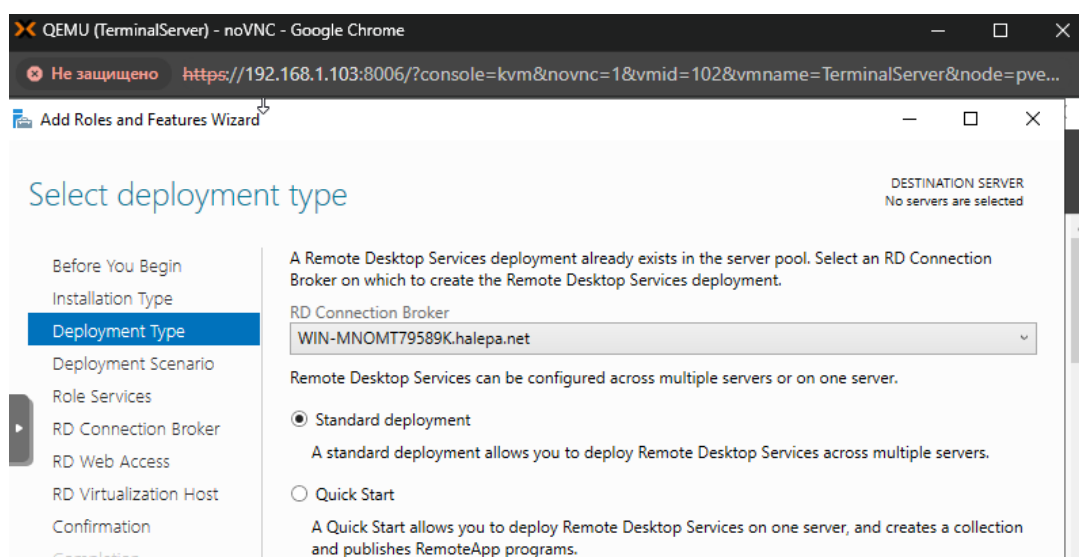


Рис. 3.77 – Налаштування RDP на термінальному сервері

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

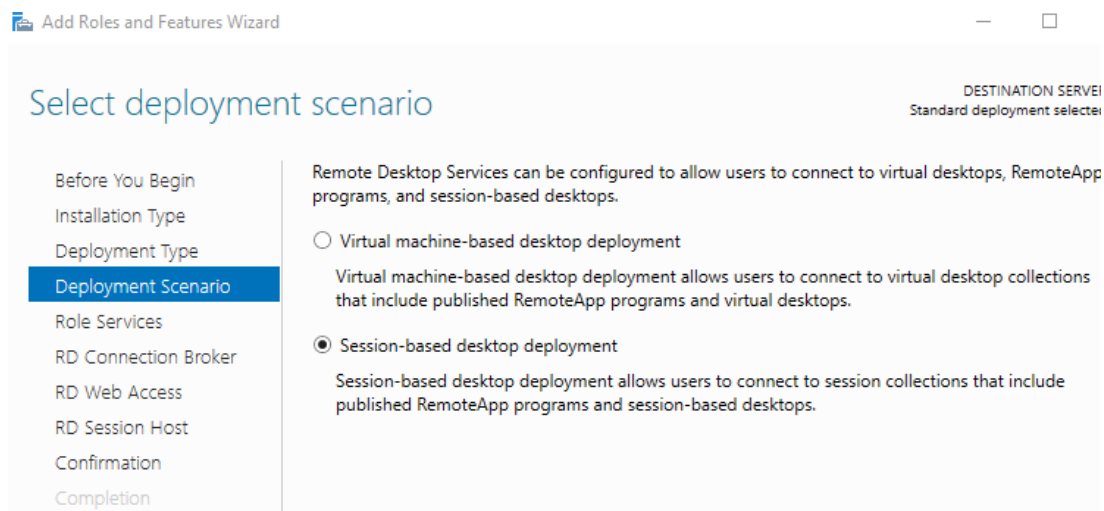


Рис. 3.78 – Налаштування RDP на термінальному сервері

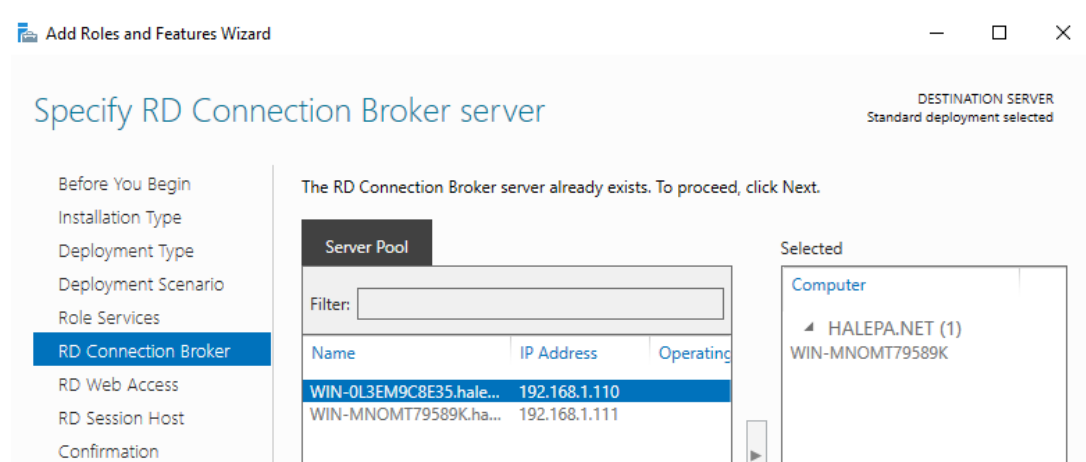


Рис. 3.79 – Налаштування RDP на термінальному сервері

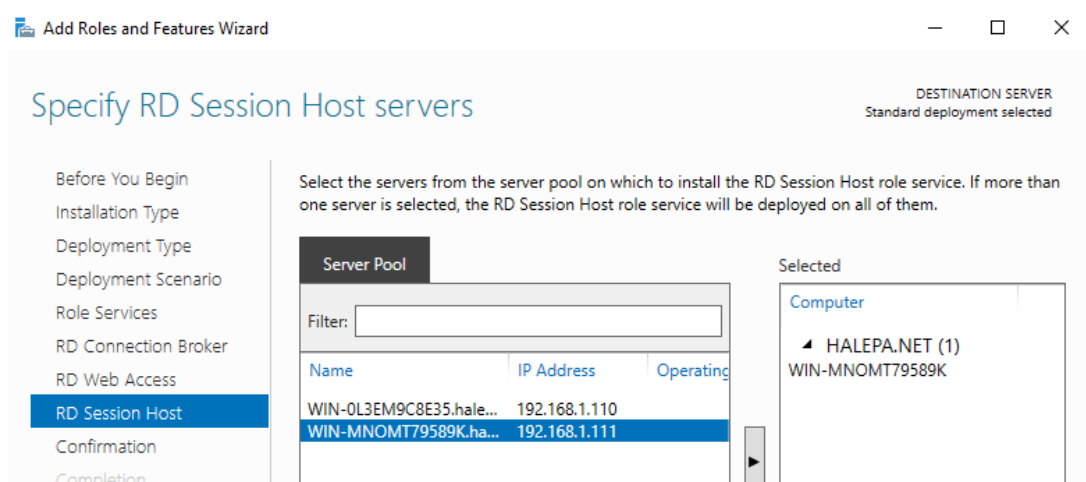


Рис. 3.80 – Налаштування RDP на термінальному сервері

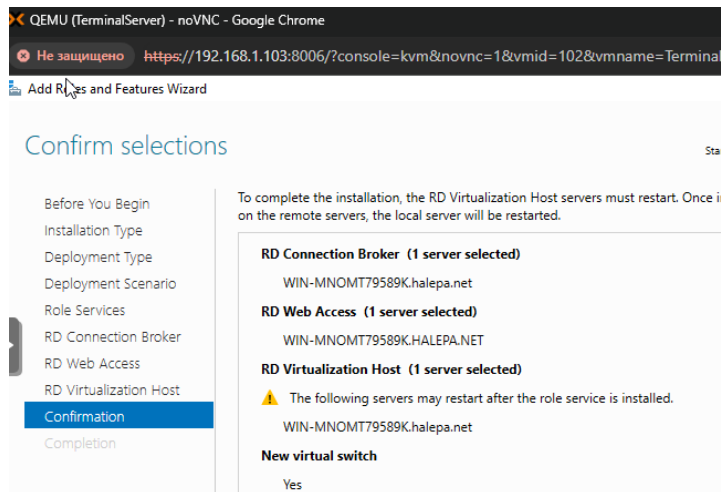


Рис. 3.81 – Налаштування RDP на термінальному сервері

