Міністерство освіти і науки України
Одеський національний технологічний університет
Кафедра комп'ютерної інженерії

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему *Підвищення гнучкості та масштабованості корпоративної мережі за допомогою віртуалізації*
(назва кваліфікаційної роботи згідно наказу ОНТУ)

Здобувача *Шевчук М.С.*
(прізвище, ініціали)

2 курсу *556а* групи

Керівники: *доцент Нєнов О.Л.*
(посада, прізвище та ініціали)
ст. викл. Слушна Н.В.
(посада, прізвище та ініціали)

Консультанти:
(посада, прізвище та ініціали)
д.е.н., проф. Басюркіна Н.Й.
(посада, прізвище та ініціали)

Кваліфікаційна робота допускається до захисту

Рішення кафедри від *30.11* 2023 р., протокол № *3*

Завідувач кафедри комп. інженерії _____ Сергій АРТЕМЕНКО
(назва кафедри) (підпис) (Ім'я ПРІЗВИЩЕ)

Одеса – 2023 рік

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет *Комп'ютерної інженерії, програмування та кіберзахисту*
Кафедра *Комп'ютерної інженерії*
Ступінь вищої освіти *магістр*
Спеціальність *123 «Комп'ютерна інженерія»*
Освітня програма *Мережеві технології та інтернет речей*

ЗАТВЕРДЖУЮ

Зав. кафедри *Комп'ютерної інженерії*
Сергій АРТЕМЕНКО
« *30* » листопада 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Шевчука Марка Сергійовича

1. Тема роботи *Дослідження можливостей підвищення гнучкості та масштабованості корпоративної мережі за допомогою віртуалізації*

Затверджена наказом університету від « *30* » *листопада* 2022 р., наказ № *884-03*

2 Термін здачі здобувачем закінченої роботи *28 листопада 2023 р.*

3. Вихідні дані роботи

1. Вивчити основні аспекти проектування локальних мереж та технології віртуальних мереж. 2. Розробити концепцію мережі з використанням технологій вітруальних мереж. 3. Реалізувати та налаштувати мережу в якій локальна мережа 4. Оптимізація мережі буде представлена на прикладі, який буде реалізований в VMware з використанням віртуальних машин Windows Server 2016, Windows 7. В прикладі буде. використовуватися безкоштовний VPN RadminVPN.

4. Перелік питань, які потрібно розробити

1. Вступ. 2. Аналіз мережевих технологій та протоколів 3. Проектування мережі. 4. Економічні розрахунки. 5. Охорона праці. 6. Загальні висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Слайд 1. Мета, предмет, об'єкт. Слайд 2. Структура підприємства
Слайд 3. Технічне завдання. Слайд 4.Використане програмне забезпечення.
Слайд 5. Детальна схема роботи системи. Слайд 6. Налаштування елементів мережі
Слайд 7. Основні завдання з адміністрування та підтримки роботи цієї мережі.
Слайд 8. Загальні висновки.

6. Консультанти по роботі, із зазначенням розділів роботи, що стосуються їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Економіка	*д.е.н., проф. Басюркіна Н.Й.*		
Охорона праці	*ст. викл. Слушна Н.В.*		
Нормоконтроль	*ст. викл. Жуковецька С.Л.*		

7. Дата видачі завдання *30.11.2022*

Керівники *Наталя СЛУШНА*

Олексій НЄНОВ

Завдання прийняв до виконання *Марк ШЕВЧУК*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Ознайомлення з літературою віртуалізації*	*26.12.2022*	
2.	*Визначення мети та завдань дипломної роботи.*	*30.01.2023*	
3.	*Детальний аналіз різних технологій віртуалізації*	*28.02.2023*	
4.	*Вивчення особливостей проектування мереж.*	*15.08.2023*	
5.	*Аналіз вимог користувачів та їх потреб щодо*	*27.10.2023*	
	вітруальних робочих станцій.		
6.	*Підготовка техніко-економічної частини*	*15.11.2023*	
7.	*Підготовка розділу охорони праці*	*15.11.2023*	
8.	*Оформлення розрахунково-пояснювальної записки*	*27.11.2023*	
	дипломної роботи		
9.	*Підготовка графічного матеріалу та лістингу*	*27.11.2023*	

Здобувач-дипломник _____ *Марк ШЕВЧУК*

Керівники роботи _____ *Наталя СЛУШНА*

_____ *Олексій НЄНОВ*

Несу відповідальність за ідентичність електронного та друкованого варіантів кваліфікаційної роботи, даю згоду на обробку персональних даних та не заперечую проти розміщення кваліфікаційної роботи на офіційних web-ресурсах ОНТУ.

Підтверджую, що в кваліфікаційній роботі відсутні порушення норм академічної доброчесності.

Здобувач-дипломник *Марк ШЕВЧУК* _____

АНОТАЦІЯ

Тема дипломної роботи «Дослідження можливостей підвищення гнучкості та масштабованості корпоративної мережі за допомогою віртуалізації» є дослідженням можливостей застосування віртуалізації для підвищення гнучкості та масштабованості корпоративних мереж.

У роботі розглядаються основні засади віртуалізації мереж, аналізуються переваги та недоліки використання віртуалізації у корпоративній мережній інфраструктурі.

Особлива увага приділяється можливостям масштабування мережевих ресурсів, оптимізації використання апаратних ресурсів, покращенню продуктивності та надійності мережі.

У результаті робиться висновок про те, що застосування віртуалізації може значно підвищити гнучкість і масштабованість корпоративних мереж, а також знизити витрати на їх підтримку та розвиток

Ключові слова: віртуалізація, локальні мережі, *WMware,VPN, CSP*.

ABSTRACT

Thesis topic "Investigation of the possibilities of increasing the flexibility and scalability of the corporate network with the help of virtualization" is a study of the possibilities of applying virtualization to increase the flexibility and scalability of corporate networks.

The paper examines the basic principles of network virtualization, analyzes the advantages and disadvantages of using virtualization in corporate network infrastructure.

Special attention is paid to the possibilities of scaling network resources, optimizing the use of hardware resources, and improving the productivity and reliability of the network.

As a result, it is concluded that the application of virtualization can significantly increase the flexibility and scalability of corporate networks, as well as reduce the costs of their maintenance and development.

Keywords: virtualization, local networks, WMware, VPN, CSP.

ЗМІСТ

стор.

					КРБ.КІ.1.884-03.2.11		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Марк ШЕВЧУК			Підвищення гнучкості та масштабованості корпоративної мережі за допомогою віртуалізації	Літ.	Арк. 6 / Акрушів 103
Перевірив		Наталя СЛУШНА					
Рецензент		Булюк М.В.					
Нормоконтроль		Жуковецька С.Л.					
Затвердив		Сергій АРТЕМЕНКО				гр. 561а, ОНТУ	

ВСТУП

На сьогоднішній день корпоративні мережі є невід'ємною частиною бізнес-інфраструктури будь-якої організації. Вони забезпечують зв'язок між співробітниками, клієнтами та партнерами, дозволяють передавати дані та інформацію, виконувати завдання та контролювати процеси.

Однак, у сучасному світі бізнес-процеси стають все більш складними та вимогливими до мережевих ресурсів. Це викликає необхідність постійного покращення мережевої інфраструктури, щоб забезпечити гнучкість та масштабованість бізнес-процесів.

У цій дипломній роботі буде досліджено застосування віртуалізації для підвищення гнучкості та масштабованості корпоративних мереж. Як платформа для дослідження буде використовуватися *VMware*, одна з найпопулярніших платформ віртуалізації.

Віртуалізація мереж – це одне з рішень, що дозволяє значно підвищити гнучкість та масштабованість корпоративних мереж, а також покращити їх продуктивність та надійність. Віртуалізація дозволяє об'єднати ресурси декількох серверів у єдине віртуальне середовище, де ресурси можуть бути ефективніше розподілені та керовані. Це може суттєво скоротити витрати на обладнання та експлуатацію мережі, а також забезпечити високу гнучкість та масштабованість для підтримки бізнес-процесів.

У роботі будуть розглянуті основні засади віртуалізації мереж, аналізовано переваги та недоліки використання віртуалізації у корпоративній мережній інфраструктурі. Особлива увага приділяється можливостям масштабування мережевих ресурсів, оптимізації використання апаратних ресурсів, покращенню продуктивності та надійності мережі.

Зазначимо мету, об’єкт, предмет та задачі, які необхідно вирішити в ході кваліфікаційної роботи.

Метою роботи є дослідження можливостей підвищення гнучкості та масштабованості корпоративної мережі за допомогою віртуалізації.

Об’єктом дослідження є процеси оптимізації корпоративної інформаційної мережі, використовуючи віртуальні машини.

Предметом дослідження є методи віртуалізації інформаційної мережі.

Основними задачами, які необхідно вирішити в ході роботи є:

1. Аналіз предметної області та існуючих аналогів.

2. Дослідження існуючих методів процедурної генерації.

3. Оптимізація віртуальної мережі.

4. Налаштування клієнтської частини для віртуального середовища.

Наукова новизна кваліфікаційної роботи полягає в удосконаленні існуючих локальних мереж за допомогою послуг віртуальних робочих столів.

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1 Огляд технологій віртуалізації мережі

Виртуалізація мережі – це технологія, що дозволяє створювати віртуальні мережі на базі фізичних пристроїв. Ця технологія дозволяє забезпечити гнучкість та масштабованість корпоративних мереж, а також поліпшити ефективність їх роботи. Однією з ключових технологій віртуалізації мережі є *VMware NSX*. Вона дозволяє створювати віртуальні мережі, що забезпечують ізоляцію трафіку, підвищену безпеку та швидкість передачі даних. Завдяки *NSX* можливо створювати віртуальні мережі між віддаленими фізичними пристроями, що забезпечує більш гнучкий та масштабований підхід до налаштування мережі. Ще однією технологією віртуалізації мережі є *Open vSwitch*. Ця технологія забезпечує можливість створювати віртуальні мережі на базі *OpenFlow*, що забезпечує більш гнучкий та простий підхід до конфігу-рування мережі. Додатково, до інших технологій віртуалізації мережі можна віднести *VXLAN* та *GRE* тунелювання, які дозволяють створювати віртуальні мережі на базі інтернет-протоколу.

Комутатор *Ethemet* є пристроєм канального рівня. Відповідно до логіки роботи розсилка широкомовних кадрів буде здійснюватись через усі порти (за винятком порту-приймача такого кадру). Хоча трафік з конкретними адресами (з'єднання «крапка - крапка») ізольований парою портів, широкомовні кадри передаються в всю мережу (на кожен порт).

Широкомовні кадри використовуються при роботі багатьох мережевих протоколів, таких як *ARP*, *BOOTP* або *DHCP*. Великий обсяг широко мовних кадрів у мережі призводить до нераціонального використання смуги пропускання, особливо у великих мережах. Для зниження цього ефекту обмежують область поширення широкомовного трафіку (ця область називається

широкомовним доменом); організують невеликі широкомовні домени або віртуальні локальні мережі (*Virtual LAN, VLAN*).

Віртуальною локальною мережею називається логічна група вузлів мережі, трафік якої, у тому числі й широкомовний, повністю ізольований від інших вузлів мережі на канальному рівні. Це означає, що передача кадрів між різними віртуальними мережами на підставі *MAC* адреси неможлива незалежно від типу адреси (індивідуальної, групової або широкомовної). У той же час усередині віртуальної мережі кадри передаються за технологією комутації, тобто тільки на той порт, який пов'язаний з адресою призначення кадру. Таким чином, за допомогою віртуальних мереж вирішується проблема поширення широкомовних кадрів і наслідків, що викликаються ними, які можуть призводити до широко мовних шторм і істотно знижувати продуктивність

VLAN мають такі переваги:

– гнучкість впровадження *VLAN* є ефективним способом угруповання мережевих вузлів у віртуальні робочі групи незалежно від їх фізичного розміщення у мережі;
– обмежують поширення широкомовного трафіку, що збільшує смугу пропускання, доступну для користувача;
– дозволяють підвищити безпеку мережі, визначивши за допомогою фільтрів, налаштованих на комутаторі або маршрутизаторі, політику взаємодії користувачів з різних віртуальних мереж.

Для коректної роботи віртуальної локальної мережі потрібно, щоб у базі даних фільтрації (*filtering database*) містилася інформація про членство у *VLAN*. Ця інформація необхідна для прийняття правильного рішення (переслати чи відкинути) під час передачі кадрів між портами комутатора.

Існують два способи, що дозволяють встановлювати членство в *VLAN*:

– статичні *VLAN*;
– динамічні *VLAN*.

У статичних *VLAN* встановлення членства здійснюється вручну адміністратором. При зміні топології мережі чи переміщенні користувача на

інше робоче місце адміністратору потрібно вручну Використовувати прив'язку *VLAN* до порту для кожного нового з'єднання.

Членство в динамічних *VLAN* може встановлюватися динамічно на портах комутаторів на основі протоколу *GVRP* (*GARP VLAN Registration Protocol*). Протокол *GARP* (*Generic Attribute Registration*) *Protocol*) використовується для реєстрації та скасування реєстрації атрибутів, таких як *VID*.

Статичні записи про реєстрацію в *VLAN* (*Static VLAN Registration Entries*) використовуються для представлення інформації про статично *VLAN* в базі даних фільтрації. Ці записи дозволяють задавати точні налаштування для кожного порту *VLAN*: ідентифікатор *VLAN*, тип порту (маркований або немаркований), один з елементів керування протоколу *GVRP*:

- *Fixed* (порт завжди є членом цієї *VLAN*);
- *ForЬidden* (порту заборонено реєструватися як члену даної *VLAN*);
- *Nonnal* (звичайна реєстрація за допомогою протоколу *GVRP*).

Керуючі елементи *GVRP* використовуються для активізації роботи протоколу на портах комутатора, а також для вказівки, чи може ця *VLAN* бути зареєстрована на порту.

Динамічні записи про реєстрацію в *VLAN* (*Dynamic VLAN Registration Entries*) використовуються для представлення в базі даних фільтрації інформації про порти, членство в *VLAN* яких встановлено динамічно. Ці записи створюються, оновлюються та видаляються в процесі роботи протоколу *GVRP*.

1.2 Перспективи розвитку віртуалізації мережі

Перспективи розвитку віртуалізації мережі дуже високі. Застосування технологій віртуалізації мережі дозволяє зменшити витрати на обладнання, спростити конфігурування мережі та забезпечити більш високу масштабованість та гнучкість. Крім того, віртуалізація мережі дозволяє забезпечити відокремлення різних мережевих сервісів, що зменшує ризик поширення вірусів та інших загроз безпеці мережі. Також віртуалізація мережі дозволяє забезпечити легкість масштабування та підтримки мережі, що є дуже важливим для

корпорацій з великою кількістю вузлів мережі та сервісів. У майбутньому, розвиток віртуалізації мережі може привести до створення ще більш складних та інноваційних технологій для керування мережею, що дозволить забезпечити ще більшу продуктивність та безпеку мережі.

1.3 Основні мережеві протоколи

Мережевий фільтр використовує *TCP* протокол для створення мережевого підключення між пристроями. *Transmission Control Protocol – TCP* є популярним протоколом зв'язку, використовуваним зв'язку через мережу. Він поділяє будь-яке повідомлення на серії пакетів, які відправляються від джерела до призначення, і там воно збирається на місці призначення. Якщо один пакет буде пошкоджений або не дійде, він буде постійно запитуватися у джерела поки не пройде. Інтернет-протокол – *IP* розроблений спеціально як протокол адресації. Він переважно використовується з *TCP*. *IP*-адреси в пакетах допомагають маршрутизувати їх через різні вузли в мережі, доки вони не досягнуть системи призначення. У цій роботі я відмовився від використання мережевого протоколу *UDP* принцип його роботи полягає в тому що він без переривчасто відправляє інформацію на хост не помічаючи того що частина пакетів вже втрачені.

Протокол користувальницьких дейтаграм *UDP* – це протокол зв'язку, що замінює протокол управління передачею, реалізований в першу чергу для створення зв'язку між різними програмами, що допускає втрати і малої затримки. Ці втрати можуть бути кретичними принцип роботи цього протоколу можна побачити на кабельному *TV*. Отримати доступ до мережевого фільтру можна за допомогою монітора і клавіатури або використовуючи мережевий інтерфейс. Підключиться до мережевого інтерфейсу можна за допомогою *Putty* або через браузер. Використовуючи мережевий протокол *HTTPS* можна отримати захищений видалений доступ.

Безпечний протокол передачі гіпертексту *HTTPS* – це стандартний протокол захисту зв'язку між двома комп'ютерами, один з яких використовує браузер, а інший - отримання даних з веб-сервера. *HTTP* використовується для передачі даних між клієнтським браузером (запит) та веб-сервером (відповідь) у

гіпертекстовому форматі, те саме у випадку *HTTPS*, за винятком того, що передача даних виконується в зашифрованому форматі. Таким чином можна сказати, що *https* заважає хакерам інтерпретувати або змінювати дані під час передачі пакетів.

1.4 Віртуальних мережа

Віртуальною мережею називається група вузлів мережі, трафік якої, на канальному рівні повністю ізольований від інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на підставі адреси канального рівня неможлива, незалежно від типу адреси унікальної, групової або широкомовної. У той самий час усередині віртуальної мережі кадри передаються за технологією комутації, тобто тільки той порт, який пов'язані з адресою кадру. Віртуальні мережі можуть перетинатися, якщо один або кілька комп'ютерів входять до складу більш ніж однієї віртуальної мережі (рис 1.4).

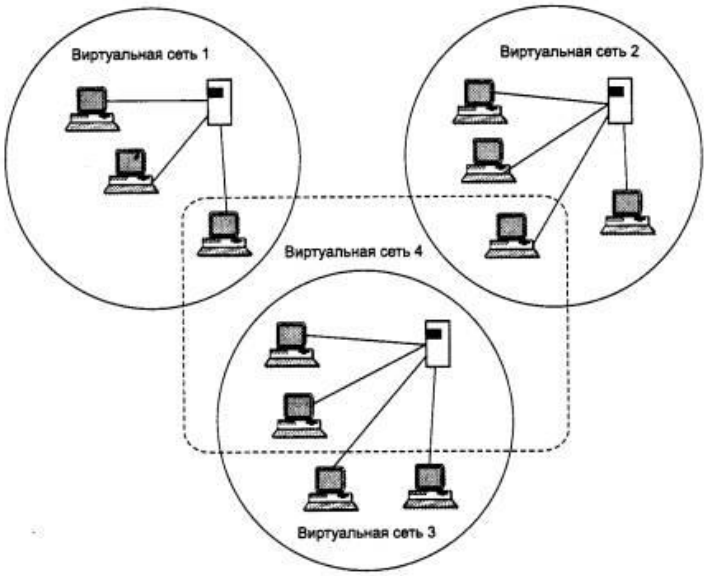

Рис. 1.4 – Віртуальна мережа

Призначення технології віртуальних мереж полягає в полегшенні процесу створення ізольованих мереж, які потім повинні зв'язуватися за допомогою маршрутизаторів, що реалізують протокол мережевого рівня, наприклад *IP*. Така побудова мережі створює набагато потужніші бар'єри на шляху помилкового

трафіку з однієї мережі до іншої. Сьогодні вважається, що будь-яка велика мережа повинна включати маршрутизатори, інакше потоки помилкових кадрів, наприклад широкомовних, періодично затоплюватимуть всю мережу через прозорі для них комутатори, приводячи її в непрацездатний стан.

Технологія віртуальних мереж створює гнучку основу для побудови великої мережі, з'єднаної маршрутизаторами, оскільки комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не вдаючись до фізичної комутації.

До появи технології *VLAN* для створення окремої мережі використовувалися або фізично ізольовані сегменти коаксіального кабелю, або незв'язані між собою сегменти, побудовані на повторювачах та мостах.

1.5 Віртуалізація мережі в організації

Віртуалізація мережі є важливою складовою сучасного IT інфраструктури в бізнесі. Вона дозволяє знизити вартість обладнання, збільшити ефективність ресурсів і забезпечити високий рівень безпеки мережі. У багатьох організаціях віртуалізація мережі використовується для розширення мережі на віддалені робочі місця, включаючи роботу з дистанційними працівниками.

Віртуалізація дозволяє забезпечити безпечний та ефективний доступ до мережі з будь-якої точки світу. Віртуалізація також дозволяє знизити витрати на обслуговування мережі та рівень відмов, що є важливим для бізнесу

Застосування віртуалізації мережі в організації може також покращити можливості моніторингу та адміністрування мережі, що дозволяє оперативно виявляти та вирішувати проблеми. Однак, важливо зазначити, що віртуалізація мережі потребує певних знань та досвіду в IT сфері. Вона може бути складною в реалізації, а також вимагати значних витрат на придбання необхідного обладнання та програмного забезпечення.

У будь якому випадку, віртуалізація мережі є важливим інструментом для забезпечення ефективного та безпечного функціонування мережі в організації.

Вона дозволяє знизити витрати на обладнання та обслуговування, забезпечити масштабованість та гнучкість мережі та покращити її безпеку.

1.6 Протокол *TCP/IP*

Конкретна реалізація набору протоколів називається протокольним стеком. Цей набір підтримують усі рівні взаємодії відкритих систем. Найбільш поширений протокольний стек *TCP/IP*.

Історія створення протоколів *TCP/IP* веде свій початок зі створення мережі *ARPANET*, для якої його було розроблено в 1970-1973 рр. Експеримент із використання *TCP/IP* у цій мережі закінчився успішно. У результаті стек *TCP/IP* було здано до промислової експлуатації. Пізніше він адаптувався для використання в ЛОМ.

На початку 1980 р. протокол став складовою ОС *Berkeley, UNIX v* 4.2. Після розпаду *ARPANET* на *Military Net* та *NSFNET* (*Internet*) у 1983 р. було прийняте рішення про його використання в мережі *Internet*. Важливою частиною технології *TCP / IP* є завдання адресації, до числа яких відносяться наведені нижче.

1. Узгоджене використання адрес різного типу. Це завдання включає відображення адрес різних типів один на одного, наприклад мережевої *IP*адреси на локальну, доменного імені на *IP* адресу тощо.

2. Забезпечення унікальності адрес. Залежно від типу адреси потрібно забезпечувати однозначність адресації в межах комп'ютера, підмережі, корпоративної мережі або Інтернету.

3. Конфігурація мережевих інтерфейсів і мережевих додатків. Стек *TCP/IP* надає користувачам дві основні служби, які використовують прикладні програми.

Дейтаграмний метод доставки пакетів. Це означає, що протоколи стеку визначають маршрут передачі повідомлення, спираючись тільки на адресну інформацію, яка міститься в цьому повідомленні. Доставка відбувається без встановлення логічного з’єднання.

В адаптерах для клієнтських комп'ютерів значна частина роботи перекладається на драйвер, тим самим адаптер виявляється простіше й дешевше. Недоліком такого підходу є високий ступінь завантаження центрального процесора комп'ютера рутинними роботами по передачі кадрів з оперативної пам'яті комп'ютера в мережу.

Центральний процесор змушений займатися цією роботою замість виконання прикладних завдань користувача. Тому адаптери, призначені для серверів, здебільшого забезпечуються власними процесорами, які самостійно виконують більшу частину роботи з передачі кадрів з оперативної пам'яті в мережу й у зворотному напрямку.