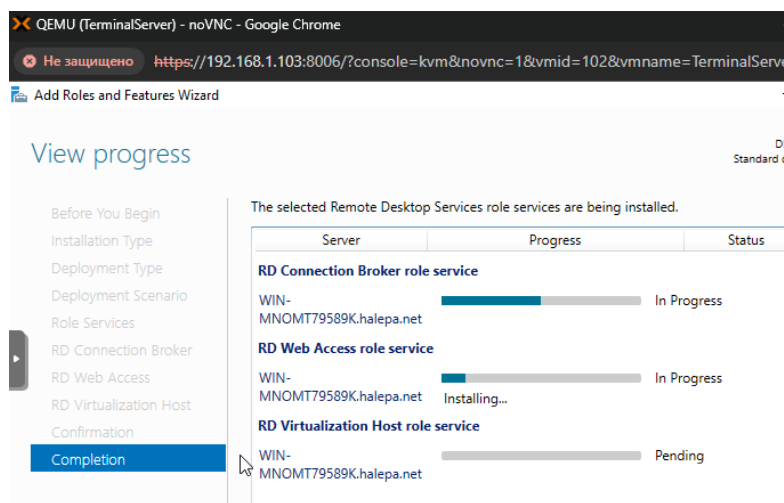


Рис. 3.82 – Налаштування RDP на термінальному сервері

Далі потрібно створити сертифікат, який використовуватиметься для ліцензування. У даному прикладі це буде самопідписаний сертифікат (selfsigned cetificate). Його можна створити засобами PowerShell.

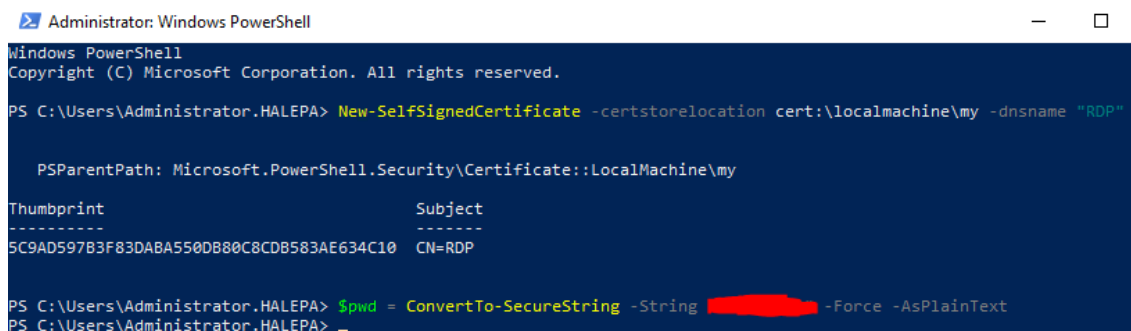


Рис. 3.83 – Створення сертифікату

Далі ми будемо завантажувати новостворений сертифікат у вигляді файлу.
Для цього необхідно консоль mmc та оснащення Certificates.