Прикладом такого адаптера може служити мережевий адаптер *SMS Ether Power* з вбудованим процесором *Intel i*960. Залежно від того, який протокол реалізує адаптер, адаптери діляться на *Ethernet*-адаптери, *Token Ring*-адаптери, *FDDI*-адаптери й т.д.

Тому що протокол *Fast Ethernet* дозволяє за рахунок процедури автопереговорів автоматично вибрати швидкість роботи мережевого адаптера залежно від можливостей концентратора, тому багато адаптерів *Ethernet* сьогодні підтримують дві швидкості роботи й мають у своїй назві приставку 10/100.

Цю властивість деякі виробники називають авточуттєвістю. Мережевий адаптер перед установкою в комп'ютер необхідно конфігурувати. При конфігуруванні адаптера задаються номер переривання *IRQ*, використовуваного адаптером, номер каналу прямого доступу до пам'яті *DMA* (якщо адаптер підтримує режим *DMA*) і базова адреса портів введення/виведення. Якщо мережний адаптер, апаратури комп'ютера й операційна система підтримують стандарт *Plug-and-Play*, то конфігурування адаптера і його драйвера здійснюється автоматично. Інакше потрібно спочатку сконфігурувати мережевий адаптер, а потім повторити параметри його конфігурації для драйвера.

У загальному випадку, деталі процедури конфігурування мережевого адаптера і його драйвера багато в чому залежать від виробника адаптера, а також від можливостей шини, для якої розроблений адаптер. й повинне бути згідно з моделлю стека протоколів *IEEE* 802.*x* Наприклад, у ОС *Windows NT* рівень *LLC* реалізується в модулі *NDIS*, загальному для всіх драйверів мережевих адаптерів, незалежно від того, яку технологію підтримує драйвер. Мережевий адаптер разом із драйвером виконують дві операції: передачу й прийом кадру.

Передача кадру з комп'ютера в кабель складається з перерахованих нижче етапів (деякі можуть бути відсутні, залежно від прийнятих методів кодування). Прийом кадру даних *LLC* через міжрівневий інтерфейс разом з адресною інформацією M*AC*-підрівень. Взаємодія між протоколами всередині комп'ютера відбувається через буфери, розташовані в оперативній пам'яті. Дані для передачі в мережу містяться в цьому буфері протоколами верхніх рівнів, які витягають їх з дискової пам'яті або з файлового кеша за допомогою підсистеми ведення/виведення операційної системи. Оформлення кадру даних M*AC*-підрівня, у який інкапсулюються кадр *LLC* (з відкинутими прапорами 01111110).

Заповнення адрес призначення й джерела, обчислення контрольної суми. Прийом із кабелю сигналів, що кодують бітовий потік. Виділення сигналів на тлі шуму. Цю операцію можуть виконувати різні спеціалізовані мікросхеми або сигнальні процесори *DSP*. У результаті в приймачі адаптера утвориться деяка бітова послідовність, яка з великим ступенем імовірності збігається з тієї, що була послана передавачем. Перевірка контрольної суми кадру.

Якщо вона неправильна, то кадр відкидається, а через міжрівневий інтерфейс наверх, протоколу *LLC* передається відповідний код помилки. Якщо контрольна сума правильна, то з *MAC*-кадру витягається кадр *LLC* і передається через міжрівневий інтерфейс наверх, протоколу *LLC*. Кадр *LLC* міститься в буфері оперативної пам'яті. Розподіл обов'язків між мережевим адаптером і його драйвером стандартами не визначається, тому кожен виробник вирішує це питання самостійно. Завичай мережеві адаптери поділяються на адаптери для клієнтських комп'ютерів і адаптери для серверів.

Надійний потоковий транспортний засіб. Більшість прикладних програм потребують від комунікаційного ПЗ автоматичного відновлення при помилках передавання, втраті пакетів або при збоях у проміжних маршрутизаторах. Надійний транспортний засіб дає змогу встановлювати логічне з'єднання між прикладними програмами, після чого відсилати великі об'єми даних через це з'єднання.

Основні переваги стеку протоколів *TCP*/*IP* Незалежність від мережевої технології. *TCP*/*IP* не залежить від обладнання, оскільки він визначає елемент передачі дейтаграму та описує спосіб її руху мережею. Загальна зв'язаність. Стек дозволяє будь-якій парі комп'ютерів, що його підтримують, взаємодіяти один з одним. Кожному комп'ютеру надається логічна адреса, а кожна дейтаграма, що передається, містить логічні адреси відправника та одержувача.

Підтвердження. Протоколи стеку *TCP*/*IP* забезпечують підтвердження правильності проходження при обміні між відправником та одержувачем. Стандартні прикладні програми. Протокол *TCP*/*IP* містить засоби підтримки основних прикладних програм, таких як, електронна пошта, передача файлів, віддалений доступ тощо. Окремі протоколи реалізовані на різних рівнях відповідно до моделі *TCP*/*IP*: на прикладному, транспортному, мережевому рівнях і рівні доступу до мережі. Протоколи *TCP*/*IP* працюють на прикладному, транспортному, мережевому рівнях. Протоколи рівня мережевого доступу забезпечують доставку *IP* пакетів із фізичного засобу підключення.

Ці протоколи нижчих мережевих рівнів розроблені організаціями зі стандартизації. Набір протоколів *TCP*/*IP* реалізований у вигляді стека *TCP*/*IP*, який працює як на відправному, так і на приймаючому вузлах для забезпечення наскрізної доставки даних по мережі. Протоколи *Ethernet* використовуються для передачі *IP*-пакетів по засобу підключення, використовуваному мережею *LAN*.

1.7 *VPN*

Щоб скласти правильне уявлення про переваги мереж *MPLS-VPN* у плані масштабування, потрібно спочатку розглянути різні моделі *VPN*, доступні на

сучасному ринку. Спочатку ми розглянемо обмеження, властиві оверлейній або накладеній моделі, а потім подивимося, які переваги по У порівнянні з нею дає однорангова модель. Сервіс-провайдер надає корпоративному замовнику технологію з'єднань між його офісами та відділеннями по приватній *WAN IP* мережі.

Для цього в кожній точці підключення потрібно встановити марш рутизатор і зв'язати його за яким-небудь *IGP* протоколом маршрутизації принаймні з центральним маршрутизатор. У цьому випадку ми говоримо, що сервіс-провайдер надає корпоративному замовнику приватну мережеву магістраль (*private network backbone*).

Якщо транспортна мережа та магістральні комутатори дійсно належать корпорації, це означає, що вона має справжню приватну мережу. Однак частіше всього транспортна мережа і принаймні частина магістральних комутаторів належать сервіс-провайдеру і спільно використовуються декількома корпоративними мережами. У цьому випадку ми говоримо, що кожна з цих корпоративних мереж є не справжньою, а віртуальною приватною мережею (*VPN*).

У мережі *VPN* з комутацією каналів маршрутизатори, які знаходяться в різних відділеннях компанії, зв'язуються між собою або за виділеними, або за комутованим лініям. У будь-якому випадку роль магістра чи найчастіше виконуватиме телефонна мережа спільного доступу. Мережі *Frame Relay* та *ATM* засновані на технології комутації каналів.

У цьому випадку маршрутизація ри, що знаходяться у відділеннях компанії-замовника, зв'язуються між собою за допомогою віртуальних каналів. Ці віртуальні канали, подібно до реальних, підтримують з'єднання типу «точка-точка». Корпоративні маршрутизатори можуть підтримувати з'єднання «точка-точка» та за допомогою засобів *IP*-тун нелірування, наприклад, *IPSec* або *GRE*.

У таких приватних або віртуальних приватних мережах завдання дизайну та функціонування магістральної топології вирішує сама корпорація або сервіс-провайдер (якщо в мережі надаються послуги з управління). Маршрутизатори,

встановлені у відділеннях корпорації, зв'язуються з сусідніми маршрутизаторами каналами «точка-точка».

Обмін даними про маршрутизацію відбувається на пряму цими каналами. З точки зору магістральної мережі сервіс провайдера, маршрутна інформація, що передається, являє собою звичайні дані, які обробляються "прозоро", тобто так само, як і всі інші.

Зі свого боку, корпоративні маршрутизатори не мають ні знань, ні засобів контролю над маршрутизуючими функціями магістралі. Цей домен відноситься до сфери, за яку відповідає сервіс-провайдер. Ми говоримо, що у цьому випадку корпоративна *IP*-мережа є оверлейною, тобто «накладається» поверх для вайдерської магістралі. При цьому корпоративну мережу можна розглядати як мережу вищого рівня, а магістраль - як мережа нижчого рівня. Обидві мережі існують незалежно одна від одної.

Такий спосіб побудови мережі вищого рівня поверх мережі нижчого рівня називається оверлейною моделлю. Щоб досягти оптимальної маршрутизації в корпоративній мережі, надбудованій поверх магістралі, корпоративна мережа повинна мати вузлову структуру (*meshed network*). Це означає, що у кожному відділенні корпорації повинен встановлюватися маршрутизатор, з'єднаний із сусідніми маршрутизаторами, що знаходяться в інших відділеннях.

Якщо корпоративна мережа буде хоча б частково відхилятися від вузлової топології (*meshed*), то виникнуть випадки, коли трафік передаватиметься від одного корпоративного маршрутизатора в магістраль провайдера, потім надходити на корпоративний магістральний (центральний) маршрутизатор, потім передаватися назад у провайдерську магістраль і лише потім надходити на кінцевий (віддалений) маршрутизатор пункт призначення.

Оскільки віддалені маршрути затори підключаються до загальної магістралі (чи магістра сервіс-провайдера), варіант, за якого трафік залишає магістраль, проходить через другий маршрутизатор і знову потрапляє в магістраль, не можна знати ефективним.

Якщо мережа має повнозв'язкову структуру (*fully meshed*), вищезазначена ситуація не зустрічається, проте виникають інші проблеми. Корпорація має платити за віртуальні канали (а провайдер має підкріплювати їх відповідними мережевими ресурсами), але при збільшенні кількості корпоративних відділень кількість каналів зростає в геометричній прогресії. Крім високої вартості проблема посилюється тим, що алгоритми *IP* маршрутизації погано масштабуються у разі нарощування кількості прямих зв'язків між маршрутизаторами. (*Peer Model*)

Для того, щоб користуватися послугами *VPN*, підприємству зовсім не потрібно проектувати та експлуатувати власну магістральну мережу. Сервіс-провайдер, який вже має магістральну мережеву інфраструктуру, цілком може взяти це завдання на себе. Однорангова модель *VPN* вимагає лише підключення маршрутизатора замовника до одного з маршрутизаторів сервіс-провайдера.

В одноранговій *VPN* два маршрутизатори *C* вважаються однорангові тільки в тому випадку, коли вони знаходяться на одному сайті. Тому той, хто належить замовнику маршрутизатор *C*1 не має однорангових (сусідських) відносин з маршрутизатором *C*2, який належить тому ж замовнику, але встановлений на іншому сайті (у іншому місці). Виходить, що на кожному сайті замовника є принаймні один корпоративний марш рутизатор (*CE*), пов'язаний одноранговими відносинами принаймні з одним маршрутизатором сервіс провайдера (*PE*).

CE маршрутизатори не обмінюються один з одним даними про маршрути. Немає взагалі ніякої необхідності в обміні будь якими даними між *CE*-маршрутами заторами. Дані передаються від вхідного *CE*-маршрутизатора через вхідний *PE*-маршрутизатор сервіс-провайдера і проходять через один або кілька магістральних *P*-маршрутизаторів. У результаті вони досягають вихідного *PE*-маршрутизатора сервіс-провайдера і попа дають на вихідний корпоративний *CE*-маршрутизатор

Таким чином, маршрутизація стає оптимальною. Оскільки *CE*-маршрутизатори не обмінюються один з одним даними про маршрути,

корпорації не потрібно мати свою магістраль чи керувати нею. Зрозуміло, корпоративний замовник може користуватися *IP*-магістраллю так, ніби в нього є мережа *Frame Relay*, і створювати свого роду «віртуальні канали» між *CE*-маршрутизаторами.

Зазвичай для цього використовується одна з форм *IP*-тунелювання. Однак це приводить нас назад до оверлейної моделі з усіма її проблемами. Однорангова модель таких проблем не має. Однорангова модель має низку переваг:

В одноранговій моделі кількість роботи, яку повинен виконати сервіс-провайдер для технічного забезпечення та управління *VPN*, прямо пропорційно до кількості сайтів замовника, підключені до *VPN*.

У оверлейній моделі кількість цієї роботи пропорційна квадрату сайтів замовника, підключених до *VPN*.

Однорангова модель підтримує оптимальну маршрутизацію користувача трафіку по магістралі сервіс-провайдера, оскільки в цій моделі немає потреби в транзитних *CE*-пристроях.

Корпоративному замовнику не потрібно керувати своєю магістраллю. Йому потрібно лише підключити *CE*-маршрутизатор на кожному сайті. Таким чином, однорангова модель вигідна і сервіс-провайдеру, і замовнику.

Для провайдера вона означає скорочення обсягу робіт, а для корпоративного замовника цінніші послуги. Хоча однорангова модель має безліч переваг у порівнянні з оверлейною, на шляху її реалізації також стоїть ряд проблем. Перевантаження P-маршрутизаторів інформацією про маршрути.

Однією з основних проблем великих *IP*-магістралей є велика кількість ресурсів (пам'яті, процесорних потужностей, смуги пропускання), необхідних для зберігання даних про маршрутизації.

Якщо взяти *IP*-магістраль та пустити по ній дані про маршрути всіх корпоративних мереж, *P*-маршрутизатори ніколи з нею не впораються. Неузгоджені (несуміжні) адресні простори. Зазвичай Інтернет-сервіс-провайдери (*ISP*) намагаються надавати адреси осмислено. Це означає, що адреса

системи повинна вказувати на місце, в якому ця система підключається до мережі *ISP*.

Однак багато корпоративних мереж мають адресні схеми, які важко поєднати з магістральною топологією будь-якого сервіс-провайдера. У цих схемах адреси сайтів розподіляються без будь-якого обліку точки, в якій здійснюється підключення до провайдерської мережі. Це скорочує можливості агрегації маршрутів та збільшує обсяг даних про маршрути, що передаються по *P*-мережі.

Приватна адресація у *C*-мережах. Адреси в багатьох корпоративних мережах не є унікальними. Це означає, що та чи інша адреса є унікальною тільки в межах одного підприємства, але втрачає унікальність у зв'язку між підприємствами.

Якщо *IP*-магістраль сервіс-провайдера використовується як загальна магістраль для двох різних корпоративних мереж і якщо адреси в цих мережах не є унікальними, *P*-маршрутизатори не зможуть гарантувати доставку пакетів за місцем призначення.

Підслуховування. Для захисту даних потрібно встановлювати шифровані тунелі «точка-точка» між кожною парою *CE*-маршрутизаторів (модель *IPSec*). Це рішення добре підходить для оверлейної моделі, оскільки вона і без того використовує тунель «крапка-крапка» між парами «сусідніх» *CE*-маршрутизатори.

Для однорангової моделі це рішення підходить не так добре, тому що тут *CE*-маршрутизатор ніколи не може визначити, куди він буде передавати наступний пакет

1.8 Мережеві адаптери

Функції й характеристики мережевих адаптерів.

Мережевий адаптер (*Network Interface Card*, *NIC*) разом зі своїм драйвером реалізує другий, канальний рівень моделі відкритих систем у кінцевому вузлі мережі – комп'ютері. Більш точно в мережній операційній системі пара адаптер

і драйвер виконує тільки функції фізичного й *MAC*підрівня, у той час як *LLC*-рівень зазвичай реалізується модулем операційної системи, єдиним для всіх драйверів і мережевих адаптерів.

Властиво так воно маршрутизатори розсилають повідомлення один одному про зміни в мережі. Після отримання цих повідомлень маршрутизатори роблять повторне призначення оптимальних маршрутів, що може викликати новий потік повідомлень. Цей процес повинен швидко завершуватись, інакше у мережевий топології можуть з'явитися петлі, чи мережа загалом перестане функціонувати.

Алгоритми маршрутизації повинні швидко враховувати зміни у стані мережі (наприклад, відмова вузла чи сегмента мережі, додавання нового обладнання тощо).

Алгоритми маршрутизації можуть бути:

- статичними чи динамічними;
- одномаршрутними чи багатомаршрутними;
- однорівневими чи багаторівневими;
- внутрішніми чи міждоменними;
- одноадресними чи груповими.

Для статичних (неадаптивних) алгоритмів маршрути вибираються заздалегідь і заносяться вручну в таблицю маршрутизації, де зберігається інформація про те, на який порт відправити пакет з певною адресою.

Протоколи, розроблені з урахуванням статичних алгоритмів, називають немаршрутизованими. Прикладом немаршрутизованих протоколів можуть бути *LAT* (*LocalAreaTransport*, транспортний протокол для канальних областей) фірми *DEC*, протокол підключення термінала та *NetBIOS*. Зазвичай разом із цими протоколами працюють мости. З використанням динамічних алгоритмів таблиця маршрутизації автоматично оновлюється відповідно до топології мережі або трафіка в ній.

Динамічні алгоритми відрізняються за способом отримання інформації про стан мережі, за часом зміни маршрутів і іншими показниками оцінки маршруту.

Одномаршрутні протоколи визначають лише один маршрут. Він завжди виявляється оптимальним. Багатомаршрутні алгоритми пропонують кілька маршрутів до одержувача.

Такі алгоритми дозволяють передавати інформацію по кількох каналах одночасно, що означає підвищення пропускної здатності мережі проектувався як протокол передачі пакетів у складених мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол *IP* добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і ефективно використовуючи пропускну спроможність низько швидкісних ліній зв'язку.

Протокол *IP* є дейтаграмним протоколом. До рівня міжмережевої взаємодії відносяться і всі протоколи, пов'язані зі складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації *RIP* (*Routing Internet Protocol*) і *OSPF* (*Open Shortest Path First*)а також протокол міжмережевих керівників повідомлень *ICMP* (*Internet Control Message Protocol*). Останній протокол призначений для обміну інформацією про помилки між маршрутизатором і шлюзом, системою-джерелом і системою-приймачем, тобто для організації зворотного зв'язку.

За допомогою спеціальних пакетів *ICMP* повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості збірки пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилки і типу обслуговування, про стан системи і т. ін.

Наступний рівень (рівень *II*) називається транспортним. На цьому рівні функціонують протокол управління передачею *TCP* (*Transmission Control Protocol*) і протокол дейтаграм користувача *UDP* (*User Datagram Protocol*). Протокол *TCP* забезпечує стійке віртуальне з'єднання між видаленими прикладними процесами.

Протокол *UDP* забезпечує передачу прикладних пакетів дейтаграмним методом, тобто без встановлення віртуального з'єднання, і тому вимагає менших накладних витрат, ніж *TCP*.

Він забезпечує з'єднання між двома хостами, при якому не гарантується доставка пакетів. Верхній рівень (рівень *I*) називається прикладним.

За довгі роки використання в мережах різних країн і організацій стек *TCP/IP* накопичив велику кількість протоколів і сервісів прикладного рівня. До них відносяться такі широко використовувані протоколи, як протокол копіювання файлів *FTP*, протокол емуляції терміналу *telnet*, поштовий протокол *SMTP*,використовуваний в електронній пошті мережі *Internet* і її російської гілки РЕЛКОМ, гіпертекстові сервіси доступу до видаленої інформації, такі як *WWW* і багато інших.

Проблема управління поділяється на два завдання. Перше завдання пов'язане з передачею інформації. Протоколи передачі інформації, що управляє, визначають процедуру взаємодії сервера з програмою-клієнтом, що працює на хості адміністратора. Вони визначають формати повідомлень, якими обмінюються клієнти і сервери, а також формати імен і адрес. Друге завдання пов'язане з контрольованими даними. Стандарти регламентують, які дані повинні зберігатися й накопичуватися у шлюзах, імена цих даних і синтаксис цих імен.

У стандарті *SNMP* визначена специфікація інформаційної бази даних управління мережею. Ця специфікація, відома як база даних *MIB* (*Management Information Base*), визначає ті елементи даних, які хост або шлюз повинен зберігати, і допустимі операції над ними. Протокол пересилки файлів *FTP* (*File Transfer Protocol*) реалізує віддалений доступ до файлу.

Для того, щоб забезпечити надійну передачу, *FTP* використовує як транспорт протокол із встановленням з'єднань *TCP*. Крім пересилки файлів, протокол *FTP* пропонує й інші послуги.

Так користувачу надається можливість інтерактивної роботи з віддаленою машиною, наприклад, він може роздрукувати вміст її каталогів, *FTP* дозволяє користувачу вказувати тип і формат даних, що запам'ятовуються. Нарешті, *FTP* виконує аутентифікацію користувачів. Перш ніж дістати доступ до файла, відповідно до протоколу користувачі повинні повідомити своє ім'я і пароль.

У стеку *TCP/IP* протокол *FTP* пропонує найбільш широкий набір послуг для роботи з файлами, проте він є і найскладнішим для програмування. Застосування, яким не потрібні всі можливості *FTP*, можуть використовувати інший, більш економічний протокол простий протокол пересилки файлів

Визначення маршруту передачі відбувається програмно. Відповідні програмні ресурси носять назви протоколів маршрутизації. Логіка їхньої роботи полягає в алгоритмі маршрутизації, який обчислює вартість доставки й обирають шлях із меншою вартістю. Найпростіші алгоритми маршрутизації визначають маршрут, зважаючи на найменшу кількість проміжних (транзитних) вузлів шляху до адресата. Більш складні алгоритми в поняття «вартість» закладають кілька показників, наприклад, затримку під час передачі пакетів, пропускну спроможність каналів зв'язку і т. ін.

Основним результатом роботи алгоритму маршрутизації є створення умов та підтримка таблиці маршрутизації, у якій записується вся маршрутна інформація. Зміст таблиці маршрутизації залежить від використовуваного протоколу маршрутизації.

Наприклад, таблиця маршрутизації може містити таку інформацію:

- справжні адреси пристроїв у мережі;
- службову інформацію протоколу маршрутизації;
- адреси найближчих маршрутизаторів.

Основними вимогами, що висуваються до алгоритму маршрутизації є:

- оптимальність вибору маршруту;
- простота реалізації;
- стійкість;
- швидка відповідність;
- гнучкість реалізації.

Оптимальність вибору маршруту є основним параметром алгоритму.

Алгоритми маршрутизації мають бути простими в реалізації й використовувати якнайменше ресурсів. Алгоритми мають бути стійкими до

відмов устаткування, високих навантажень і помилок у фізичному середовищі мережі.

Збіжність – це процес узгодження між маршрутизаторами інформації про топології мережі. Якщо певні події мережі призводять до того, що деякі маршрути стають недоступними чи з'являються нові маршрути,

Маршрутизатор базової мережі складається з таких основних компонентів:

- мережеві адаптери, які з'єднують маршрутизатор через відповідні інтерфейси з локальними і глобальними мережами;
- управляючий процесор, який визначає маршрут і оновлює інформацію про топології;
- основна магістраль, яка після вступу пакета на інтерфейсний модуль аналізує адресу призначення та приймає команди управляючого процесора для визначення вихідного порту.