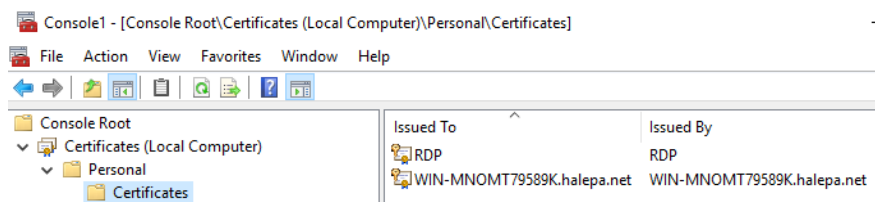


Рис. 3.84 – Створений сертифікату

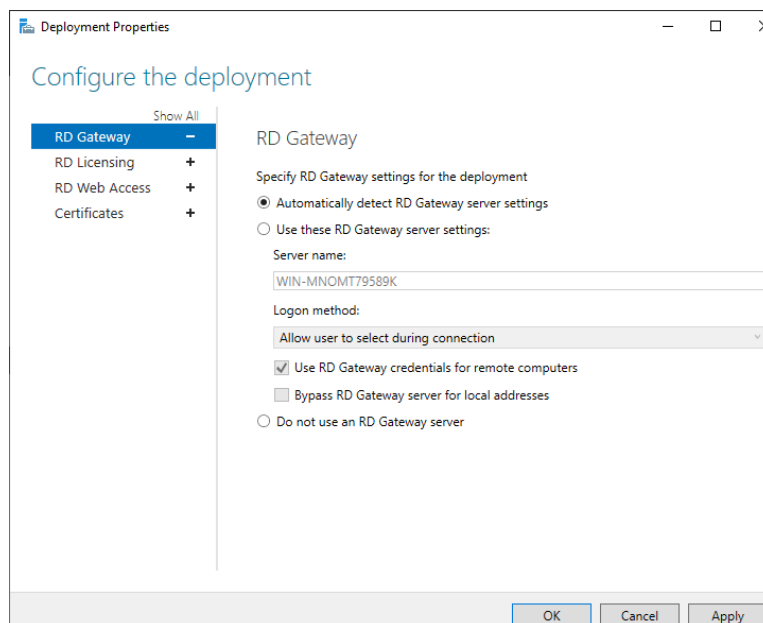


Рис. 3.85 – Налаштування RD

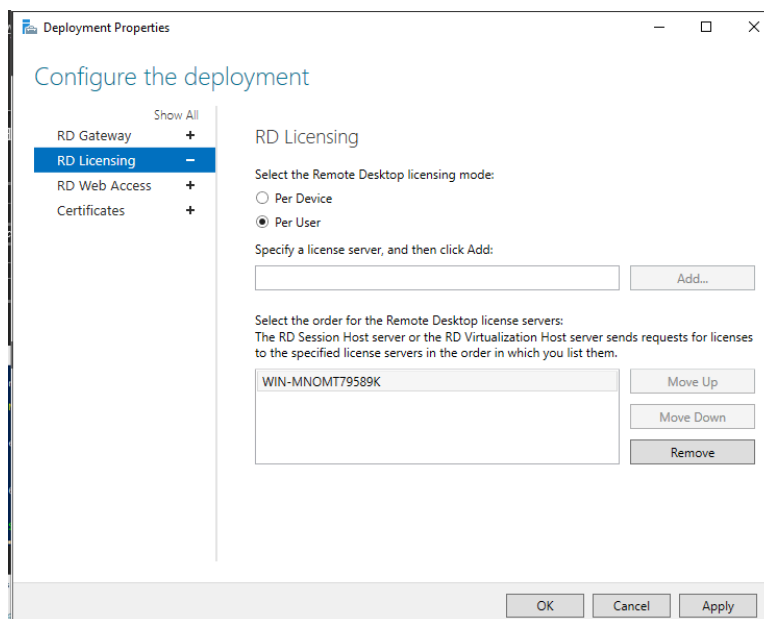


Рис. 3.86 – Налаштування RD

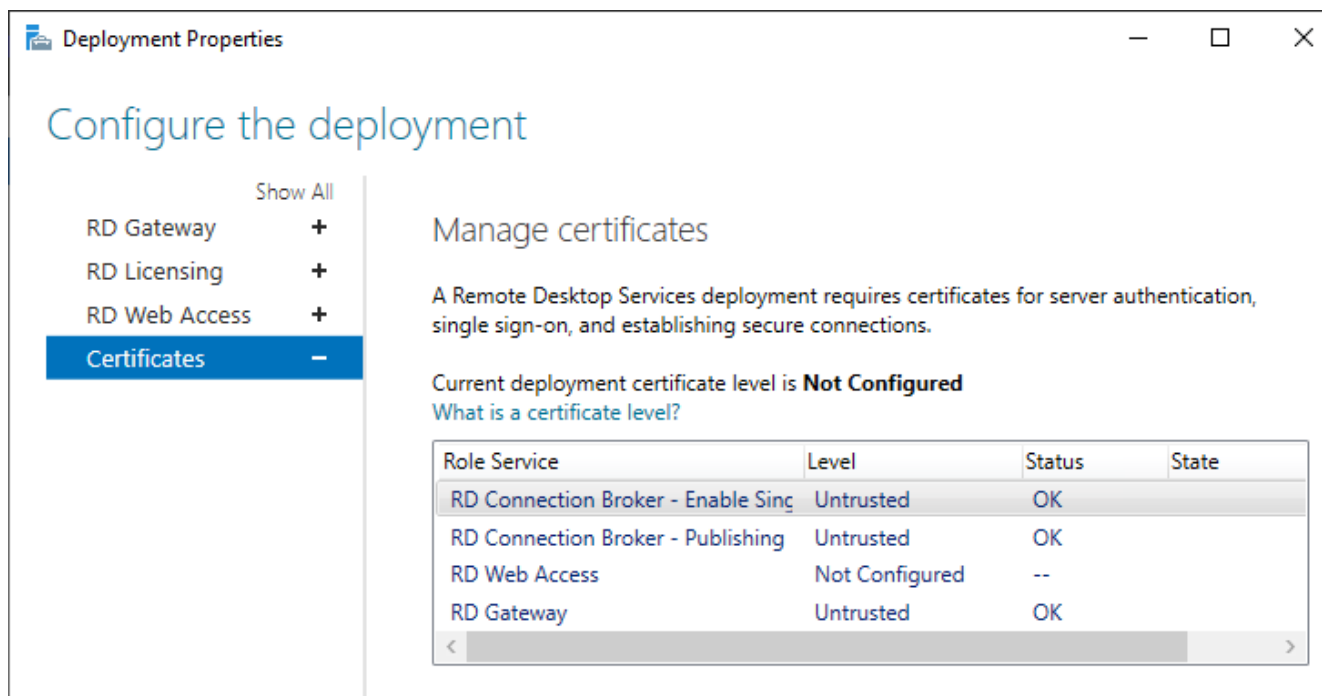


Рис. 3.87 – Імпортування сертифікату