Потім пакет по основний магістралі маршрутизатора передається в інтерфейсний модуль, який слугує для зв'язку із сегментом локальної чи глобальної мережі, на який пакет було адресовано. У ролі маршрутизатора може виступати також робоча станція чи сервер, що мають кілька мережевих інтерфейсів і забезпечені спеціальним програмним забезпеченням.

Маршрутизатори верхнього класу – це, зазвичай, спеціалізовані пристрої, які об'єднують в окремому корпусі безліч маршрутизуючих модулів. За визначенням, основне призначення маршрутизаторів – це маршрутизація трафіку мережі.

1.9 Типи комп'ютерних мереж

Єдиною системи, якої задовольняють всі комп'ютерні мережі не існує. Для систематизації виділяють своєрідні властивості, які дають можливість поділити мережі на окремі типи.

В якості ідентифікаційних причин відрізняються належні характеристики:

- спосіб організації мережі;
- область обслуговування мережі;

– тип використовуваних мережевих пристроїв;
– тип середовища передачі даних, який використовується для підключення пристроїв.
– спосіб зберігання даних;
– спосіб управління ресурсами.

Розмір комп'ютерних мереж є найважливішим класифікаційним параметром оскільки визначає застосовувані мережеві технології. Існує кілька способів об'єднання мережевих пристроїв.

Пристрої можуть передавати дані на невеликі відстані за допомогою персональної мережі (*PAN*). *PAN* ідентифікує ці гаджети як телефони, планшети, принтери, миші та клавіатури. Найпопулярнішою технологією підключення вважається *Bluetooth*.

PAN також може бути розроблений з використанням інших технологій, які забезпечують обмін даними на короткій відстані, наприклад *RFID* (радіочастотна ідентифікація), яка використовує радіохвилі для зчитування даних, що містяться в транспондерах, або тегах *RFID* для автоматичної ідентифікації предметів.

Локальна мережа, часто відома як локальна мережа або *LAN*, є різновидом комп'ютерної мережі, яка зазвичай охоплює лише обмежений регіон і знаходиться в одній або кількох будівлях. У цьому випадку слово «локальний» натякає на спільне локальне керування, а не обов'язково фізичну близькість між комп'ютерами. Прикладами локальних мереж є домашні мережі, комп'ютерні мережі невеликих офісів і великі корпоративні комп'ютерні мережі. В *LAN* широко застосовуються провідні з'єднання, основна маса з яких виробляється з підтримкою мідних проводів, а деякі - оптоволоконних. Як правило, провідні мережі працюють на швидкостях від 100 Мбіт / с до 1 Гбіт / с.

Більш сучасні *LAN* можуть рабоать зі швидкістю 10 Гбіт / с. Найбільш поширеним стандартом проводового з'єднання вважається стандарт *IEEE* 802.3, як правило іменований *Ethernet*.

У локальних мережах в одному ряду з провідними технологіями широко застосовуються бездротові з'єднання за стандартом *IEEE* 802.11, більше

знайомим як *Wi-Fi*. Бездротові мережі *Wi-Fi* працюють на швидкостях від декількох до 100 мегабіт в секунду.

Міські мережі (іноді відомі як *MAN*) з'єднують комп'ютери в міських районах. Розглянемо як приклад систему кабельного телебачення. Завдяки певним модифікаціям з'явився потенціал цифрової передачі даних, і система з часом перетворилася на державну комп'ютерну мережу.

Глобальні мережі (*WAN*) з'єднують локальні мережі, які можуть бути поширені на великі географічні відстані та охоплювати значні регіони. Велику дротову локальну комп'ютерну мережу можна порівняти з *WAN*, проте є важливі відмінності:

Управління локальними мережами та передача доступу до міжмережевих середовищі передачі даних здійснюється різними організаціями.

Можуть з'єднувати мережі, що використовують всілякі види мережевих технологій.

1.10 Види топологій

Топологія локальної мережі описує, як комп'ютери фізично з'єднані один з одним. Лінії зв'язку з'єднують кожен пристрій у локальній мережі. Фізична топологія - це розташування ліній зв'язку по відношенню до вузлів мережі та фактичні фізичні з'єднання між вузлами і мережею. Залежно від цього мережі поділяються на шинні, кільцеві, зірчасті, ієрархічні та з довільною структурою.

Мережева топологія може бути:

- фізична яка описує реальне місце розташування і зв'язку між вузлами мережі;
- логічна яка описує ходіння сигналу в рамках фізичної топології;
- інформаційна яка визначає напрям потоків інформації, що передаються по мережі;
- управління обміном принцип передачі права на користування мережею.

Необхідно враховувати фізичний (фізичний рівень) і канал (рівень каналу даних) еталонної моделі *ISO/OSI*, щоб визначити відмінності між логічною та нижчою фізичною топологіями мережі. Водночас важливо пам'ятати, що канальний рівень поділяється на два окремих підрівні: управління доступом до середовища (*MAC*) і управління логічним з'єднанням (*LLC*). Топологія мережі встановлюється на фізичному та канальному рівнях, і в залежності від цих рівнів вона може бути фізичною або логічною.

Логічна – відображає логічну організацію мережі. Цей план визначає, як елементи мережі спілкуються один з одним, як дані надсилаються через мережу та яким маршрутом вони проходять.

Фізичні – де розташовані роз'єми мережевого кріплення. Він описує внутрішні електричні з'єднання компонентів мережі або схеми підключення. визначає реакцію мережі у випадку збою будь-якого вузла.

Є велика кількість видів топології, серед яких можна відзначити три основні:

– «шина» (*bus*);
– «зірка» (*star*);
– «кільце» (*ring*).

Топологія зазвичай застосовується до локальних мереж, де легко простежити структуру з'єднань. Оскільки кожен сеанс зв'язку може проходити різними маршрутами, побудова з'єднань у масових мережах, як правило, прихована від користувачів і не є особливо значущою.

Наприклад, топологія визначає запити до обладнання, тип застосовуваного кабелю, допустимі і найбільш зручні методи керування обміном, надійність, можливості розширення мережі.

У великих мережах з довільними зв'язками між комп'ютерами краще використовувати змішану топологію. Такі мережі відомі як мережі зі змішаною топологією, оскільки вони можуть розрізняти окремі вільно з'єднані частини (підмережі) зі звичайною топологією.

Топологія «Зірка» – кожен комп'ютер підключається до окремого порту пристрою, який називається комутатором, за допомогою окремого кабелю (найчастіше це вита пара категорії 5) як основної структури комп'ютерної мережі. При пошуку пошкоджень кабелів, мережевих адаптерів або роз'ємів така топологія мережі є найбільш практичною.

Недоліки:

1. Топологія "зірка" дорожча за інші топології, оскільки вимагає набагато більше дроту.
2. У разі виходу з ладу центрального сервера така локальна мережа стає абсолютно непрацездатною.

Переваги:

1. Архітектура локальної мережі "зірка" відрізняється від інших повною відсутністю конфліктів в локальній мережі, що стає можливим завдяки централізованому адмініструванню.
2. Групування точок підключення в межах обмеженої території полегшує моніторинг мережі та підвищує безпеку, запобігаючи несанкціонованому доступу.
3. Мережеве обладнання можна спростити, маючи лише двох абонентів головного та периферійного.
4. Відмова одного з вузлів або пошкодження кабелю не вплине на роботу мережі в цілому.
5. Архітектура шини "зірка" також більш практична для додавання додаткових пристроїв, ніж стандартна конструкція шини. Можна також розглянути той факт, що мережі 100 Мб і 1 Гб будуються з використанням архітектури "зірка".

Оскільки в топології "кільце" кожен комп'ютер з'єднується лише двома лініями зв'язку, він може отримувати інформацію лише від одного і надсилати її іншому комп'ютеру. Кожне з'єднання, як зірка, може вмістити лише один передавач і один приймач. Після цього вже не можна використовувати зовнішні термінатори. Загасання сигналу по всьому кільцю не має сенсу, оскільки кожен

комп'ютер діє як ретранслятор, ретранслюючи (відновлюючи) сигнал, враховується тільки загасання між сусідніми комп'ютерами. У цьому випадку всі комп'ютери можуть бути однаковими, оскільки немає окремого концентратора.

Для обслуговування або спостереження за обміном часто виділяється певний абонент, який обслуговує кільце. Зрозуміло, що наявність такого контрольного абонента знижує надійність мережі, оскільки його відмова миттєво паралізує весь обмін.

Плюси:

1. Швидке створення і налаштування даної топології локальних мереж.
2. Проста масштабованість, але вимагає відключення мережі на час налаштування нового вузла.
3. Потенціал для зростання мережі до величезних розмірів в результаті ретрансляції сигналу між комп'ютерами.
4. Велика кількість можливих абонентів.
5. Стабільність до перевантажень і відсутність мережевих конфліктів.

Мінуси**:**

1. Складне налаштування;
2. Кожна робоча станція повинна брати активну участь у потоці інформації; якщо будь-яка з них виходить з ладу або обривається кабель, мережа в цілому стає непрацездатною.
3. Виявити несправності складно. Встановлення нового комп'ютера вимагає тимчасового вимкнення мережі, оскільки кільце має бути відкритим.
4. Хоча додавання нових абонентів до «кільця» зазвичай відбувається безболісно, це вимагає тимчасової зупинки всіх мережевих дій на час встановлення з’єднання. Максимальна кількість абонентів у кільці може бути відносно високою (1000 або більше), подібно до топології «шина».

Архітектура «шини» передбачає підключення всіх робочих станцій до одного кабелю, який часто називають шиною або магістралью. Для підключення

будь-якого комп'ютера до коаксіального кабелю використовується Т-роз'єм (*T-connector*). Щоб уникнути відбиття сигналу, на кінцях кабелю є термінатори. При такій формі підключення всі робочі станції підключаються до однієї коаксіальної лінії, а дані передаються в напівдуплексному режимі обміну від одного абонента до іншого. Цей тип топології локальної мережі передбачає спеціальний термінатор на кожному кінці шини; інакше сигнал буде спотворено. Сигнали, які використовуються для придушення сигналів, які перетинають кінець каналу передачі даних, не відображаються терміналом.

Переваги:

1. Витрата кабелю істотно зменшений.
2. Відмова вузла не впливає на інші вузли.
3. Пропускна здатність мережі може бути легко розширена навіть під час її роботи.
4. Всі комп'ютери рівноправні.

Недоліки**:**

1. Складне управління та виявлення несправностей через паралельне підключення адаптерів.
2. Недостатня надійність мережі через проблеми з кабельними з'єднаннями.
3. Низька продуктивність, оскільки всі абоненти використовують один канал.

Ці топології локальних мереж використовуються для невеликої кількості комп'ютерів через малу довжину лінії зв'язку.

1.11 Загрози у мережі Інтернет

На сьогоднішній день відомі такі види мережевих атак:

1. *Mailbombing* – простий і невигадливий спосіб кібератаки, суть якого полягає у порушенні нормальної роботи електронної пошти адресата шляхом закидання його поштової адреси повідомленнями великого об'єму або у великих кількостях.

2. *IP*-спуфінг – вид хакерської атаки, що полягає у використанні чужої *IP*-адреси джерела з метою обману системи безпеки. Метод, який використовується в деяких атаках. Полягає у зміні поля "адреса відправника" *IP*-пакета.
3. *DDOS*-атака – хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, за яких сумлінні користувачі системи не зможуть отримати доступ до системних ресурсів, що надаються, або цей доступ буде утруднений.
4. *Man-in-the-Middle* – вид атаки у криптографії та комп'ютерній безпеці, коли зловмисник таємно ретранслює та за необхідності змінює зв'язок між двома сторонами, які вважають, що вони безпосередньо спілкуються один з одним.
5. *XSS*-атака – тип атаки на веб-системи, що полягає у впровадженні сторінку шкідливого коду, що видається веб-системою, і взаємодії цього коду з веб-сервером зловмисника.

Найбільш поширені види мережевих атак:

1. Підслуховування (*sniffing*). Здебільшого дані по комп'ютерних мережах передаються в незахищеному форматі (відкритим текстом), що дозволяє зловмиснику, який отримав доступ до ліній передачі даних у мережі, підслуховувати або зчитувати трафік. Для підслуховування у комп'ютерних мережах використовують сніффер. Сніффер пакетів є прикладною програмою, яка перехоплює всі мережеві пакети, що передаються через певний домен.
2. Перехоплення пароля (*password sniffing*), що передається через мережу в незашифрованій формі, шляхом «підслуховування» каналу є різновидом атаки підслуховування. Перехоплення імен і паролів створює велику небезпеку, оскільки користувачі часто застосовують один і той же логін і пароль для багатьох програм і систем.
3. Зміна даних. Дані пакета можуть бути змінені, навіть якщо зловмисник нічого не знає ні про відправника, ні про одержувача.

4. Аналіз мережного трафіку. Метою атак подібного типу є прослуховування каналів зв'язку та аналіз даних і службової інформації (наприклад, паролів користувачів або номерів кредитних карток, що передаються у відкритому вигляді). Атакам даного типу схильні такі протоколи, як *FTP* або *Telnet*, особливістю яких є те, що ім'я та пароль користувача передаються в рамках цих протоколів у відкритому вигляді.
5. Підміна довіреного суб'єкта. Більшість мереж та операційних систем використовує *IP*-адресу комп'ютера для того, щоб визначати, чи це адресат, який потрібен. В деяких випадках можливе некоректне присвоєння *IP*-адреси (заміна *IP*-адреси відправника іншою адресою) – такий спосіб атаки називають фальсифікацією адреси (*IP-spoofing*).

Атака типу «посередництво» має на увазі активне підслуховування, перехоплення і керування переданими даними невидимим проміжним вузлом. Коли комп'ютери взаємодіють на низьких мережевих рівнях, вони завжди можуть визначити, з ким саме вони обмінюються даними.

Посередництво обміну незашифрованими ключами (атака *Man-in-the-Middle*). Для проведення атаки *Man-in-the-Middle* (людина в середині) зловмиснику потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера *ISP* в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніфери (прослуховування) пакетів, транспортні протоколи та протоколи маршрутизації.

В більш загальному випадку атаки *Man-in-the-Middle* проводяться з метою крадіжки інформації, перехоплення поточної сесії та отримання доступу до приватних мережевих ресурсів, для аналізу трафіку та отримання інформації про мережу та її користувачів, для проведення атак типу *DoS*, спотворення даних, що передаються та введення несанкціонованої інформації у мережеві сесії. Ефективно боротися з атаками типу *Man-in-the-Middle* можна лише за

допомогою криптографії. Для протидії атакам цього використовується інфраструктура управління відкритими ключами *PKI* (*Public Key Infrastructure*).

Перехоплення сеансу (*Session hijacking*). Після закінчення початкової процедури аутентифікації з'єднання, встановлене законним користувачем, наприклад, з поштовим сервером, перемикається зловмисником на новий хост, а вихідному серверу видається команда розірвати з'єднання. У результаті «співрозмовник» законного користувача виявляється непомітно підміненим.

Після отримання доступу до мережі у атакуючого зловмисника з'являються великі можливості: він може надсилати некоректні дані додаткам і мережевим службам, що призводить до їх аварійного завершення або неправильного функціонування; системи у зв'язку з перевантаженням; нарешті, атакуючий може блокувати трафік, що призведе до втрати доступу авторизованих користувачів до мережевих ресурсів.

Відмова в обслуговуванні (*Denial of Service, DoS*). Ця атака відрізняється від інших типів. Вона не націлена на отримання доступу до вашої мережі або вилучення з цієї мережі будь-якої інформації.

Атака *DoS* робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. Ця атака позбавляє звичайних користувачів доступу до ресурсів або комп'ютерів мережі організації.

Більшість атак *DoS* спирається на загальні слабкості системної архітектури. У разі використання деяких серверних програм (таких як *Web*-сервер або *FTP*-сервер) атаки *DoS* можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих програм, і тримати їх у зайнятому стані, не допускаючи обслуговування звичайних користувачів.

Під час атак *DoS* можуть використовуватися звичайні інтернет-протоколи, такі як *TCP* та *ICMP* (*Internet*: *Control Message Protocol*). Атаки *DoS* важко запобігти, тому що для цього потрібна координація дій із провайдером.

Якщо трафік, призначений для переповнення вашої мережі, не зупинити у провайдера, то на вході в мережу ви цього зробити вже не зможете, тому що вся

смуга пропускання буде зайнята. Якщо атака цього типу проводиться одночасно через безліч пристроїв, ми говоримо про розподілену атаку відмови в обслуговуванні *DDoS* (*distributed DoS*). Простота реалізації атак *DoS* і величезну шкоду, яку вони завдають організаціям і користувачам, привертають цим атакам пильну увагу адміністраторів мережевої безпеки.

Парольні атаки.

Метою цих атак є заволодіння паролем та логіном законного користувача. Зловмисники можуть проводити парольні атаки, використовуючи такі методи, як:

– підміна *IP*-адреси (*I*P-спуфінг);
– підслуховування (сніффінг);
– простий перебір.

Ці методи дозволяють заволодіти паролем і логіном користувача, якщо вони передаються відкритим текстом незахищеним каналом. Часто хакери намагаються підібрати пароль та логін, використовуючи для цього численні спроби доступу. Такий підхід називається атака повного перебору (*brute force attack*).

Для цієї атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, сервера). Якщо в результаті зловмиснику вдається підібрати пароль, він отримує доступ до ресурсів на правах звичайного користувача. Якщо цей користувач має значні привілеї доступу, зловмисник може створити для себе прохід для майбутнього доступу, який діятиме, навіть якщо користувач змінить свій пароль і логін. Засоби перехоплення, підбору та злому паролів нині вважаються практично легальними та офіційно випускаються досить великою кількістю компаній. Вони позиціонуються як програми для аудиту безпеки та відновлення забутих паролів, і їх можна на законних підставах придбати у розробників.

Парольних атак можна уникнути, якщо не скористатися паролями в текстовій формі. Використання одноразових паролів та криптографічної аутентифікації можуть практично звести нанівець загрозу таких атак. На жаль,

не всі програми, хости та пристрої підтримую зазначені методи автентифікації. При використанні звичайних паролів необхідно вигадати такий пароль, який було б важко підібрати. Мінімальна довжина пароля повинна бути не менше восьми символів. Пароль повинен містити символи верхнього регістру, цифри та спеціальні символи (#, $, &, % тощо).

Вгадування ключа.

Криптографічний ключ є кодом або числом, необхідним для розшифровування захищеної інформації. Хоча дізнатися ключ доступу важко і потрібні великі витрати ресурсів, проте це можливо. Зокрема, визначення значення ключа може бути використана спеціальна програма, що реалізує метод повного перебору. Ключ, до якого отримує доступ атакуючий, називається скомпрометованим. Атакуючий використовує скомпрометований ключ для отримання доступу до захищених даних без відома відправника і одержувача. Ключ дає можливість розшифровувати та змінювати дані.

Атаки на рівні додатків. Ці атаки можуть проводитись декількома способами. Найпоширеніший їх полягає у використанні відомих слабкостей серверного програмного забезпечення (*FTP*, *HTTP*, *Web*-сервера). Головна проблема з атаками на рівні додатків полягає в тому, що вони часто користуються портами, яким можна проходити через міжмережевий екран. Відомості про атаки на рівні додатків широко публікуються, щоб дати можливість адміністраторам виправити проблему за допомогою корекційних модулем (патчів).

На жаль, багато хакерів також мають доступ до цих відомостей, що дозволяє пм вчитися. Неможливо повністю виключити атаки на рівні додатків. Хакери постійно відкривають і публікують на своїх сайтах в Інтернеті всі нові вразливі місця прикладних програм, тут важливо здійснювати хороше системне адміністрування, щоб знизити вразливість від такого типу, можна вжити наступних заходів: за допомогою спеціальних аналітичних додатків відстежувати дані *CERT* про слабкі місця прикладних програм користуватися найсвіжішими версіями операційних систем та додатків та останніми

корекційними модулями (патчами) використовувати системи розпізнавання атак *IDS* (*Intrusion Detection Systems*).

Розвідка мережі – це збір інформації про мережу за допомогою загальнодоступних даних та програм. При підготовці атаки проти будь-якої мережі хакер, як правило, намагається отримати про неї якомога більше інформації. Запити *DNS* допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену надано. Ехо-тестування адрес, розкритих за допомогою *DNS*, дозволяє побачити, які хости реально працюють у цьому середовищі.

Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, що підтримуються цими хостами. В результаті видобувається інформація, яку можна використовувати для злому.

Повністю позбутися мережевої розвідки неможливо. Якщо, наприклад, відключити відлуння *ICMP* і відлуння на периферійних маршрутизаторах, ви позбавитеся від ехо-тестування, але втратите дані, необхідні діагностики мережевих збоїв. Крім того, сканувати порти можна і без попереднього ехо-тестування. Просто це займе більше часу, тому що сканувати доведеться і неіснуючі *IP*-адреси.

Системи *IDS* на рівні мережі і хостів зазвичай добре справляються із завданням повідомлення адміністратора про мережну розвідку, що ведеться, що дозволяє краще підготуватися до майбутньої атаки і оповістити провайдера (*ISP*), в мережі якого встановлена система, що виявляє надмірну цікавість.

Зловживання довірою.

Цей тип дій не є атакою в повному розумінні цього слова. Він є зловмисне використання відносин довіри, що існують в мережі. Типовим прикладом такого зловживання є ситуація у периферійній частині корпоративної мережі. У цьому сегменті зазвичай розміщуються сервери *DNS*, *SMTP* та *HTTP*.

Оскільки всі вони належать до того самого сегменту, злом одного з них призводить до злому і всіх інших, оскільки ці сервери довіряють іншим системам своєї мережі. Ризик зловживання довірою можна знизити за рахунок

жорсткішого контролю рівнів довіри в межах своєї мережі. Системи, розташовані із зовнішнього боку міжмережевого екрану, ніколи не повинні користуватися абсолютною довірою з боку систем, захищених міжмережевим екраном.

Шкідливі програми.

До таких програм належать комп'ютерні віруси, мережеві черв'яки, програма «троянський кінь».

Віруси є шкідливими програмами, які впроваджуються в інші програми для виконання певної небажаної функції на робочій станції кінцевого користувача.

Вірус зазвичай розробляється зловмисниками таким чином, щоб якнайдовше залишатися невиявленим у комп'ютерній системі. Початковий період дрімоти вірусів є механізмом їх виживання. Вірус виявляється повною мірою в конкретний момент часу, коли відбувається певна подія виклику, наприклад, п'ятниця 13-е, відома дата і т.п.

Різновидом програми-вірусу є мережевий черв'як, який поширюється глобальною мережею і не залишає своєї копії на магнітному носії. Цей термін використовується для іменування програм, які, подібно до стрічкових хробаків, переміщаються по комп'ютерній мережі від однієї системи до іншої. Черв'як використовує механізми підтримки мережі для визначення вузла, який може бути вражений.

Потім за допомогою цих механізмів черв'як передає своє тіло в цей вузол і або активізується, або чекає відповідних умов для активізації. Мережеві черв'яки є небезпечним видом шкідливих програм, оскільки об'єктом їх атаки може стати будь-який з мільйонів комп'ютерів, підключених до глобальної мережі Інтернет. Для захисту від хробака необхідно вжити запобіжних заходів проти несанкціонованого доступу до внутрішньої мережі.

До комп'ютерних вірусів примикають звані «троянські коні» (троянські програми). «Троянський кінь» - це програма, яка має вигляд корисної програми, а насправді виконує шкідливі функції (руйнування програмного забезпечення,

копіювання та пересилання зловмиснику файлів з конфіденційними даними тощо).