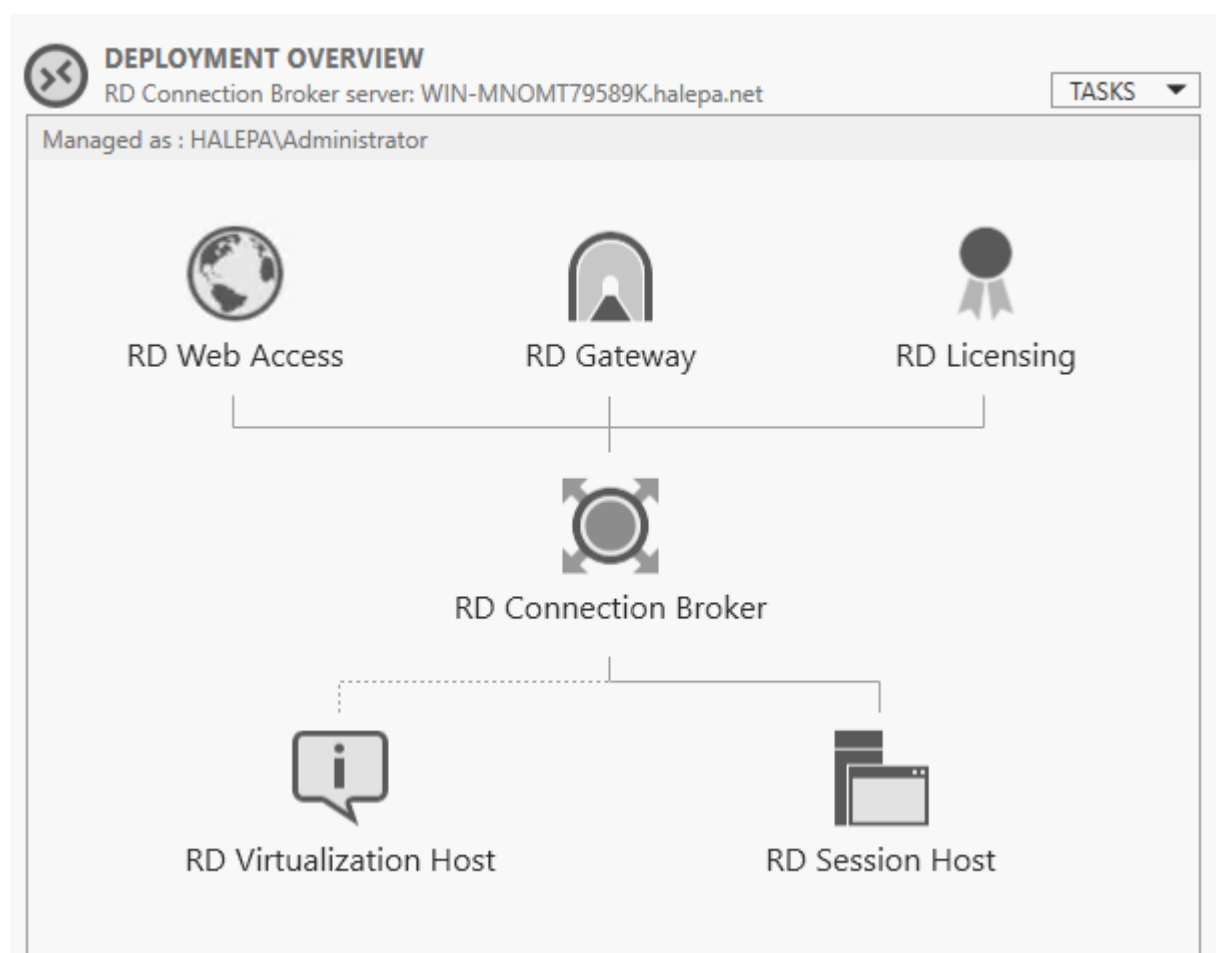


Рис. 3.88 – Результат налаштування RD на термінальному сервері

3.5. Налаштування робочої станції

В цьому пункті будуть показано налаштування ір-адресації на робочій станції та підключення його до домену halera. Також буде показано спробу підключитись через робочу станцію до головного серверу.

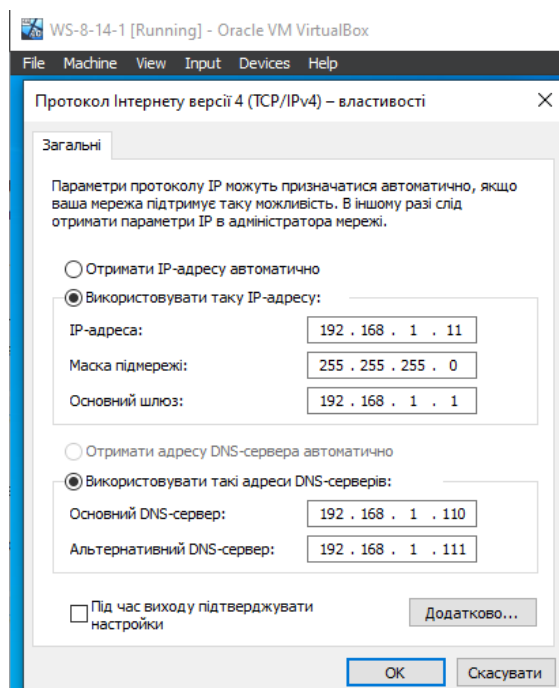


Рис. 3.89 – Налаштування ір-адресації

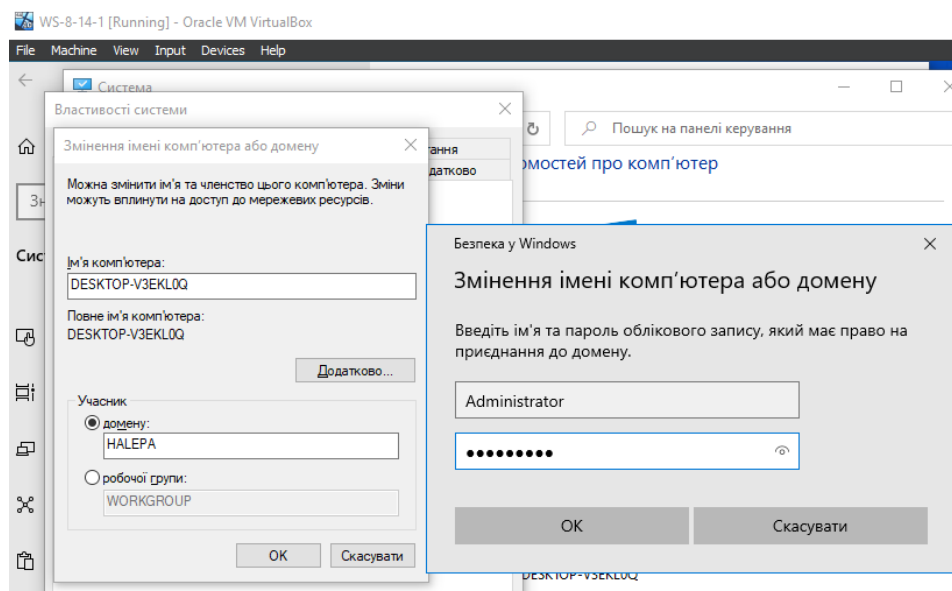


Рис. 3.90 – Підключення робочої станції до домену

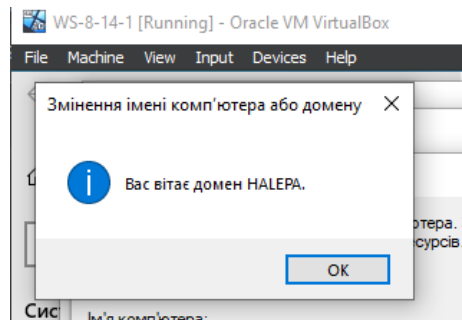


Рис. 3.91 – Підключення робочої станції до домену

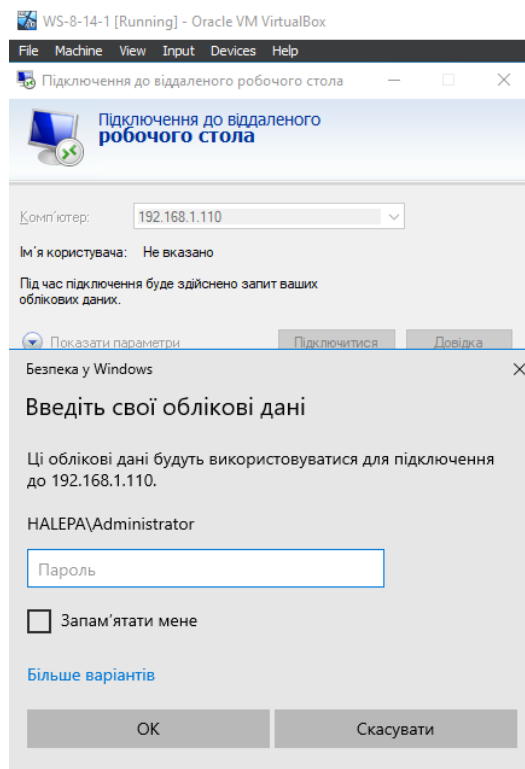


Рис. 3.92 – Підключення робочої станції до серверу

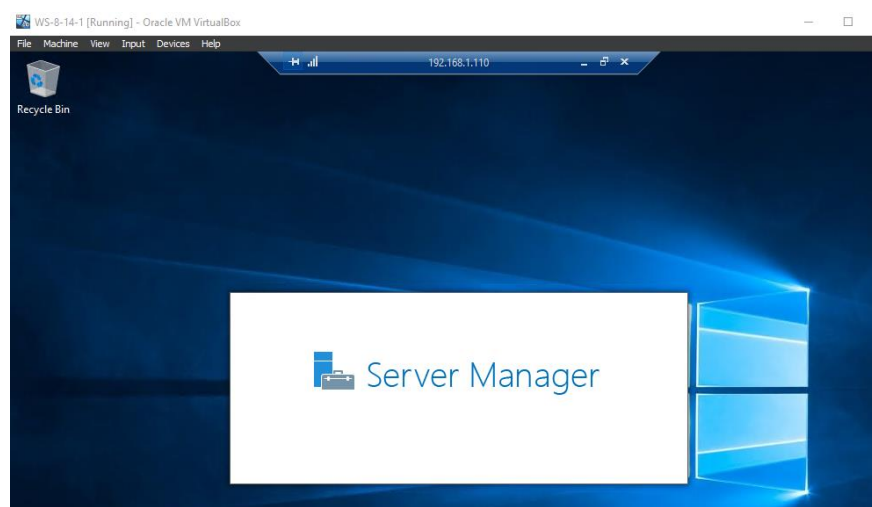


Рис. 3.93 – Підключення робочої станції до серверу

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

3.6. Налаштування OpenVPN

Для початку, потрібно встановити сам VPN-сервіс OpenVPN

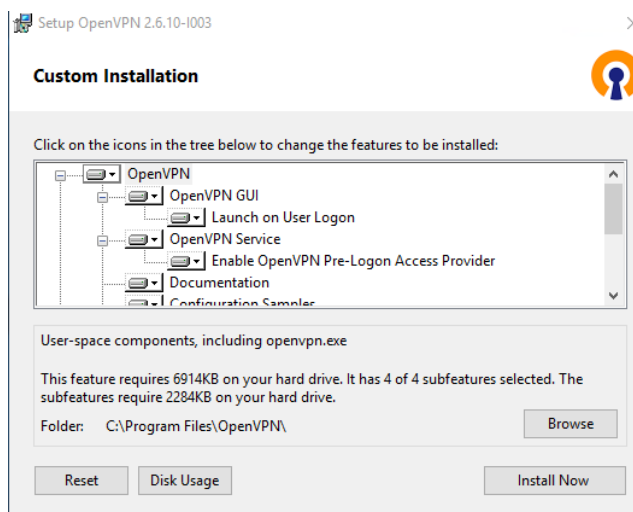


Рис. 3.94 – Встановлення OpenVPN

```
EasyRSA Shell
# ./easysrsa init-pki

WARNING!!!

You are about to remove the EASYRSA_PKI at:
* C:/Program Files/OpenVPN/easy-rsa/pki

and initialize a fresh PKI here.

Type the word 'yes' to continue, or any other input to abort.
Confirm removal: yes

Notice
-----
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* C:/Program Files/OpenVPN/easy-rsa/pki

Using Easy-RSA configuration:
* undefined

EasyRSA Shell
# ./easysrsa build-ca nopass
No Easy-RSA 'vars' configuration file exists!

Using SSL:
* openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:server

Notice
-----
CA creation complete. Your new CA certificate is at:
* C:/Program Files/OpenVPN/easy-rsa/pki/ca.crt
```

Рис. 3.95 – Створення сертифікатів

```

EasyRSA Shell
# ./easyrsa build-server-full server nopass
No Easy-RSA 'vars' configuration file exists!

Using SSL:
* openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)

Notice
-----
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: C:/Program Files/OpenVPN/easy-rsa/pki/reqs/server.req
* key: C:/Program Files/OpenVPN/easy-rsa/pki/private/server.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = server

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes

Using configuration from C:/Program Files/OpenVPN/easy-rsa/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'server'
Certificate is to be certified until Sep 11 23:27:15 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/issued/server.crt

Notice
-----
Inline file created:
* C:/Program Files/OpenVPN/easy-rsa/pki/inline/server.inline

```

Рис. 3.96 – Створення сертифікатів

```

EasyRSA Shell
# ./easyrsa gen-dh
No Easy-RSA 'vars' configuration file exists!

Using SSL:
* openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
Generating DH parameters, 2048 bit long safe prime
DH parameters appear to be ok.

Notice
-----

DH parameters of size 2048 created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/dh.pem