Небезпека «троянського коня» полягає у додатковому блоці команд, вставленому у вихідну нешкідливу програму, яка потім надається користувачам *АС*. Цей блок команд може спрацьовувати при настанні будь-якої умови (дати, стан системи) або по команді ззовні. Користувач, який запустив таку програму, наражає на небезпеку як свої файли, так і всю *АС* в цілому.

Згідно з даними огляду загроз інформаційній безпеці *Sophos Security Threat Management Report* у першій половині 2006 року кількість «троянських» програм, що розповсюджуються, перевищила кількість вірусів і черв'яків у чотири рази, але порівняно з дворазовою перевагою за перші шість місяців 2005. *Sophos* також повідомляє про появу нового виду троянських» програм, що отримав назву *ransomware*. Такі програми викрадають дані із заражених комп'ютерів, а потім користувач пропонує заплатити за них певний викуп.

Робочі станції кінцевих користувачів дуже вразливі для вірусів, мережевих хробаків та «троянських коней».

Особливістю сучасних шкідливих програм є їхня орієнтація на конкретне прикладне ПЗ, що стало стандартом де-факто для більшості користувачів, насамперед це *Microsoft Internet Explorer* та *Microsoft Outlook*. Масове створення вірусів під продукти *Microsoft* пояснюється як низьким рівнем безпеки і надійності програм, важливу роль грає глобальне поширення цих продуктів. Автори шкідливого програмного забезпечення дедалі активніше починають досліджувати «дірки» у популярних СУБД, що пов'язують ПЗ та корпоративні бізнес-додатки, побудовані на базі цих систем.

Віруси, черв'яки та «троянські» програми постійно еволюціонують, основною тенденцією їх розвитку є поліморфізм. Сьогодні вже досить складно провести кордон між вірусом, черв'яком і «троянською» програмою, вони використовують практично одні й ті самі механізми, невелика різниця полягає лише у ступені цього використання.

Пристрій шкідливого програмного забезпечення став сьогодні настільки уніфікованим, що, наприклад, відрізнити поштовий вірус від хробака з деструктивними функціями практично неможливо. Навіть у «троянських» програмах з'явилася функція реплікації (як один із засобів протидії антивірусним засобам), так що за бажання їх можна назвати вірусами (з механізмом поширення у вигляді маскування під прикладні програми).

Для захисту від зазначених шкідливих програм необхідно вжити ряд заходів:

– виключення несанкціонованого доступу до виконуваних файлів;
– тестування придбаних програмних засобів;
– контроль цілісності виконуваних файлів та системних областей;
– створення замкнутого середовища виконання програм.

Боротьба з вірусами, хробаками і «троянськими кіньми» ведеться за допомогою ефективного антивірусного програмного забезпечення, що працює на рівні користувача і, можливо, на рівні мережі. У міру появи нових вірусів, черв'яків та «троянських коней» потрібно встановлювати нові бази даних антивірусних засобів та додатків.

Спам, обсяг якого перевищує 80% від загального обсягу поштового трафіку, може створювати загрозу доступності інформації, блокуючи поштові сервери, або використовуватися для поширення шкідливого програмного забезпечення.

Фішинг є відносно новим видом інтернет-шахрайства, мета якого отримати ідентифікаційні дані користувачів. Сюди належать крадіжки паролів, номерів кредитних карток, банківських рахунків, *PIN*-кодів та іншої конфіденційної інформації, яка дає доступ до грошей користувача.

Фішинг використовує не технічні недоліки програмного забезпечення, а легковірність користувачів Інтернету. Сам термін *phishing*, співзвучний з *fishing* (рибний лов), розшифровується як *password harvesting fishing* вивужування пароля. Справді, фішинг дуже схожий на риболовлю. Зловмисник закидає в

Інтернет приманку та «виловлює всіх рибок» користувачів Інтернету, які клюнуть на цю приманку.

Зловмисником створюється практично точна копія сайту обраного банку (електронної платіжної системи, аукціону тощо). Потім за допомогою спам-технології електронною поштою розсилається лист, складений таким чином, щоб бути максимально схожим на цей лист від обраного банку. При складанні листа використовуються логотипи банку, імена та прізвища реальних керівників банку.

У такому листі, як правило, повідомляється про те, що через зміну програмного забезпечення в системі інтернет-банкінгу користувачеві необхідно підтвердити або змінити свої облікові дані. В якості причини для зміни даних може бути названий вихід з ладу ПЗ банку або напад хакерів.

Наявність правдоподібної легенди, що спонукає користувача до необхідних дій, неодмінна складова успіху шахраїв-фішерів. У всіх випадках мета таких листів одна змусити користувача натиснути наведене посилання, а потім ввести свої конфіденційні дані (паролі, номери рахунків, *PIN*-коди) на хибному сайті банку (електронної платіжної системи, аукціону). Зайшовши на хибний сайт, користувач вводить у відповідні рядки свої конфіденційні дані, а далі аферисти отримують доступ у кращому випадку до його поштової скриньки, у гіршому – до електронного рахунку.

Технології фішерів удосконалюються, використовуються методи соціальної інженерії. Клієнта намагаються налякати, придумати критичну причину для того, щоб він видав свої конфіденційні дані. Як правило, повідомлення містять погрози, наприклад, заблокувати рахунок у разі невиконання одержувачем вимог, викладених у повідомленні.

З'явилося поєднане з фішингом поняття фармінг. Це теж шахрайство, що ставить за мету отримати персональні дані користувачів, але не через пошту, а прямо через офіційні *Web*-сайти. Фармери замінюють на серверах *DNS* цифрові адреси легітимних *Web*-сайтів на підроблені адреси, в результаті чого користувачі перенаправляються на сайти шахраїв. Цей вид шахрайства ще небезпечніший, оскільки помітити підробку практично неможливо.

В даний час шахраї часто використовують "троянські" програми. Завдання фішера в цьому випадку дуже спрощується досить змусити користувача перебратися на фішерський сайт і «підчепити» програму, яка самостійно знайде на жорсткому диску жертви все, що потрібно. Нарівні з «троянськими» програмами стали використовуватися і кейлоггери, на підставних сайтах на комп'ютери жертв завантажують шпигунські утиліти, що відстежують натискання клавіш. При використанні такого підходу необов'язково знаходити виходи на клієнтів конкретного банку або компанії, а тому фішери стали підробляти і сайти загального призначення, такі як стрічки новин та пошукові системи.

Висновок до першого розділу

Враховуючи ключові технології, такі як *VMware NSX*, можна забезпечити ізоляцію трафіку, підвищити рівень безпеки та прискорити передачу даних. *NSX* дозволяє створювати віртуальні мережі між віддаленими фізичними пристроями, що сприяє більш гнучкому та масштабованому підходу до конфігурації мережі.

РОЗДІЛ 2
РОЗГЛЯД ОСНОВНИХ ПОНЯТЬ ОПТИМІЗАЦІЇ МЕРЕЖІ

2.1 Ідея мережі

Корпоративна мережа має бути гнучкою та легко підлаштовуватися під потреби начальства. У подібному середовищі все працює це стосується навіть робочих станцій, адже не робочий комп'ютер це гроші на вітер і щоб уникнути такої ситуації робочу мережу потрібно оптимізувати віртуалізацією.

Сьогодні всі лідируючі компанії переходять на "хмарні технології" плюси від цього дуже вагомі найголовніший з них це відсутність потреби у догляді за технікою та її утилізацією. Компанії більше не потрібно буде стежити за технікою, ремонтувати її, продавати чи викидати. Варто лише змінити умови контракту та все.

У вас робочі станції, а у *Cloud Service Provider* задоволений клієнт, причому у вас так само є страховка, що дозволить вам отримати виплату, якщо ваш *CSP* не виконав умову контракту, що тільки підвищує цінність даної оптимізації.

2.2 Функціональна структура підприємства

Ця оптимізація підходить не тільки конгломератам але й простим приватним бізнесам з надання онлайн послуг. Адже ви можете спокійно розширити вашу мережу, купивши ще віртуальну машину і підключити її до вашого сервера.

Але тут важливо зрозуміти що вам доведеться використовувати ліцензовані продукти і платити за підписки, адже ваш *CSP* не надаватиме послуги вкрадених ключів. Що в свою чергу стимулює переходити на *Linux* сервера і використовувати системи як *Windows* 7 або ті ж безкоштовні *Ubuntu* та інші. У цій роботі я демонструватиму оптимізацію використовую *Windows Server* 2016 та клієнти на *Windows* 7.

2.3 Вимоги до мережі

Корпоративна мережа повинна мати свого системного адміністратора, адже збій роботи мережі в корпорації може обійтися як кілька місячних зарплат фахівця. Мережа повинна мати контракт з провайдером і резервні виходи в мережу використовуючи інші лінії, якщо одна пошкодиться. Підключення має бути реалізовано використовуючи мінімум гігабітне з'єднання по оптоволоконному кабелю, а сама мережа повинна мати свою резервну електрику на випадок збою електроживлення в місті

2.4 Вимоги до мережевих сервісів

До вибору провайдера варто підходити дуже уважно так-як вибір прискіпливого провайдера може привести тільки до повторного виклику мережевих інженерів для підключення нового. Основні вимоги для провайдера це можливість покупки і продовження оренди для білих *ip* адрес. Так як мережа повинна бути статичною для можливості віддаленої конфігурації адміністратором. Також один дуже добре побудований сервер може видавати свої ресурси за межі мережі для сусіднього офісу. Вибір оператора так само допоможе в майбутньому, убезпечити від атак з поза які можуть відключити інтернет для сервера.

2.5 Вимоги до надійності мережі

Надійність мереж має особливе значення, оскільки будь-яка втрата даних може призвести до серйозних наслідків, включаючи втрату цінних бізнес даних або особистих файлів користувачів.

У цьому розділі буде розглянуто надійність мереж для бездискових систем, використовувані для забезпечення надійності.

Важливим методом забезпечення надійності мереж є резервне копіювання даних. Це дозволяє створити копію даних, які зберігаються на серверах або в хмарі, у разі втрати або пошкодження. Існує кілька способів резервного копіювання даних, інкрементальне та диференціальне копіювання.

Крім того, можна використовувати такі методи, як дзеркальне копіювання, коли дані дублюються на декількох серверах або вузлах мережі, та реплікація, коли дані копіюються на віддалені сервери.

Для забезпечення надійності мережі важливо також контролювати цілісність даних. Це означає, що потрібно перевіряти, чи дані, які зберігаються на серверах або в хмарі, не пошкоджені та не були змінені без дозволу користувача. Для цього можна використовувати різні методи, такі як контроль суми (*hash*-сума), який обчислює хеш-код для кожного файлу та перевіряє його щоразу, коли файл читається чи записується.

Якщо хеш-код не відповідає оригінальному, значить, файл пошкоджено або змінено, і користувачеві потрібно буде вжити заходів для відновлення.

Для забезпечення високої надійності мереж необхідно забезпечити безперервність живлення та зв'язку. Для цього можна використовувати такі методи, як резервування харчування та засобів зв'язку.

Наприклад, можна встановити додаткові джерела живлення, які будуть запасними у разі відключення основного, а також використовувати кілька засобів зв'язку, щоб забезпечити надійний зв'язок між серверами та вузлами мережі.

Зрештою, для забезпечення надійності мереж важливо моніторити роботу мережі та її вузлів.

Це допомагає виявляти проблеми, пов'язані з відмовами обладнання або програмного забезпечення, перш ніж вони призведуть до втрати даних. Для моніторингу можна використовувати різні інструменти, наприклад моніторинг завантаження мережі, системного журналу, сигналізації про відмови та ін.

2.6 Вимоги до якості обслуговування

Сервер вимагає окремої кімнати з хорошою системою охолодження так, як він буде працювати в не безперервно сеансі для підтримки віддалених робочих столів. Але це не єдина вимога, адже сам сервер потребуватиме щотижневої перевірки для його Сабліною роботи і подальшого використання.

У цю перевірку входить:

– обдув комплектуючих від шару пилу;
– перевірки на підвищену температуру;
– при підвищенні температури вище норми доведеться міняти термопасту;
– перевірка самого сервера на наявність сторонніх пристроїв;
– перевірка справності безперебійного живлення.

Ці мінімальні вимоги ставляться не тільки до сервера. Оскільки бездискові станції теж потребують щомісячної перевірки для збереження стабільності роботи.

Висновок до другого розділу

Загалом, щоб гарантувати надійність мереж, необхідна ретельна стратегія з використанням цілого ряду методів і технологій. Дуже важливо планувати мережу так, щоб вона могла протистояти сбоям, управляти цілісністю даних, резервувати енергетичні та комунікаційні ресурси, а також стежити за тим, як працює мережа та її вузли. Всі ці методи дозволяють захистити дані користувачів від втрати та пошкодження, забезпечуючи при цьому відмінну надійність мережі.

РОЗДІЛ 3
АНАЛІЗ ВІРТУАЛІЗАЦІЇ МЕРЕЖІ

3.1 *VMware* і *Windows Server*

1. Вся дипломна робота буде реалізована в *VMware* з використанням віртуальних машин. Після створення віртуальної машини з *windows server* 2016 приступаємо до налаштування статичної *IP*-адреси. Для цього потрібно натиснути на іконку мережі ПКМ і вибрати «Центр керування мережами», «Зміна параметрів адаптера», ПКМ по адаптеру та по скріншотах виконати налаштування статичного *IP* (рис 3.1).

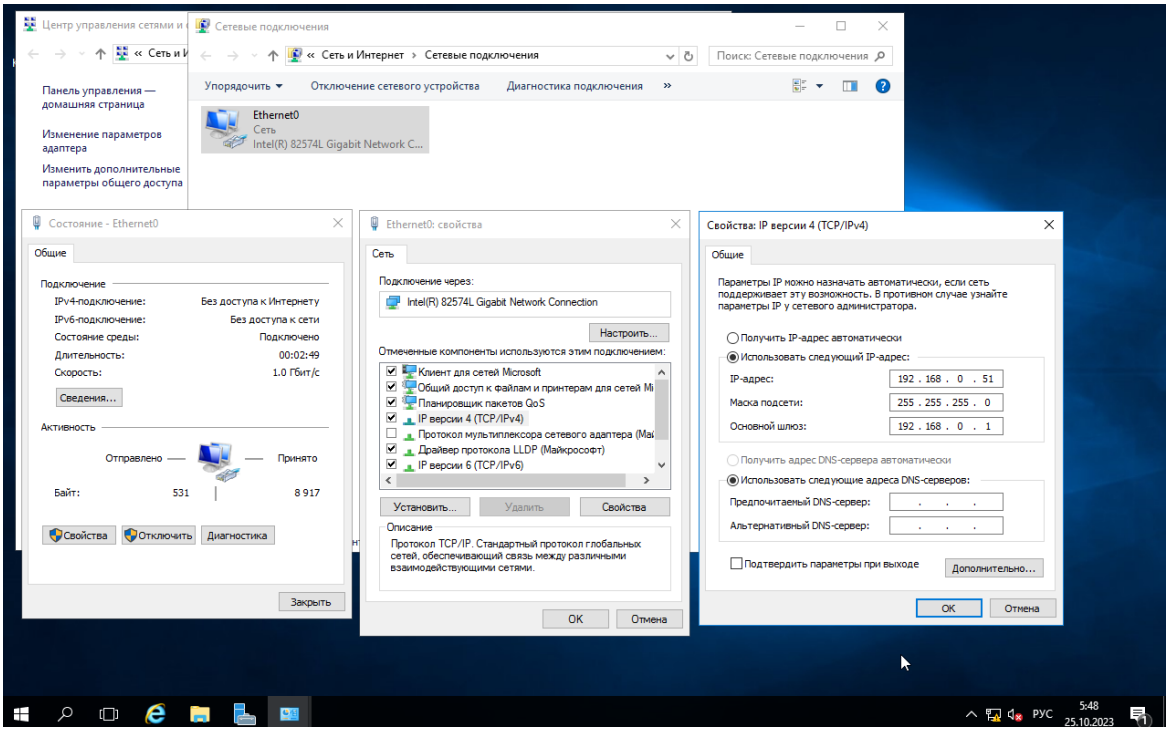

Рис. 3.1 – Налаштування статичного IP

2. Далі потрібно змінити ім'я станції, яка «тримає» сервер на більш читаний варіант. Для цього переходимо в «Диспетчер серверів», «Локальний сервер» та натискаємо на ім'я комп'ютера і вже як вказано на скріншотах змінюємо ім'я (рис 3.2) .

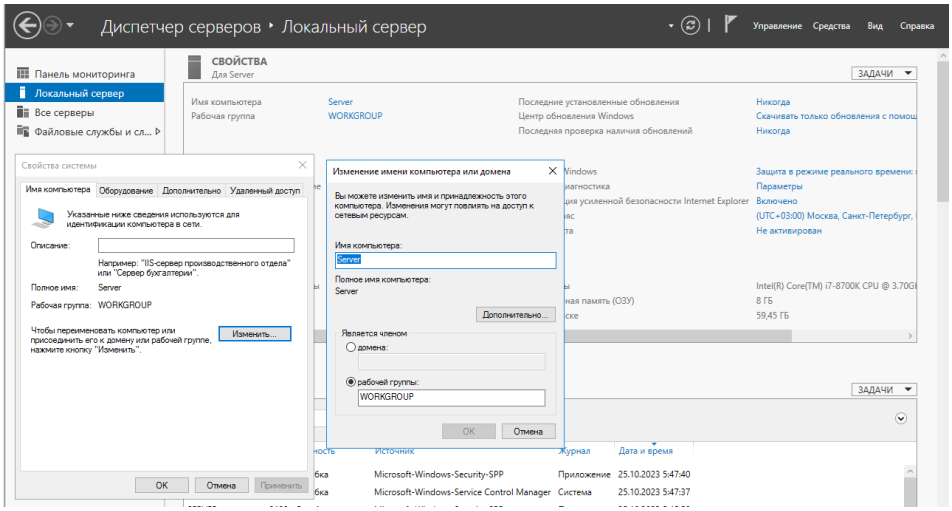

Рис. 3.2 – Підготовка сервера

3. Приступаємо до додавання компонентів на наш сервер для цього в «Диспетчер серверів» > «Локальний сервер» натискаємо «Управління» > «Додати ролі та компоненти» (рис 3.3).

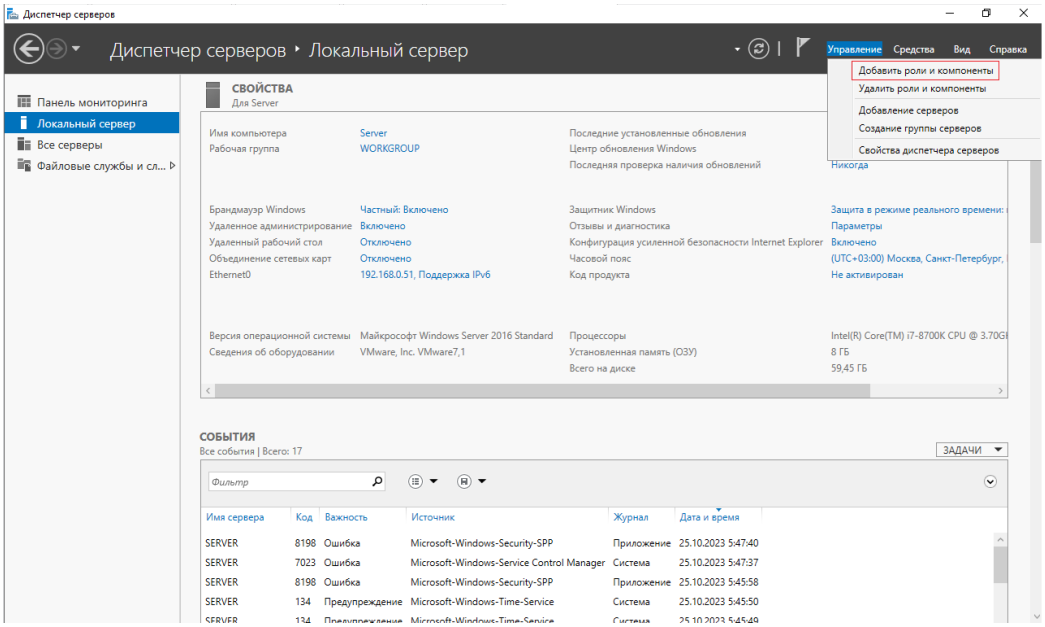

Рис. 3.3 – Додавання компонентів

4. Нас відразу зустрічає вікно установки (рис 3.4).

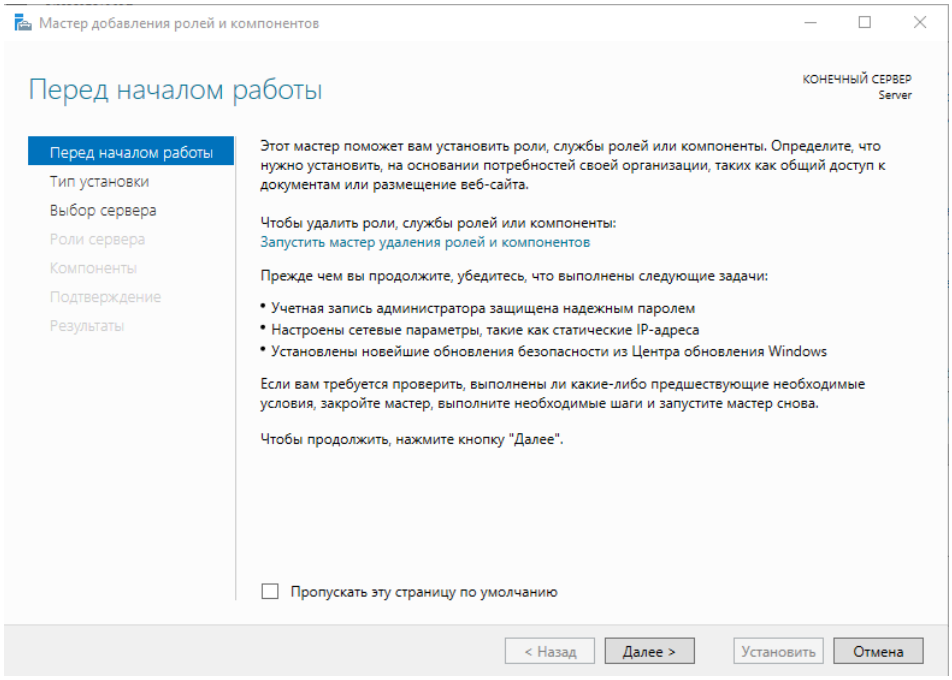

Рис. 3.4 – Майстер додавання компонентів

5. Як на скріншоті вибираємо "Встановлення ролей або компонентів" (рис 3.5).