```

Рис. 3.97 – Створення сертифікатів

Створенні файли копіюємо в папку config-auto, потім переходимо до створення конфігураційного файлу. Налаштування конфігураційного файлу показано у додатку А

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

This PC > Local Disk (C:) > Program Files > OpenVPN > config-auto				
	Name	Date modified	Type	Size
	ca	6/9/2024 3:30 AM	Security Certificate	2 KB
	dh.pem	6/9/2024 3:32 AM	PEM File	1 KB
	ipp	6/10/2024 11:49 AM	Text Document	1 KB
	openvpn	6/10/2024 7:33 AM	Text Document	1,361 KB
	openvpn-status	6/10/2024 8:37 PM	Text Document	1 KB
	README	5/23/2024 3:08 PM	Text Document	1 KB
	server1	6/9/2024 3:31 AM	Security Certificate	5 KB
	server1.key	6/9/2024 3:31 AM	KEY File	2 KB
	Server1	6/10/2024 7:27 AM	OpenVPN Config ...	1 KB

Рис. 3.98 – Папка config-auto

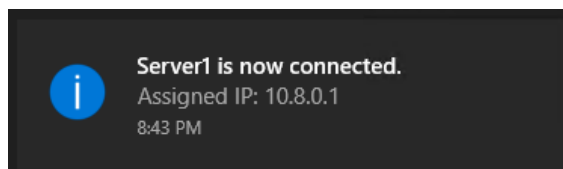


Рис. 3.99 – Успішне включення VPN-серверу

Тепер потрібно створити сертифікат і приватний ключ для клієнта. Потім створити також для нього конфігураційний файл, його налаштування показано в додатку А. Після цього відправити сертифікат, ключ і конфігураційний файл клієнту, де ці файли мають бути в папці config.

```
EasyRSA Shell
# ./easyrsa build-client-full Client nopass
No Easy-RSA 'vars' configuration file exists!

Using SSL:
* openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
Notice
-----
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: C:/Program Files/OpenVPN/easy-rsa/pki/reqs/Client.req
* key: C:/Program Files/OpenVPN/easy-rsa/pki/private/Client.key

You are about to sign the following certificate:
Request subject, to be signed as a client certificate
for '825' days:

subject=
  commonName              = Client

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes

Using configuration from C:/Program Files/OpenVPN/easy-rsa/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'Client'
Certificate is to be certified until Sep 11 02:10:58 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/issued/Client.crt

Notice
-----
Inline file created:
* C:/Program Files/OpenVPN/easy-rsa/pki/inline/Client.inline
```

Рис. 3.100 – Створення сертифікату для клієнта

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

This PC > Local Disk (C:) > Program Files > OpenVPN > config				
Name	Date modified	Type	Size	
ca	6/8/2024 4:45 AM	Security Certificate	2 KB	
Client	6/8/2024 5:11 AM	Security Certificate	5 KB	
Client.key	6/8/2024 5:10 AM	KEY File	2 KB	
Client	6/8/2024 5:16 AM	OpenVPN Config ...	1 KB	
README	5/23/2024 3:08 PM	Text Document	1 KB	

Рис. 3.101 – Папка config

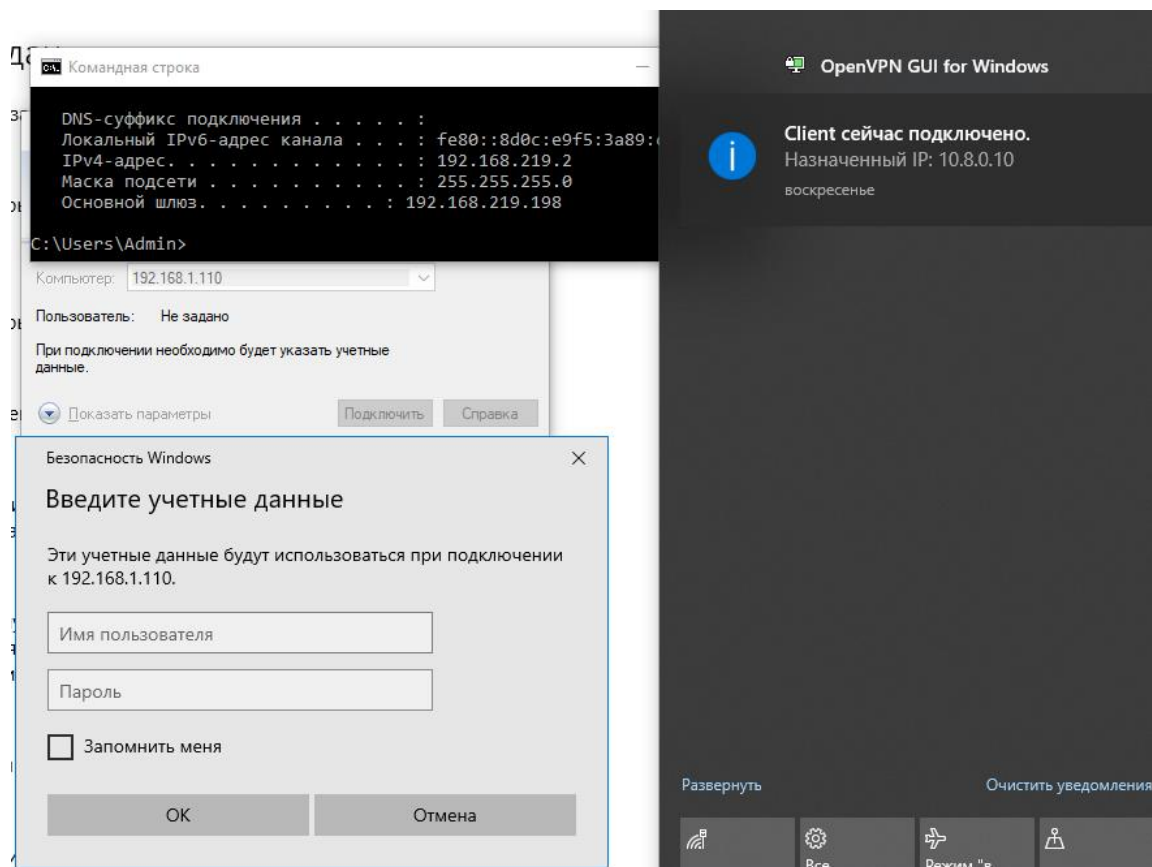


Рис. 3.102 – Успішне підключення до VPN-серверу

Висновок до третього розділу:

Протягом виконання даного розділу було зосереджено на процесах розгортання та налаштування віртуального середовища Proxmox VM на сервері. Показано розгортання Proxmox Backup серверу для віртуальних машин у Proxmox VE, щоб у випадку несправності відновити по снапшотами його попередній стан. Детально показано створення і налаштування головного та термінального сервера.

На головному сервері показано налаштування Active Directory та створення домену для корпоративної мережі. Створення груп користувачів та самих користувачів. Налаштовано доступ до папки на сервері для працівників компанії і розподілено права для груп користувачів. Налаштовано автоматичне встановлення потрібного ПЗ на робочих станціях працівників. Було показано налаштування DHCP-сервера. На термінальному сервері показано налаштування Remote Desktop Connection(Віддалене підключення до робочого стола). Налаштовано OpenVPN на сервері і клієнтах, тому адмін може підключитися до контролера ззовні корпоративної мережі через інтернет.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У ході виконання дипломної роботи, були ретельно розглянуті та вивчені теоретичні аспекти, пов'язані з серверами, віртуалізацією. Отримані знання надали змогу визначити ключові аспекти оптимального проектування інфраструктури, спрямованої на забезпечення ефективності, безпеки та високої доступності корпоративної мережі.

У першого розділу було дослідженню принцип роботи сервера і в чому заключається його ціль. Його основна ціль заключається в обміні інформації між ним і клієнтом. Існує декілька моделей серверу, наприклад сервер-клієнт або peer-to-peer, де нема централізованої бази даних і клієнти виступаю в якості серверів. Був проведений аналіз існуючих операційних систем для серверів, де були розглянуті різні дистрибутиви linux для серверів, windows server, та інші відносно популярні ОС. Було коротко описано самі ОС і для чого вони підходять. Був проведений аналіз існуючих систем віртуалізацій, так яку роль вони відіграють в роботі серверів. Вони дозволяють більш ефективно використовувати фізичне обладнання комп'ютера. Зазначено всі популярні системи віртуалізації та описано їхні особливості. Був проведений аналіз існуючих протоколів VPN, так як вони відіграють велику роль в безпеці мережі на сьогоднішній момент. Зазначено популярні VPN-протоколи і особливості їх роботи.