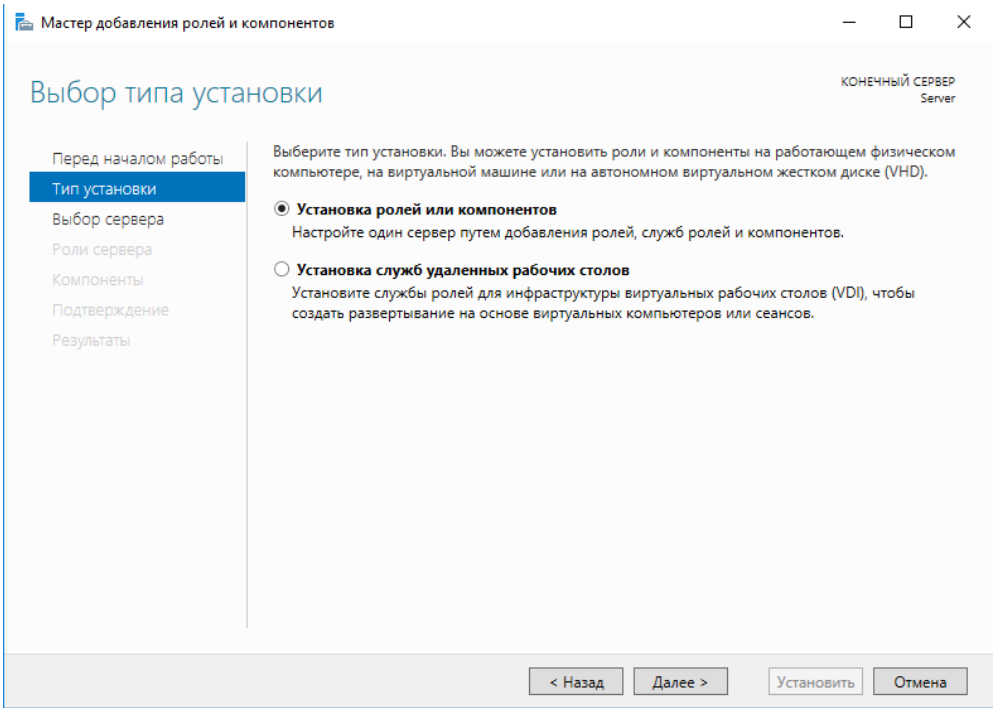

Рис. 3.5 – Тип установки

6. Оскільки це навчальний проект, то зі списку серверів ми вибираємо лише наш (рис 3.6).

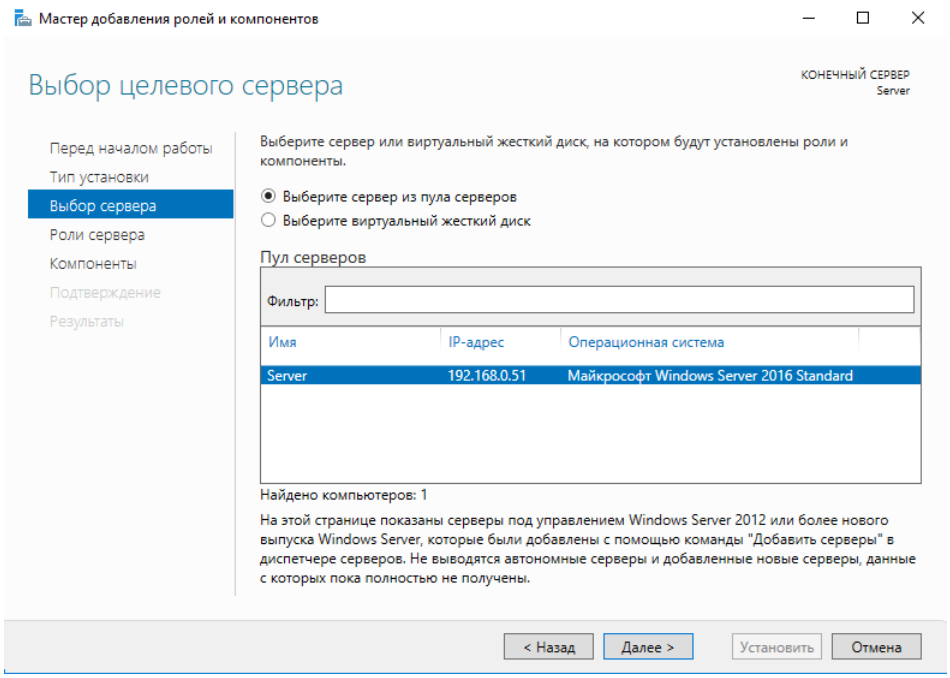

Рис. 3.6 – Вибір сервера

7. Тут важливо вибрати три компоненти, вказані на скріншоті (рис 3.7).

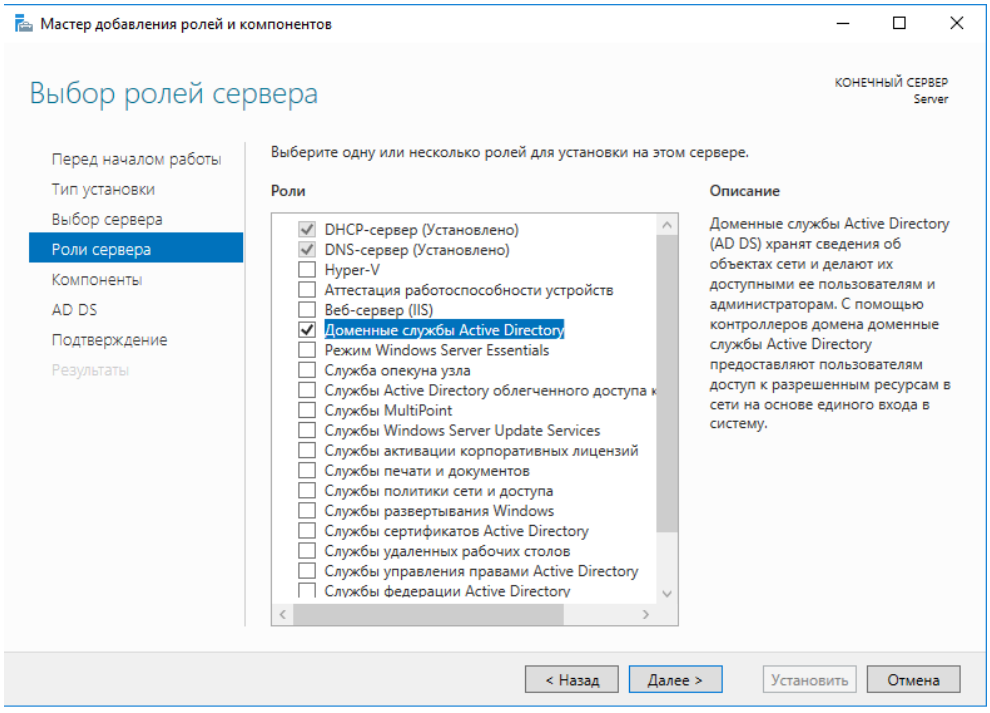

Рис. 3.7 – Додавання ролей

8. Наступні пункти можна пропустити натискаючи кнопку «Далі» (рис 3.8).

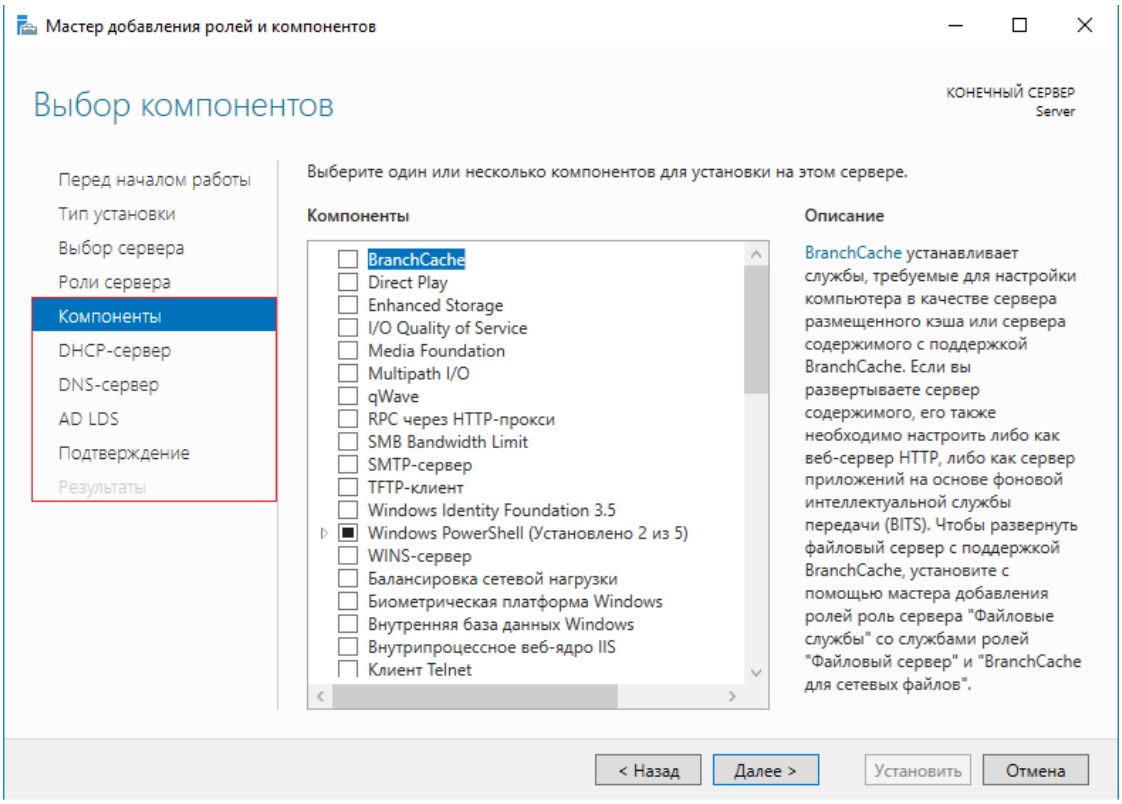

Рис. 3.8 – Завершення вибору

9. Приступаємо до завершення налаштування компонента *Active Directory* переходимо по пункту, який вказаний нижче (рис 3.9).

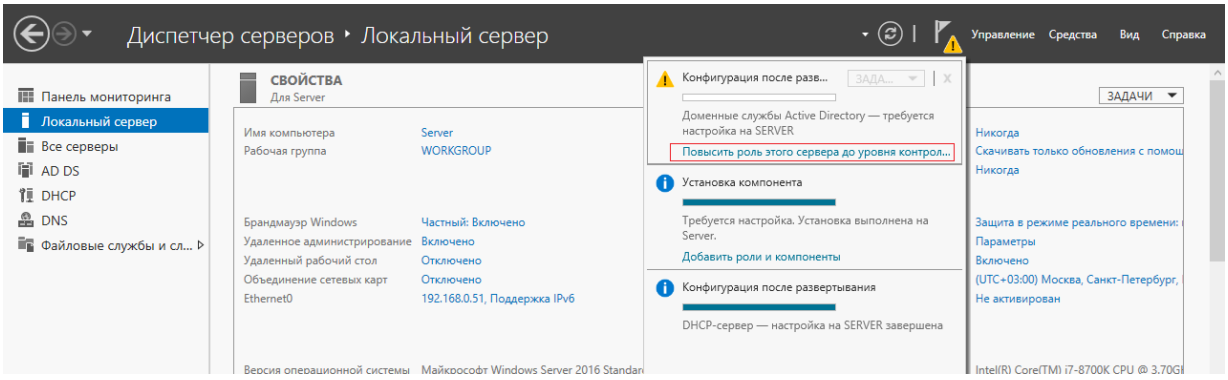

Рис. 3.9 – Налаштування Active Directory

10. Пропускаємо вітальні вікно та одразу вибираємо пункт «Додати новий ліс» і вказуємо доменне ім'я, за яким будуть підключатися користувачі (рис 3.10).

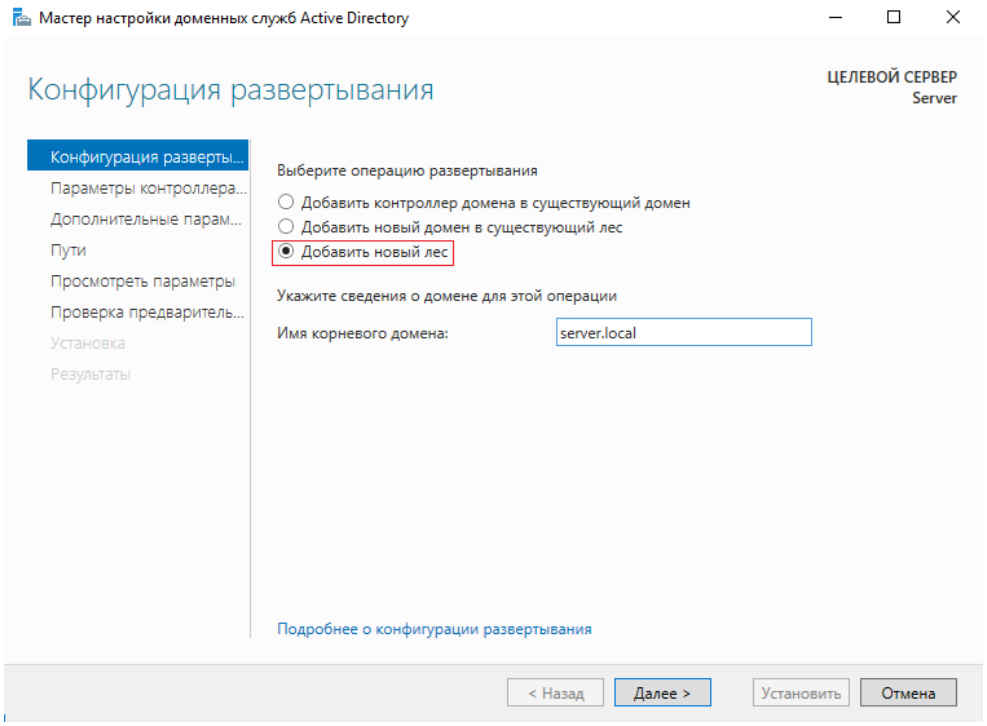

Рис. 3.10 – Створення нового лісу

11. Наступні пункти також пропускаємо (рис 3.11).

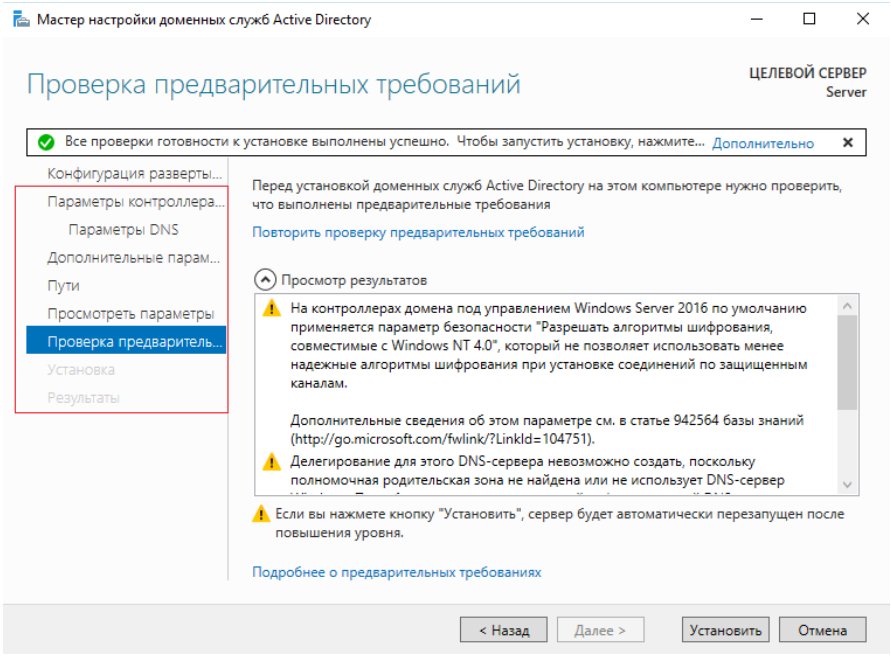

Рис. 3.11 – Завершення налаштування Active Directory

12. Далі переходимо до налаштування компонента *DHCP*, а саме створимо пул для наших користувачів з яким ми взаємодіятимемо. Для цього переходимо в «Диспетчер серверів» > *DHCP* і натискаємо ПКМ на сервері вибравши пункт «Диспетчер *DHCP*» (рис 3.12).

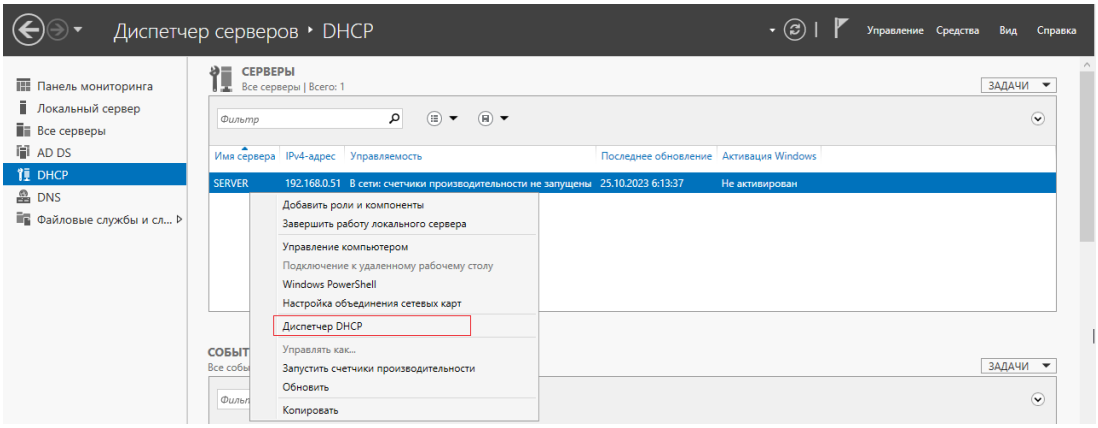

Рис. 3.12 – Створення DHCP пулу

13. У диспетчері ми можемо побачити два пули, з яких нам потрібен *IPv4*. Натискаємо на нього ПКМ та вибираємо "Створити область"

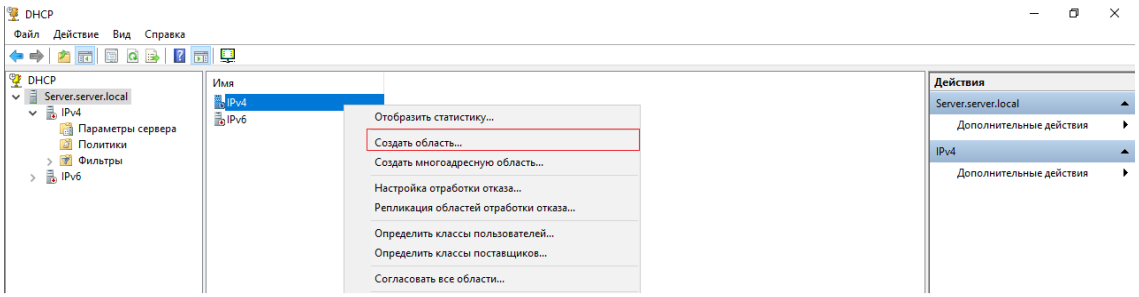

Рис. 3.13 – Створюємо область

14. Вказуємо ім'я пула (рис 3.15).

Рис. 3.14 – Ім'я пула

15. Важливо виділити пул не зайнятих *IP*-адрес у мене це 192.168.0.60-70 з 24 маскою (рис 3.15).

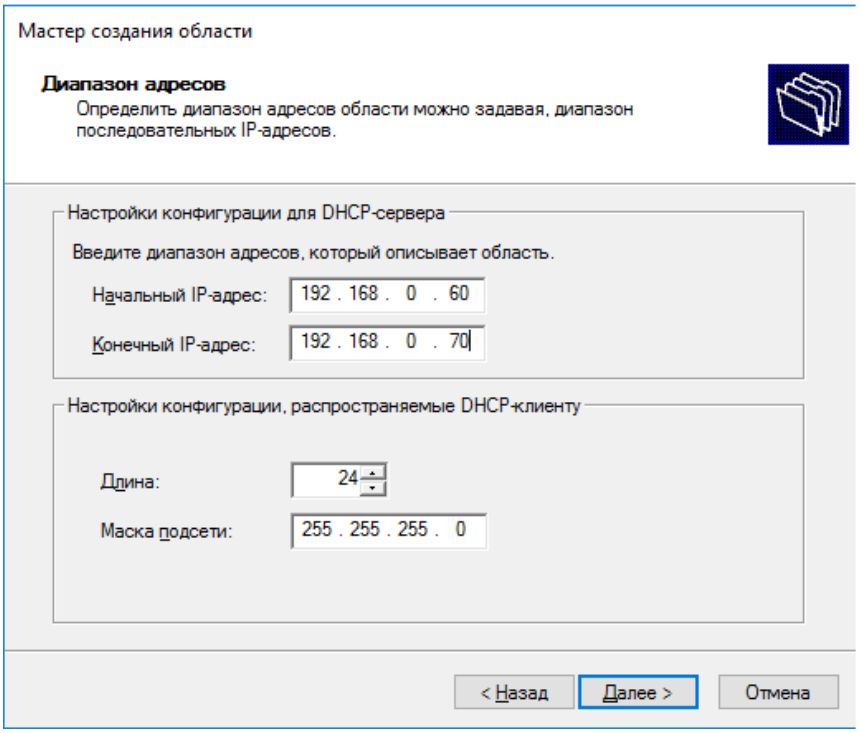

Рис. 3.15 – Вказуємо область IP

16. Пропускаємо винятки оскільки це дипломна робота (рис 3.16).

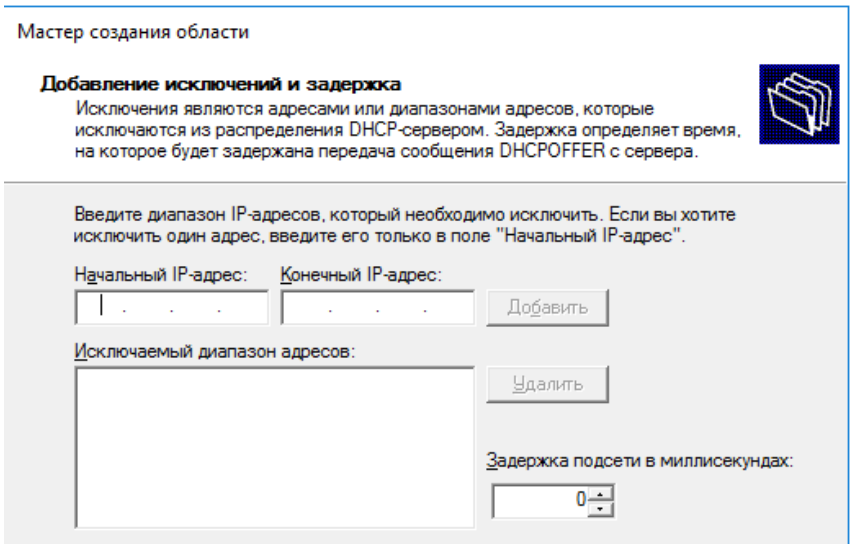

Рис. 3.16 – Виключення IP-адрес

17. «Термін дії оренди адреси» залишаємо не зрадою (рис 3.17).

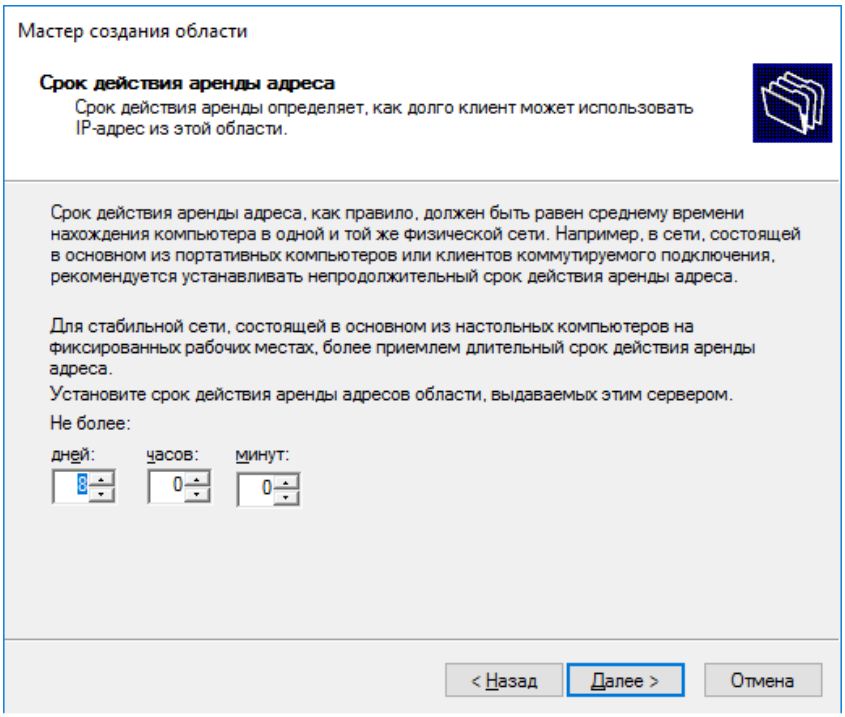

Рис. 3.17 – Термін придатності IP

18. Важливо вказати *IP*-адресу маршрутизатора для працездатності мережі (рис 3.18).

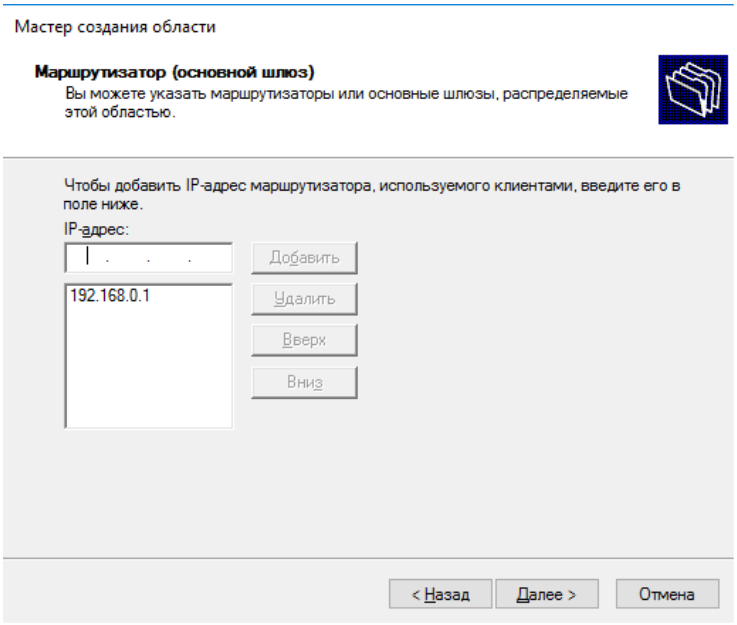

Рис. 3.18 – IP-маршрутизатора

19. Обов'язково вибираємо пункт як на скріншоті (рис 3.19).

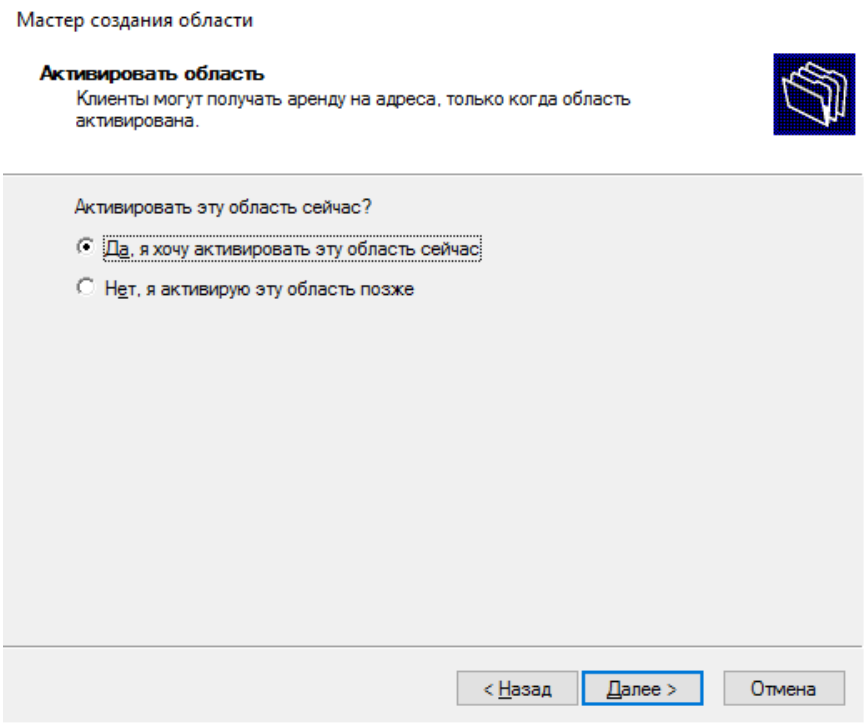

Рис. 3.19 – Активація нового пулу

20. Після створення *DHCP* пула приступаємо до створення облікового запису користувача, який дістанеться співробітнику корпорації. Для цього натискаємо на «Кошти» і переходимо в «Центр адміністрування *Active Directory*» (рис 3.20).

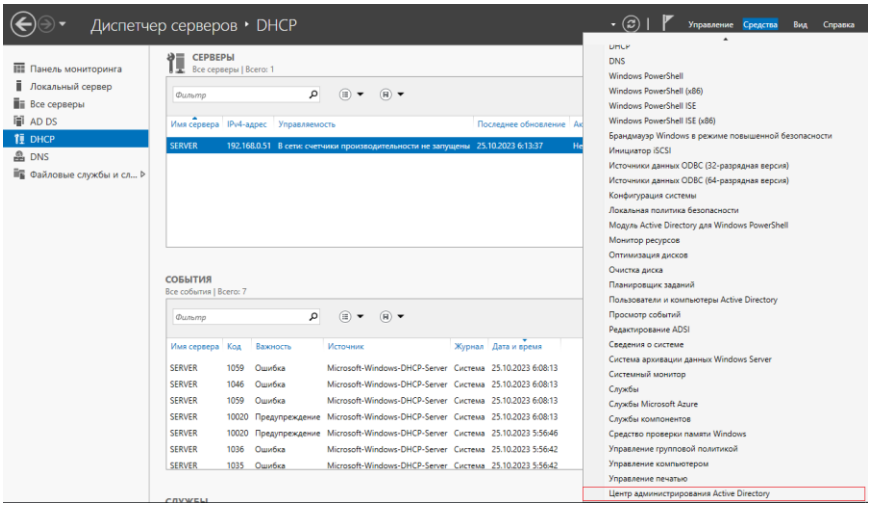

Рис. 3.20 – Центр адміністрування Active Directory

21. Як показано на малюнку нижче, ми натискаємо на «*Users*» ПКМ і вибираємо «Створити» > «Користувача» (рис 3.21).

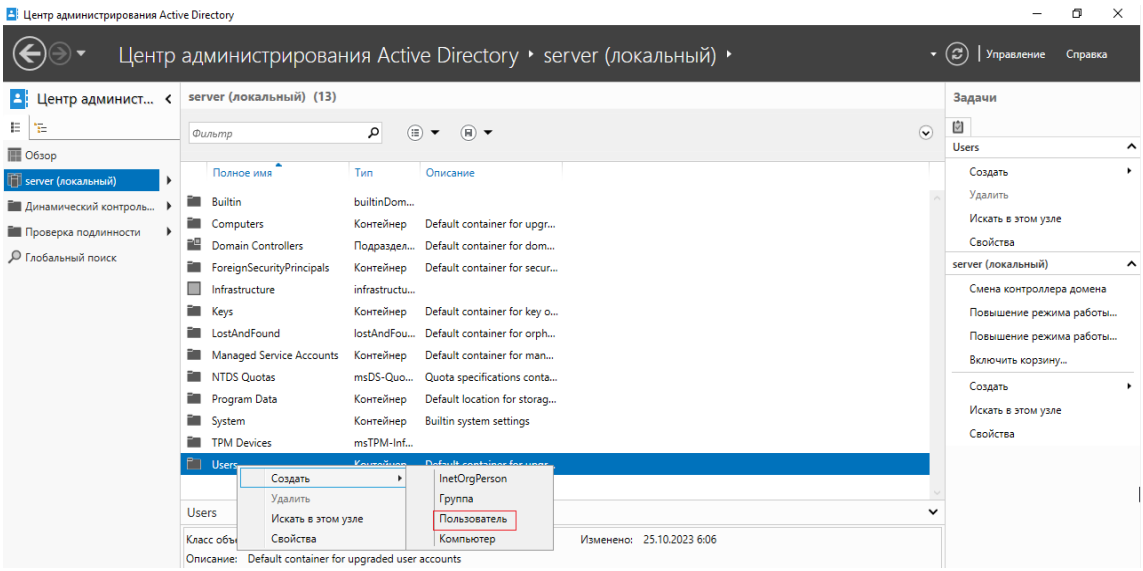

Рис. 3.21 – Створення користувача

22. У вікні вводимо всю потрібну інформацію, вказуємо зручний логін в рядку «*UPN*» для користувача і обов'язково натискаємо на «Заборонити зміну пароля користувачем» (рис 3.22).

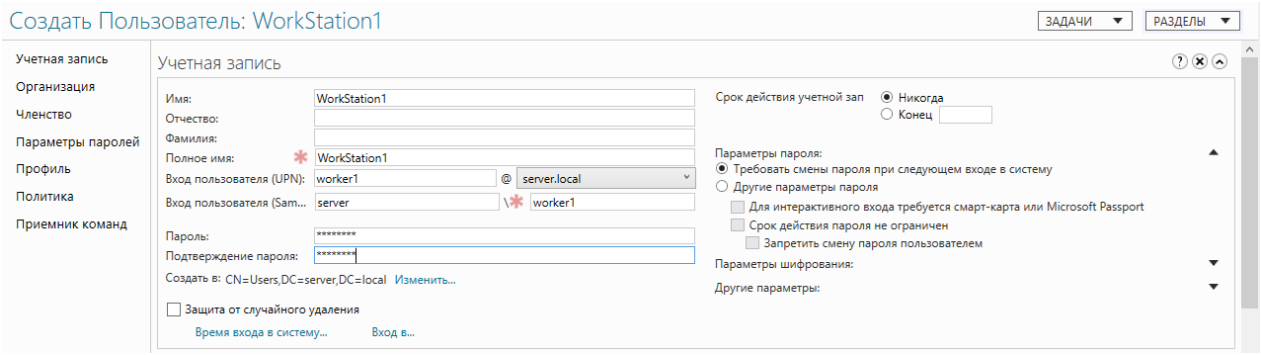

Рис. 3.22 – Вікно створення користувача

23. Важливий пункт, оскільки без цього неможливо буде підключиться до *RDP*. Переходимо в «Членство» і натискаємо кнопку «Додати» та копію «Додатково» (рис 3.23).

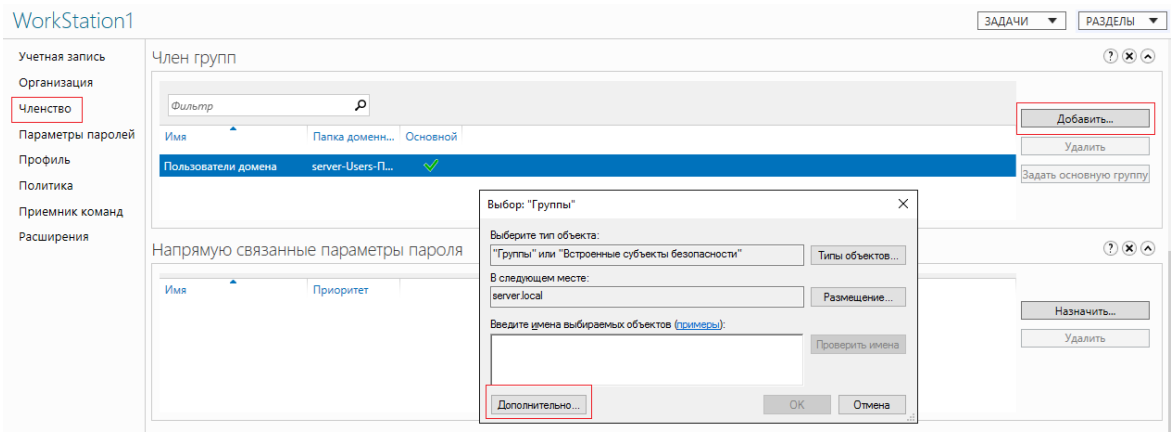

Рис. 3.23 – Додавання до членства

24. Натискаємо на кнопку «Пошук», що дозволить нам побачити список з усіма групами. Вибираємо «Користувачі віддаленого робочого столу» (рис 3.24).

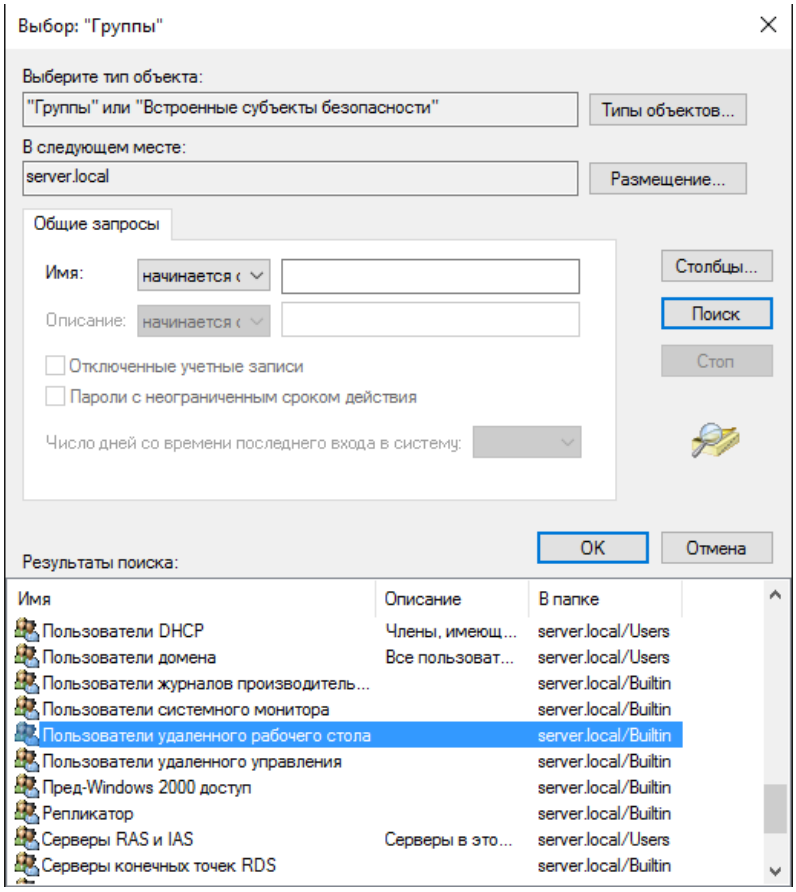

Рис. 3.24 – Вибір групи

25. Після цього зберігаємо нашого новоствореного користувача натиснувши кнопку «Ок» (рис 3.25).

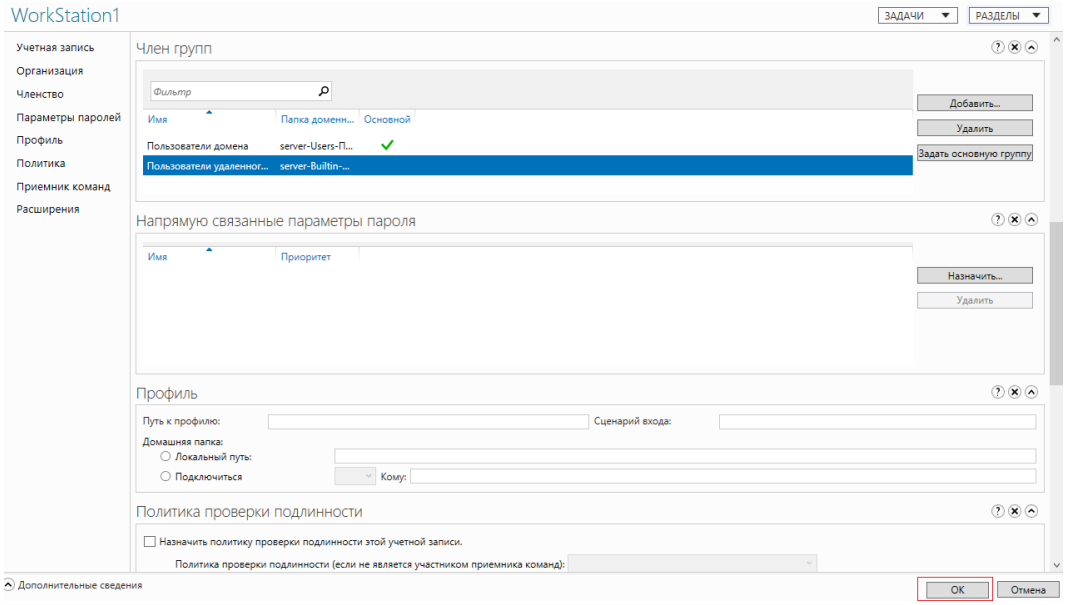

Рис. 3.25 – Завершення створення користувача

26. Для цієї дипломної роботи був вибраний безкоштовний *RadminVPN* який дозволить нам створити *RDP* підключення. Як адмін сервера, створюємо новий сервер на якому будуть користувачі (рис 3.25).

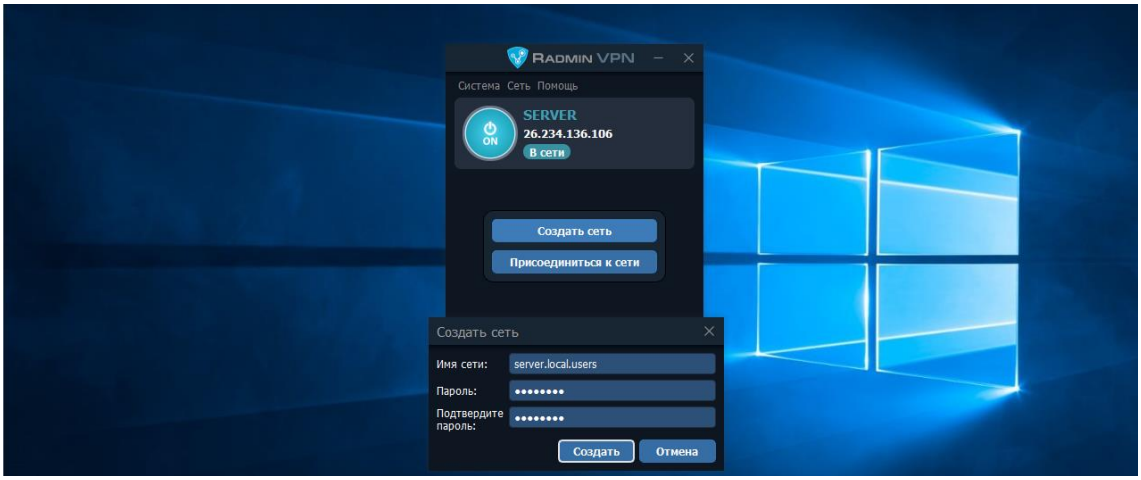

Рис. 3.26 – *RadminVPN*

3.2 Клієнтська частина

27. Після налаштування серверної частини, приступимо до створення клієнтської частини для цього в *VMware* створюємо нову машину з *Windows* 7 . Після встановлення приступаємо до налаштування статичної *IP* адреси виберемо *IP* адресу з нашого пулу і обов'язково вкажемо *DNS* нашого сервера (рис 3.27).

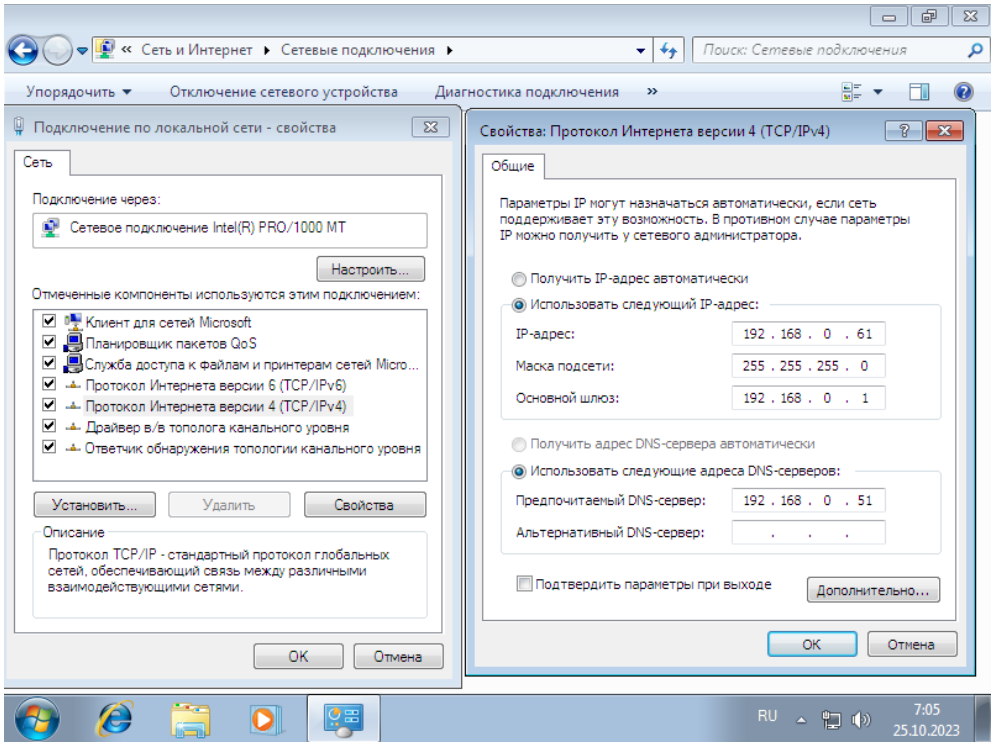

Рис. 3.27 – Налаштування статичної *IP*-адреси

28. Натискаємо на «Мій комп'ютер» ПКМ та вибираємо «Властивості» далі «Змінити параметри» > «Змінити» . Вводимо ім'я нашого домену (рис 3.28).