У другому розділі відбувалося проектування логічної і фізичної топології мережі. Розглянуто основні види фізичних і логічних топологій, де було вибрано оптимальний варіант для корпоративної мережі. Спроектовано розгортання серверу, де зазначено яка там буде віртуальне середовище і віртуальні машини в ньому, також було обрано оптимальні характеристики серверу для його роботи. Показано які будуть основні налаштування серверу, тобто його віртуальних машин, де кожна відіграє свою роль в корпоративній мережі. Був обраний оптимальний VPN-сервіс і розписано дії при його налаштуванні, щоб клієнт ззовні корпоративної мережі міг підключитися до серверу.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		91

У третьому розділі було зосереджено на процесах розгортання та налаштування віртуального середовища Proxmox VM на сервері. Показано розгортання Proxmox Backup серверу для віртуальних машин у Proxmox VE, щоб у випадку несправності відновити по снапшотами його попередній стан. Детально показано створення та налаштування головного і термінального сервера. На головному сервері показано налаштування Active Directory та створення домену для корпоративної мережі. Було показано створення груп користувачів та самих користувачів. Налаштовано доступ до папки на сервері для працівників компанії і розподілено права для груп користувачів. Налаштовано автоматичне встановлення потрібного ПЗ на робочих станціях працівників. Було показано налаштування DHCP-сервера. На термінальному сервері показано налаштування Remote Desktop Connection (Віддалене підключення до робочого стола). Налаштовано OpenVPN на сервері і клієнтах, тому адмін може підключитися до контролера ззовні корпоративної мережі через інтернет.

При роботі з цією дипломною роботою, було створено і налаштовано серверну інфраструктуру для корпоративної мережі. Було отримано цінний досвід з роботою віртуального середовища Proxmox VE, налаштуванням Active Directory на його головному та термінальному сервері, налаштування OpenVPN на стороні сервера та клієнта.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tanenbaum S. A. Computer networks (5th edition) / Tanenbaum A. S., Wetherall D. J. 2010. – 960 с.
2. 15 different types of servers in computing. Zenarmor - Agile Service Edge Security. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.zenarmor.com/docs/network-basics/types-of-servers>.
3. Server Operating System: Server OS Types & How to Choose [Електронний ресурс] – Режим доступу до ресурсу: <https://phoenixnap.com/kb/server-operating-system>.
4. Comparison of platform virtualization software [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software.
5. The best VPN protocols and different VPN types [Електронний ресурс] – Режим доступу до ресурсу: <https://nordvpn.com/ru/blog/protocols/>.
6. What is ipsec?: security policy; security services. [Електронний ресурс] – Режим доступу до ресурсу: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776369\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776369(v=ws.10)?redirectedfrom=MSDN).
7. Протокол L2TP [Електронний ресурс] – Режим доступу до ресурсу: [https://web.archive.org/web/20110604032114/http://technet.microsoft.com/ru-ru/library/cc759432\(WS.10\).aspx](https://web.archive.org/web/20110604032114/http://technet.microsoft.com/ru-ru/library/cc759432(WS.10).aspx).
8. Layer two tunneling protocol: virtual private network (VPN); remote access. [Електронний ресурс] – Режим доступу до ресурсу: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759432\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759432(v=ws.10)?redirectedfrom=MSDN).
9. PPTP [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/PPTP>.
10. What is OpenVPN Protocol. Network Access & Security Solutions. [Електронний ресурс] – Режим доступу до ресурсу:

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

https://nordlayer.com/learn/vpn/openvpn/?gclid=CjwKCAiAtt2tBhBDEiwALZuhAOINSF0zUymjqfXrj81qIFB-548ghZb47UHXzmUzhTrCLgWaPcBXYBoC4y0QAvD_BwE.

- 11.How To Guide: Set Up & Configure OpenVPN Client/server [Електронний ресурс] – Режим доступу до ресурсу: <https://openvpn.net/community-resources/how-to/#installing-openvpn>.
- 12.Secure Socket Tunneling Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol.
- 13.Install Active Directory on Windows Server 2012, 2016, and 2019 - Tutorial & Documentation. Tutorial & Documentation. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.webhi.com/how-to/install-active-directory-on-windows-server-2012-2016-and-2019/>.
- 14.Active Directory security groups. [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>.
- 15.Different Types of Network Topology [Електронний ресурс] – Режим доступу до ресурсу: <https://www.shiksha.com/online-courses/articles/different-types-of-network-topology/>.
- 16.How to Create a File Share in Windows Server. NAKIVO [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nakivo.com/blog/create-file-share-windows-server/>.
- 17.Install and configure DHCP Server on Windows Server. [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server?tabs=gui>.
- 18.Installing the RDP (Remote Desktop Protocol) on a Windows Server [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sim-networks.com/en/kb/remote-desktop-protocol-setup-to-windows>.

19. Install Proxmox VE [Электронный ресурс] – Режим доступа до ресурсу: <https://phoenixnap.com/kb/install-proxmox>.
20. Proxmox Backup Server: Install and configure [Электронный ресурс] – Режим доступа до ресурсу: <https://4sysops.com/archives/proxmox-backup-server-install-and-configure/>.
21. Use Group Policy to remotely install software - Windows Server [Электронный ресурс] – Режим доступа до ресурсу: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>.

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

ДОДАТКИ

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

Конфігураційний файл Server

```

port 1194

proto tcp

dev tun

ca ca.crt
cert server1.crt
key server1.key
dh dh.pem

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

push "route 192.168.1.0 255.255.255.0"

push "redirect-gateway def1 bypass-dhcp"

client-to-client

keepalive 10 120

cipher AES-256-CBC

persist-key
persist-tun

status openvpn-status.log

log-append openvpn.log

management 192.168.1.111 10256

verb 6

explicit-exit-notify 1

```

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційний файл Client

client

dev tun

proto tcp

remote 31.42.179.240 1194

resolv-retry infinite

bind

persist-key

persist-tun

ca ca.crt

cert client.crt

key client.key

remote-cert-tls server

cipher AES-256-CBC

verb 6

		Макаров О.В.			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		98