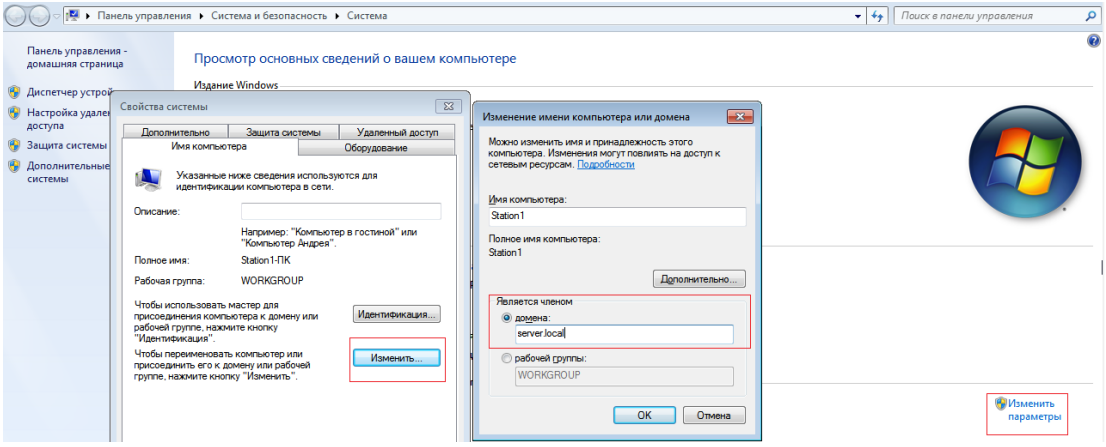

Рис. 3.28 – Підключення до домену

29. Підключаємося до нашого сервера, використовуючи обліковий запис Адміністратора (рис 3.29).

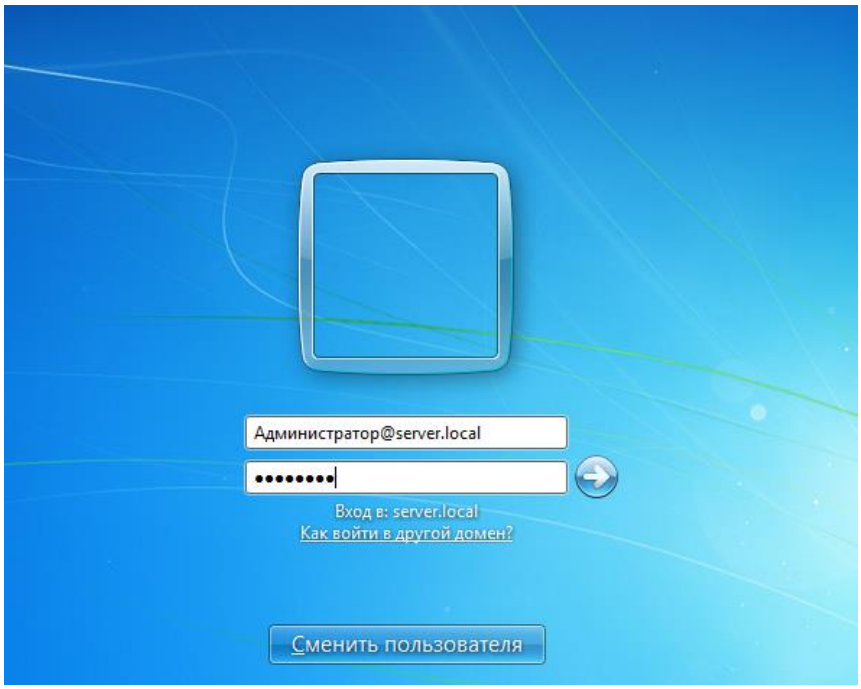

Рис. 3.29 – Підключення до сервера

30. Тепер, приступаємо до важливого налаштування, без цього, ця станція не дозволить користувачам підключатися до *RDP* цього комп'ютера. Для цього, переходимо в «Додаткові параметри системи» > вкладка «Видалений доступ» вибираємо останній пункт і натискаємо на кнопку «Вибрати користувачів» > «Додати», і в порожньому полі вводимо «логін@домен», і натискаємо на кнопку «Перевірити імена» (рис 3.30).

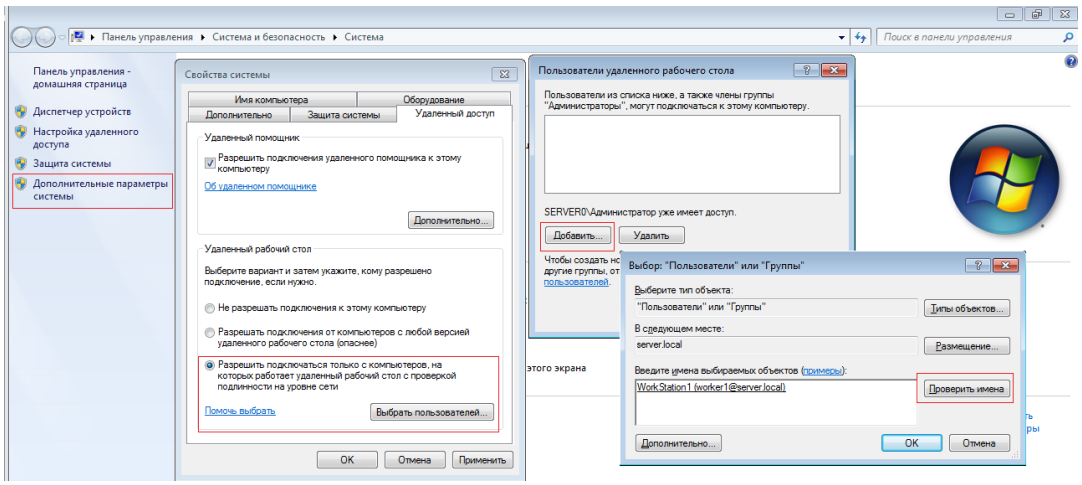

Рис. 3.30 – *RDP*

31. Заходимо на цю станцію, використовуючи створений для неї обліковий запис для того, щоб створився робочий стіл.

32. Завантажуємо *VPN* та підключаємося на сервер (рис 3.32).

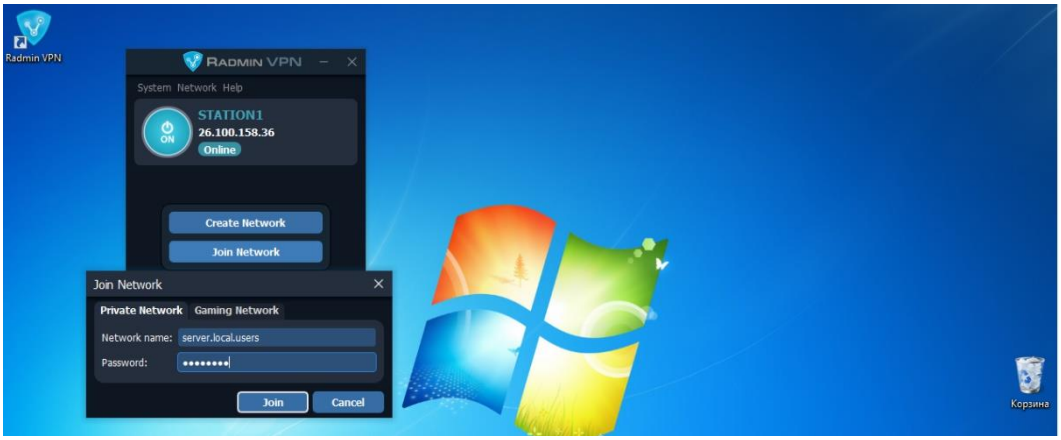

Рис. 3.32 – *VPN* тунель

33. Тепер, проведемо перевірку доступності *RDP* робочої станції. Для цього, створимо ще одну віртуальну машину і назвемо її *HomePc*, на ній так само має бути *VPN* тунель до корпоративної мережі. Підключившись, копіюємо *IP*-адресу *Station*1 (рис 3.33).

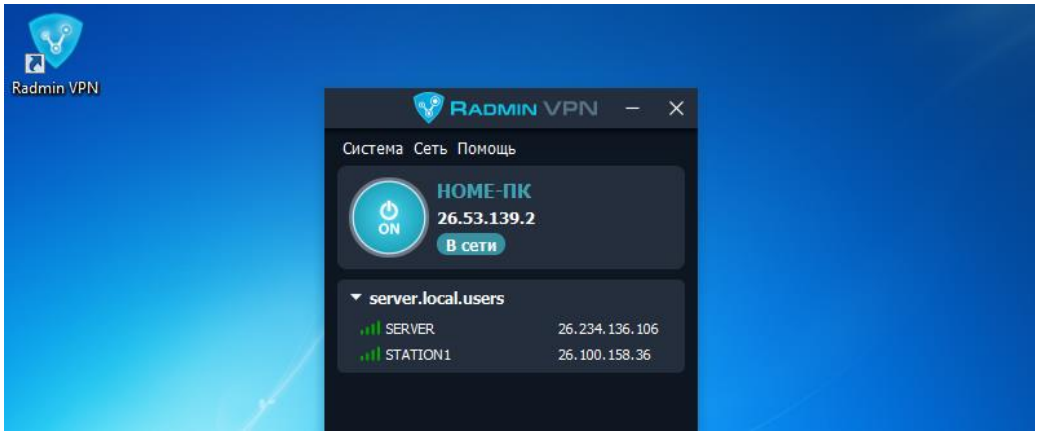

Рис. 3.33 – Доступ до *RDP*

34. Здійснюємо підключення. Вказуємо *IP*-адресу станції та вибравши кнопку «Параметри» вказуємо логін нашого користувача, натискаємо на кнопку «Підключиться» (рис 3.34).

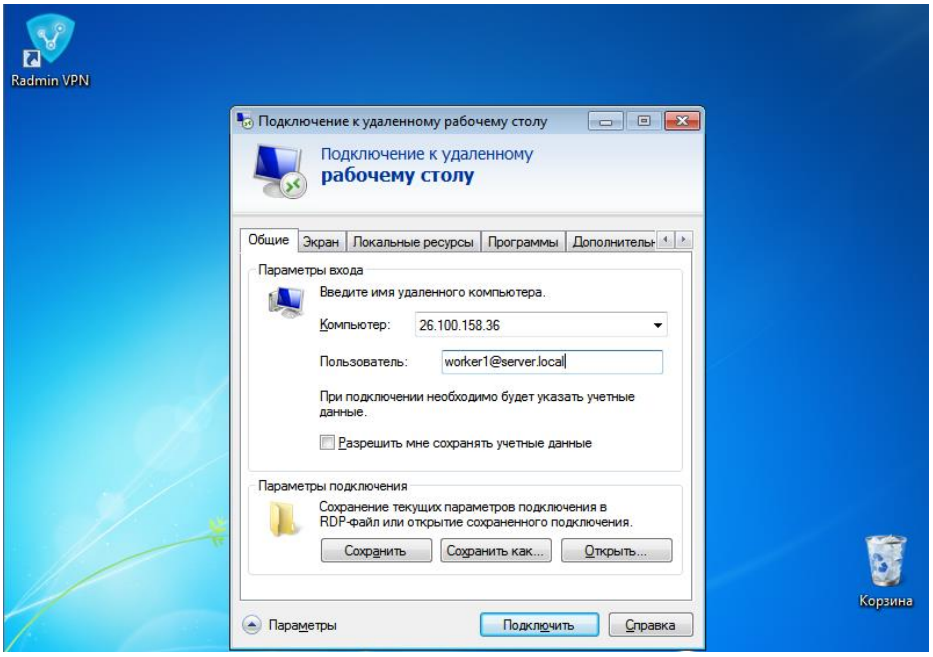

Рис. 3.34 – Підключення до сервера

35. Через те, що це дипломна робота, то у нашої робочої станції немає ліцензії на *RDP*, через це, нам висвічується попередження, що «Сертифікат виданий не має довіри центром сертифікації» (рис 3.35).

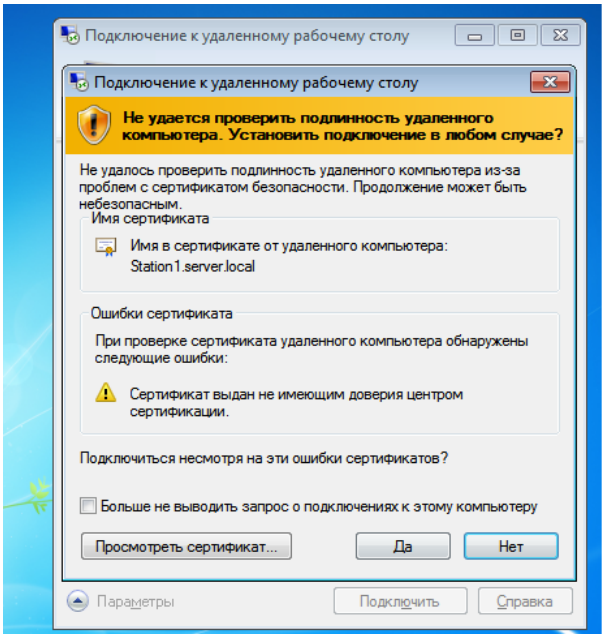

Рис. 3.35 – Сертифікат

36. Ось, ми і підключилися до нашої віддаленої станції. Цей підхід допоможе з підключенням не тільки стаціонарних комп'ютерів, але й віртуальних машин, створених в *AWS* або *Google* (рис 3.36).

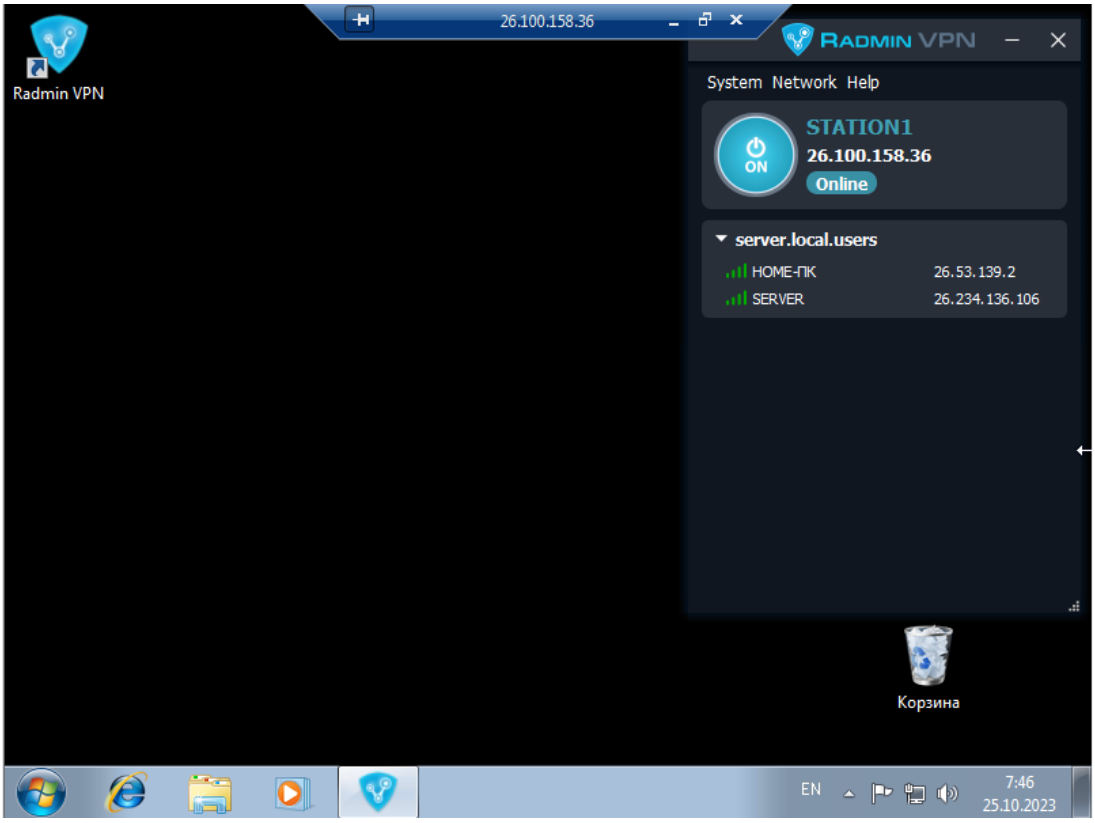

Рис. 3.36 – Робочий стіл віддаленої станції

Висновок до третього розділу

У висновках до третього розділу можна відзначити, що аналіз процесу створення мережі дозволив виявити ключові аспекти та основні етапи цього процесу. Зокрема, було висвітлено етапи встановлення віртуальних мереж за допомогою технологій, таких як *VMware, RadminVPN*. Цей розділ надає зрозуміння про те, як віртуалізація мережі взаємодіє з фізичними пристроями та технологіями.

РОЗДІЛ 4
ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ПРОЕКТУ

4.1 Основні завдання маркетингового обґрунтування проекту

Аналіз техніко-економічної доцільності проекту, визначення потенційних споживачів продукції, оцінка ринкового потенціалу проекту, вибір стратегії виходу на ринок, розрахунок вартості проекту та оцінка його ефективності є основними завданнями. організаційно-економічне та маркетингове обґрунтування проекту.

Розробка організаційної структури проекту, планування витрат і прибутків, оцінка ефективності використання ресурсів, розрахунок фінансових показників, виявлення можливостей фінансування проекту є частиною організаційно-економічного обґрунтування проекту. .

Дослідження ринку та конкурентного середовища, визначення побажань і готовності споживачів купувати товари, формулювання маркетингової стратегії та планування маркетингових дій все це частина маркетингового обґрунтування.

Усі ці обов’язки сприяють успіху проекту шляхом максимізації його прибутковості та ефективності використання ресурсів.

Основними завданнями організаційно-економічного обґрунтування проекту оптимізація локальної мережі з використанням *CSP* є розрахунок витрат на проектування та будівництво мережі, оцінка довгострокової прибутковості та ефективності проекту, як а також створення фінансового та бізнес-плану проекту.

Основними цілями маркетингового обґрунтування є визначення перспективного споживання послуг мережі доступу, створення маркетингового та рекламного плану та оцінка конкурентоспроможності мережі на ринку послуг зв'язку.

Організаційно-економічне та маркетингове обґрунтування проекту також розглядає ризики та можливості, пов’язані з його реалізацією, а також законодавчі та нормативні вимоги щодо розвитку та обслуговування мережі доступу.

У проекті з проектування локальної мережі з тонких клієнтів, витрати в економічній частині можуть бути спрямовані на наступні напрямки:

1. Придбання необхідного обладнання та програмного забезпечення для забезпечення функціонування мережі.
2. Навчання та підготовка персоналу для роботи з мережею, що включає в себе курси навчання, семінари та тренінги.
3. Реклама та маркетингові заходи для просування мережі серед потенційних користувачів та клієнтів.
4. Фінансування досліджень та розробок для постійного вдосконалення мережі та впровадження нових технологій.
5. Оплата витрат на електроенергію, інтернет-підключення та інші операційні витрати, пов'язані з експлуатацією мережі.

Щоб переконатися, що гроші, витрачені на проект, будуть використані максимально ефективно і що він буде успішно реалізований, ці витрати повинні бути обґрунтовані ще на етапі планування проекту шляхом проведення необхідних розрахунків і аналізу ринку.

Оцінка прибутковості проекту є важливою складовою його економіки. Для цього необхідно проаналізувати витрати на проект та очікувані доходи.

Витрати на проект локальної мережі з тонких клієнтів можуть також включати придбання необхідних інструментів і витратних матеріалів, оплату послуг фахівців з проектування, налаштування обладнання, а також витрати на маркетинг і просування.

4.2 Організаційне обґрунтуванням проекту

Для проведення організаційного обґрунтування проекту необхідно розглянути деякі його характеристики.

1. По-перше, слід провести класифікаційну оцінку різновиду проекту:

– за класом проект слід вважати монопроектом;

– тип проекту технічний;

– вид учбово-освітній;

– за тривалістю проведення аналізу живучості та можливих робіт з резервування, у відповідності до створених рекомендацій, проект можна класифікувати як короткостроковий;

– за складністю та розмірами як проект простий невеликих розмірів, бо мережа доступу, обрана для аналізу розміщується на території, що не перевищує 0,34 км2;

– за рівнем проект можна віднести до галузевих проектів.

2. По-друге, необхідно визначити мету та результати проекту.

Мета: проведення оптимізації мережі доступу, побудованої за технологією *PON*, розробка рекомендацій щодо підвищення живучості мережі шляхом резервування окремих елементів мережі.

Результат: створення необхідної документації, розрахунків та функціональної схеми, які необхідні для аналізу живучості мережі доступу та рекомендацій щодо її підвищення, проведення робіт з резервування *OLT* та фідерного волокна.

Етапи виконання проекту з орієнтовними строками, їх послідовність та тривалість:

1. Збір інформації з предметної області та ознайомлення з характеристиками мережі, яка буде досліджуватися (15 днів).
2. Формування технічного завдання (7 днів).
3. Опис території мережі, особливостей її будови, окремих секторів, технічних характеристик мережі доступу (наприклад, довжини ліній зв’язку) та затвердження плану проекту (10 днів).

4. Ознайомлення з фаховою документацією та загальний опис технології *PON* (8 днів).
5. Розгляд основоположних понять для аналізу живучості (наприклад, живучість та надійність) (5 днів).
6. Дослідження шкідливих чинників, які можуть впливати на мережу, та шляхів захисту від них (5 днів).
7. Проведення класифікації шкідливих чинників, що діють на оптичні мережі доступу (2 дні).
8. Ознайомлення з критеріями та показниками живучості мережі доступу (4 дні).
9. Порівняльний аналіз методів та показників живучості мереж (9 днів);
10. Створення пояснювальної записки на основі проведеної роботи (16 днів).
11. Проведення порівняльного аналізу оптичних пасивних мереж, побудованих згідно з різними топологіями (8 днів).
12. Розрахунок показників живучості різних секторів досліджуваної мережі та проведення аналізу живучості секторів (12 днів) .
13. Розгляд різних видів резервування, для підвищення живучості мереж, та побудова схем резервування для кожного з них (7 днів).
14. Рекомендації щодо підвищення живучості досліджуваної мережі, шляхом часткового резервування з боку *OLT* (4 дні).
15. Створення загальної функціональної схеми мережі (5 днів).
16. Перевірка та доробка пояснювальної записки та технічної документації (10 днів).
17. Реалізація резервування мережі на території, на основі виконаних розрахунків та аналізу. Встановлення додаткового обладнання *OLT*, фідерних оптичних ліній та налагодження системи управління мережею, згідно з додаткових обладнанням (18 днів).
18. Підведення підсумків, щодо виконаного проекту (1 день).

3. Структура проекту, орієнтована на життєвий цикл:

1. Підготовка до виконання проекту (підготовчий етап): збір інформації з предметної області, знайомство з територією розміщення мережі, її характеристиками та технічними особливостями, затвердження плану, затвердження групи спеціалістів для виконання проекту, опис досліджуваної мережі та технології *PON*.
2. Початковий етап: розгляд основоположних понять необхідних для аналізу живучості, дослідження шкідливих факторів впливу на мережу та їх класифікація, ознайомлення з критеріями та показниками живучості мережі.
3. Етап аналізу: ознайомлення з методами та показниками живучості мереж, проведення порівняльного аналізу оптичних пасивних мереж, які побудовані згідно з різними топологіями, розрахунок показників живучості різних секторів досліджуваної мережі та проведення аналізу живучості секторів.
4. Етап реалізації проекту: ознайомлення з різними видами резервування та створення схем для кожного з них, створення рекомендацій для підвищення живучості розглянутої мережі, шляхом часткового резервування з боку центрального вузла, побудова функціональної схеми резервованої мережі, встановлення необхідного обладнання на території мережі, прокладення оптичних ліній доступу та налагодження системи управління мережею.
5. Заключний етап: завершення підготовки технічної документації проекту, створення декомпозиції проекту, задля успішного управлінням проектом, підбиття підсумків і завершення проекту.

4. Визначення навколишнього середовища та учасників проекту.

Навколишнім середовищем проекту вважається сукупність зовнішніх та внутрішніх факторів, що впливають на проект.

До зовнішніх факторів відносяться економічні та науково-технічні. На проект впливає вартість обладнання, яку треба приймати до уваги під час

створення рекомендацій щодо резервування мережі. Одним з важливих чинників є сучасний рівень розробок у сфері живучості мереж та взагалі телекомунікацій, а також законодавство у сфері інформаційних технологій.

Внутрішніми чинниками є зміни на ринку надання телекомунікаційних послуг та вдосконалення мереж доступу, а також постачальники оптичного обладнання.

Учасниками проекту є:

– керівник проекту;
– розробники;
– замовник;
– користувачі мережі доступу, яка аналізується;
– органи місцевого самоврядування.

5. Календарний план робіт проекту створено за результатами побудови та розрахунків параметрів і оптимізації його сітьової моделі. Календарний план наведено у табл. 4.2.

Таблиця 4.2.

Склад робіт проекту та їх тривалість

№ коду роботи	№ коду попередньої роботи	Найменування роботи	*T* (дні)
0-1	–	Збір інформації з предметної області та ознайомлення з характеристиками мережі, яка буде досліджуватися	15
1-2	0-1	Формування технічного завдання	7

Продовження таблиці 4.2.

№ коду роботи	№ коду попередньої роботи	Найменування роботи	*T* (дні)
2-3	1-2	Опис території мережі, особливостей її будови, окремих секторів, технічних характеристик мережі доступу та затвердження плану проекту	10
3-4	2-3	Ознайомлення з фаховою документацією та загальний опис технології *PON*	8
2-5	1-2	Розгляд основоположних понять для аналізу живучості	5
5-6	2-5	Дослідження шкідливих чинників, які можуть впливати на мережу, та шляхів захисту від них	5
6-7	5-6	Проведення класифікації шкідливих чинників, що діють на оптичні мережі доступу	2
5-8	2-5	Ознайомлення з критеріями та показниками живучості мережі доступу	4
8-9	5-8	Порівняльний аналіз методів та показників живучості мереж	9
7-10	6-7	Створення пояснювальної записки на основі проведеної роботи	17

Продовження таблиці 4.2.

№ коду роботи	№ коду попередньої роботи	Найменування роботи	*T* (дні)
9-10	8-9	Проведення порівняльного аналізу оптичних пасивних мереж, побудованих згідно з різними топологіями	8
10-11	7-10, 9-10	Розрахунок показників живучості різних секторів досліджуваної мережі та проведення аналізу живучості секторів	12
4-12	3-4	Розгляд різних видів резервування, для підвищення живучості мереж, та побудова схем резервування для кожного з них	7
11-13	10-11	Рекомендації щодо підвищення живучості досліджуваної мережі, шляхом часткового резервування з боку *OLT*	4
13-14	11-13	Створення функціональної схеми мережі	5
12-14	4-12	Перевірка та доробка пояснювальної записки та технічної документації	10

Продовження таблиці 4.2.

№ коду роботи	№ коду попередньої роботи	Найменування роботи	*T* (дні)
14-15	12-14, 13-14	Реалізація резервування мережі на території, на основі виконаних розрахунків та аналізу. Встановлення додаткового обладнання *OLT*, фідерних оптичних ліній та налагодження системи управління мережею, згідно з додатковим обладнанням	18
15-16	15-16	Підведення підсумків стосовно виконаного проекту	1

Спираючись на значення таблиці, було побудовано сітьовий графік, якийнаведено на рис. 4.2.

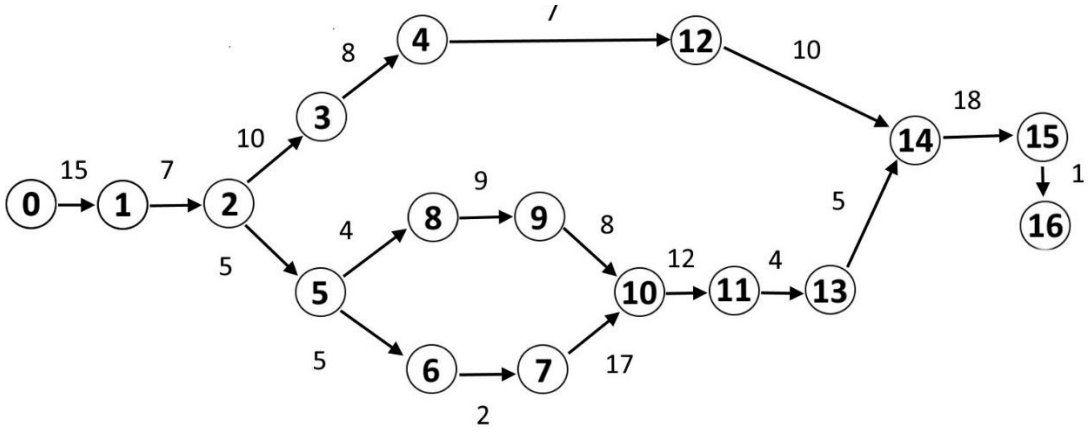

Рис. 4.2.– Сітьовий графік проекту

На наступному етапі слід розглянути тривалість проекту з прив’язкою дореального часу у таблиці 4.3 .

Таблиця 4.3.

Час реалізації проекту

№ попередньої роботи	№ фактичної роботи	Зміст роботи	Тривалість робіт	Виконавці
0	1	Збір інформації з предметної області та ознайомлення з характеристиками мережі доступу	11.08-25.08	Керівник проекту
1	2	Формування технічного завдання	25.08-02.09	Керівник проекту
2	3	Опис території мережі доступу та її особливостей, затвердження плану проекту	02.09-12.09	Керівник проекту, розробник
3	4	Ознайомлення з фаховою документацією та загальний опис технології *PON*	12.09-20.09	Розробник
2	5	Розгляд основоположних понять для аналізу живучості	02.09-07.09	Розробник

Продовження таблиці 4.3.

№ попередньої роботи	№ фактичної роботи	Зміст роботи	Тривалість робіт	Виконавці
5	6	Дослідження шкідливих чинників, які можуть впливати на мережу, та шляхів захисту від них	07.09-12.09	Розробник
6	7	Проведення класифікації шкідливих чинників, що діють на оптичні мережі доступу	12.09-14.09	Розробник
5	8	Ознайомлення з критеріями та показниками мережі	07.09-11.09	Розробник
8	9	Порівняльний аналіз методів та показників живучості мереж	11.09-20.09	Розробник
7	10	Створення пояснювальної записки на основі проведеної роботи	14.09-31.09	Керівник проекту, розробник

Продовження таблиці 4.3.

№ попередньої роботи	№ фактичної роботи	Зміст роботи	Тривалість робіт	Виконавці
9	10	Проведення порівняльного аналізу мережі, побудованих згідно з різними топологіями	20.09-28.09	Розробник
10	11	Розрахунок показників живучості різних секторів мережі, проведення аналізу живучості секторів	28.09-09.10	Розробник
4	12	Розгляд різних видів резервування, для підвищення живучості мереж, та побудова схем резервування для кожного з них	20.10-27.10	Розробник
11	13	Рекомендації щодо підвищення живучості мережі, шляхом часткового резервування з боку *OLT*	09.10-13.10	Розробник

Продовження таблиці 4.3.

№ попередньої роботи	№ фактичної роботи	Зміст роботи	Тривалість робіт	Виконавці
13	14	Створення функціональної схеми мережі	13.10-18.10	Розробник
12	14	Перевірка та доробка пояснювальної записки та технічної документації	27.09-06.10	Керівник проекту та розробник
14	15	Реалізація резервування мережі натериторії	18.10-06.11	Розробник
15	16	Підведення підсумків стосовно виконаного проекту	06.11-07.11	Керівник проекту та розробник

4.3 Вибір відповідного *Cloud Service Provider*

Amazon і *Google* обидва надають широкий спектр хмарних послуг через свої платформи *Amazon Web Services* (*AWS*) і *Google Cloud Platform* (*GCP*).

Amazon Web Services (*AWS*):

1. *Amazon EC2* (*Elastic Compute Cloud*): Надає вираховувальні ресурси у віртуальних серверах. Можливості масштабування і вибір різних типів інстанцій роблять його популярним серед користувачів.
2. *Amazon S3* (*Simple Storage Service*): Облачне сховище для зберігання та витягування будь-якого обсягу даних.

3. *Amazon RDS* (*Relational Database Service*): Управління реляційними базами даних, що дозволяє легко налаштовувати та масштабувати бази даних.
4. *AWS Lambda*: Сервіс для виконання коду без необхідності керування інфраструктурою. Ідеально підходить для реалізації *serverless* архітектури.
5. *Amazon VPC* (*Virtual Private Cloud*): Дозволяє створювати і управляти ізольованими просторами для обчислення у хмарі.

Google Cloud Platform (*GCP*):

1. *Google Compute Engine*: Надає вираховувальні ресурси у віртуальних машинах з можливостями масштабування та широким вибором типів інстанцій.
2. *Google Cloud Storage*: Сховище для зберігання та витягування об'ємних даних.
3. *Cloud SQL*: Управління реляційними базами даних, які легко розгортати та масштабувати.

Вибір між *AWS* та *GCP* в Україні:

1. Місце розташування даних: Важливо враховувати географічне розташування центрів обробки даних. *AWS* та *GCP* мають свої дата-центри в Європі, що може вплинути на швидкість доступу до послуг.
2. Ціна: Розрахунок вартості послуг включає в себе ціну за вираховувальні ресурси, зберігання даних, передачу даних та інші параметри. Перевірте тарифи для свого конкретного типу використання.
3. Підтримка та Інфраструктурна Цілісність: Обидва постачальники мають високий рівень підтримки, але *AWS* вже має довший термін функціонування та більшу кількість клієнтів.
4. Інновації та Машинне Навчання: *GCP* відомий своєю спеціалізацією в галузі машинного навчання. Якщо ваш проект включає в себе великі обчислення або роботу зі штучним інтелектом, це може бути важливим фактором.

5. Екосистема та Партнери: *AWS* має широку екосистему та велику кількість партнерів, що може полегшити інтеграцію та підтримку.

4.4 Маркетингове обґрунтуванням проекту

На заключному етапі обґрунтування доцільності впровадження проекту необхідно розглянути елементи майбутнього бізнес-плану його реалізації.

Ринок збуту та конкуренцію можна оцінити за такими параметрами:

- область використання даної продукції та регіон збуту: мережа доступу на основі технології *PON*, місто Одеса;
- коло потенційних споживачів: працівників та прилеглих підприємства, що розміщуються на вказаній території, провайдери послуг кабельного Інтернету;
- очікувані конкурентні переваги: надання провайдеру аналітичної інформації з дослідженням параметрів живучості обраної мережі та відповідними рекомендаціями щодо її підвищення; підвищення живучості мережі доступу, завдяки втіленню розроблених рекомендацій, що наддасть гарантії безперебійного та надійного доступу до всесвітньої мережі Інтернет як звичайним користувачам, так і підприємствам розміщеним на території, яку охоплює досліджувана мережа.

Стратегія маркетингу:

- проведення аналітичної роботи та виконання робіт з резервування згідно договору з провайдером;
- реклама серед компаній з надання телекомунікаційних послуг використовуючи паперові оголошення та рекламу в Інтернеті. Повідомлення місцевих компаній та провайдерів про удосконалення мережі доступу на основі проведених розрахунків та рекомендацій;
- ціни встановлюються беручи до уваги витрати на аналіз живучості мережі, розробку та впровадження рекомендацій з підвищення живучості мережі.

4.5 Розразухок науково-технічної ефективності

В умовах відкритої ринкової економіки розширюється діапазон оцінки ефективності науково-технічних розробок, а отже, збільшується кількість основних видів ефективності НДДКР, які необхідно визначити з метою цієї оцінки.

До них належать:

- Соціальний ефект: Створення такої мережі може покращити доступ до інформації та освіти у тих місцях, де це було важко. Це може призвести до більш рівного розподілу знань та освіти у суспільстві, а також підвищить рівень освіти загалом.
- Екологічний ефект: Використання тонких клієнтів дозволяє знизити кількість проводів та кабелів, необхідних для створення мережі. Це може знизити кількість відходів та зменшити вплив виробництва проводів на довкілля. Крім того, використання більш ефективної системи передачі даних може знизити споживання енергії та знизити викиди парникових газів.

Науково-технічну ефективність (НТЕ) результатів прикладних робіт визначають на основі показників науково-технічного рівня. Оцінка науково-технічної ефективності НДДКР відбувається на основі показникая ($О_{НТЕ}$), який представляє собою ступінь досягнення максимально можливого рівня, значення якого дорівнює 1 (одиниці):

$$\boldsymbol{O_{НТЕ} = K^{Ф}_{НТЕ} / K^{П}_{НТЕ},} \quad (4.1)$$

де

$К^{Ф}_{НТЕ}$ – показник (коефіцієнт) фактичного рівня науково-технічної ефективності;

$К^{П}_{НТЕ}$ – показник (коефіцієнт) потенціально можливого рівня науково-технічної ефективності (дорівнює одиниці).

Значення показника $К^{Ф}_{НТЕ}$ визначають на основі шкали експертних оцінок. Шкала експертних оцінок для виміру рівня науково-технічної ефективності проектів в таблиці 4.5.

Таблиця 4.5

Значення експертних оцінок

№	Групи показників	Характиристика показників	Інтервал рейтингового числа	Коефіцієнт значущості показників
1	Науково-технічний рівень	Ступінь науково технічного рівня тонких клієнтів	1-10	0.25
2	Перспективність	Можливість засто-сування в різних галузях	1-10	0.2
3	Потенційний масштаб практичного використання	Обсяг практичного застосування тонких клієнтів в галузі	1-10	0.3
4	Ступінь вірогідності досягнення позитивних результатів	Ймовірність успіш-ного впровадження тонких клієнтів на практиці	1-10	0.25

Примітка: об'єкт оцінки і аналог(и), які порівнюють за однаковими показниками, наведеними у співставленому вигляді відхилення в значеннях кожного з показників, мають бути однаковими для варіантів, що порівнюються.

4.6 Проведення оцінки науково-технічного рівня розробки

Визначають $К^{Ф}_{НТЕ}$ на основі експертної оцінки науково-технічного рівня розробки.

З цією метою:

- розроблюють перелік специфічних показників, необхідних для виміру науково-технічного рівня розробки;
- здійснюють відповідні розрахунки для співставлення показників і визначення балів по Таблиці 4.1.

До числа специфічних показників відносять:

- для нової техніки: продуктивність, споживання інженерних ресурсів на виробітку одиниці продукції, потреба в робочих, які обслуговують;
- для нових технологій: якість виробленої продукції, енергоємність і трудомісткість продукції, собівартість одиниці продукції.

Експертна оцінка і розрахунок величини інтегрального показника НТЕ в таблиці 4.6

Таблиця 4.6

Розрахунок величини

№	Групи показників	Рейтинг експертів			Середня за експертними оцінками	НТЕ
		1	2	3		
1	Науково-технічний рівень	8	7	9	8	2 (8 х 0,25)
2	Перспективність	9	9	8	9	3,15 (9 х 0,35)
3	Потенційний масштаб практичного використання	6	7	7	7,25	1,45 (7,25 х 0,20)
4	Ступінь вірогідності досягнення позитивних результатів	8	8	8	8	1,6 (8, х 0,20)
В С Ь О Г О						8,2

НТЕ = 8·0,25+9·0,35+7,25·0,20+8·0,20=2+3,15+1,45+1,6 = 8,2

Отриманий результат слід порівняти з максимально можливим значенням, яке дорівнює 10 балам (10·0,25 + 10·0,35 + 10·0,20 + 10·0,20).

На основі даних (Таблиці 4.6), можна дійти до висновку, що $К_{НТЕ}$ відповідає 82%, тобто

В тому випадку, коли значення КНТЕ перевищує середнє значення, яке дорівнює 5.0, має бути зроблено висновок про достатній рівень *НТЕ*:

- цілком достатній 5,0 – 6,0;
- достатній 6,1 – 8,0;
- достатньо високий 8,1 – 9,0;
- високий 9,1 – 10.

Таким чином, рівень *НТЕ* технології можна визнати достатнім. Отже, розроблену технологію пропонується впроваджувати у виробництво.

4.7 Розрахунок економічної ефективності проекту

Розрахунок економічної ефективності проекту – це процес визначення потенційного доходу та витрат проекту, а також оцінювання того, наскільки доцільно вкладати гроші у реалізацію проекту.

Для розрахунку економічної ефективності проекту необхідно визначити наступні показники:

1. Вартість проекту: це загальна вартість всіх витрат, пов'язаних з реалізацією проекту, включаючи затрати на розробку, впровадження та експлуатацію.
2. Прибуток від проекту: це дохід, отриманий від реалізації продукту або послуги, яку реалізовує проект.
3. Термін окупності: це період, за який витрати на реалізацію проекту повернуться від прибутку.
4. Рентабельність інвестицій (*PI*): це відношення чистого дисконтованого доходу до вартості інвестицій.

Витрати на експлуатацію системи були розраховані в розмірі 10 000 грн на рік. Вони включають витрати на оплату праці фахівців, витрати на електроенергію, водопостачання та інші незначні витрати.

Очікувана прибутковість від проекту була оцінена в розмірі 150 000 грн на рік. Цей показник було розраховано на основі досліджень ринку та конкурентного середовища.

Проведемоо розрахунок:

Ціна = 100 000 грн + 150 000 грн * 30% = 145 000 грн

Підставляю свої значення:

Рентабільність проекту дорівнює R = 104%

Час, за який проект окупиться дорівнює T = 0,9 року або 11 місяці.

Отже, проект мережі доступу на базі технології з витратами 100000 грн та очікуваним прибутком 150000 грн при реалізації за ціною 145 000 грн матиме рентабільність 104% і буде окупатися за 11 місяців.

Висновок до четвертого розділу

Вибір *Amazon Web Services* (*AWS*) для наших потреб виявився оптимальним і відповідає нашим вимогам. *AWS* пропонує широкий спектр послуг, які відповідають нашим потребам у вирахувальних ресурсах, зберіганні даних, управлінні базами даних, інфраструктурному віртуалізації та іншим аспектам облачних технологій.

Обрані сервіси, такі як *Amazon EC2* для вирахувальних ресурсів, *Amazon S3* для зберігання даних та *Amazon RDS* для управління базами даних, відповідають нашим вимогам до масштабованих, безпечних та надійних хмарних рішень. *AWS* також надає нам можливість ефективно використовувати послуги іншого напрямку, такі як машинне навчання та аналітика.

Гнучкість, широка географічна розгалуженість центрів обробки даних, та високий рівень безпеки і підтримки - це додаткові фактори, які роблять *AWS* оптимальним вибором для нашого бізнесу.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

При виконанні монтажних робіт із прокладки мереж, працівник зіштовхується з небезпекою отримання різного роду травм, будь то механічні травми від обертових частин електроінструмента, електротравми від пробою ізоляції в електроінструменті або опіки від нагрітих у процесі роботи електроінструментів і продуктів їхньої обробки.

5.1 Характеристика приміщення

Під час планування будівлі варто врахувати три головні речі:

- місце знаходження сервера;
- місце знаходження маршрутизаторів;
- місце знаходження робочих місць співробітників.

З урахуванням цих пунктів і їх положення ми повинні побудувати мережу. Місце знаходження сервера. Серверам виділяють окрему кімнату з хорошою вентиляцією і резервним живленням. Але в практиці сервер знаходиться в офісі адміністратора або адміністраторів які мають як і фізичний доступ до нього так і віддалений по мережі.

Варто приділити увагу на максимальній відстані тонкого клієнта від сервера ця довжина становить 35 метрів. Це обмеження виправляється простою установкою репітера або додаткового маршрутизатора.

Відразу ж видно, чому мережу тонких клієнтів варто планувати під час планування будівлі: це допомагає скоротити витрати на репітери і маршрутизатори. Кращий спосіб розміщення мережі це використовувати топологію «зірка», що дозволить ділити офіси і розширювати мережу.

Місцезнаходження маршрутизатора. Ці пристрої відповідають за передачу інформації для тонких клієнтів. Які дуже вразливі до енергійних перепадів і

грозових атакам. Варто приділити увагу покупці маршрутизатора з урахуванням захисту від електричних перепадів.

Маршрутизатор знаходитися далеко від співробітників і мати резервне живленням. Краще місце для нього може бути під стелею або в стінці у ящику ключ від якого може бути у адміністраторів.

Виділення окремого живлення потрібно для підтримки мережі під час критичних ситуацій.

Місцезнаходження робочих місць співробітників. Ми вже уточнили що мережу буде розроблено топологією «Зірка», так що розміщення робочих місць варто виділяти біля маршрутизатора, що дасть можливість зручно встановити патч-корди для тонких клієнтів.

Так само не варто забувати про резервне живлення, що дасть можливість зберегти проекти під час перебоїв живлення.

5.2 Техніка безпеки

Небезпечні фактори при монтажних роботах. При прокладці телекомунікацій в офісних приміщеннях монтажник виконує роботу як ручним, так й електроінструментом.

Роботи, виконувані електроінструментом:

- перфорування отворів у бетонних і цегельних стінах;
- штроблення каналів у бетонних і цегельних стінах;
- обрізка кабельних каналів;
- свердлення отворів у легких перегородках (гіпсокартон, ДСП);
- загортання шурупів і гвинтів.

При цьому він користується наступним інструментом: дриль, перфоратор, кутова шліфувальна машинка, шуруповерт.

У перерахованого інструмента є обертові частини, які можуть нанести механічну травму. Крім того, при виконанні перерахованих вище робіт утворяться стружка, пил, осколки оброблюваної поверхні. Вони можуть поранити шкірні покриви, очі, дихальні шляхи. Також існує небезпека

електротравм як від пробою ізоляції в електроінструменті, так і при виникненні короткого замикання у випадку ушкодження схованої електропроводки. Не варто забувати про шуми й вібрацію, які супроводжують роботі даним інструментом. При роботі електроінструмент і продукти його обробки можуть нагріватися й, отже існує небезпека термічних травм (опіків).

Роботи, виконувані ручним інструментом:

- забивання в отвори пластикових пробок і дюбелів;
- обрізка кабелю;
- зачищення кабелю від ізоляції;
- обтиск проводів у технологічні клеми.

При виконанні даних робіт монтажник користується наступним ручним інструментом: викрутка, молоток, пасатижі, гострозубці, бокорізи, пристосування для зачищення й обрізки кабелю. У перерахованого інструмента є гострі ріжучі крайки, об які можна порізатися.

5.3 Електробезпека

Для правильної побудови й експлуатації мережі бажано знати термінологію й розуміти основні принципи роботи мережі 220/380 Вольтів. Хоча потрібно враховувати, що строго говорячи, це прерогатива людей, що мають спеціальні знання й дозволи. А будь-які самостійні дії можуть бути пов’язані з реальним ризиком для життя.

Всі роботи, пов’язані із прокладкою й обслуговуванням електричних мереж, повинні виконуватися тільки кваліфікованим електротехнічним персоналом з відповідною групою допуску електробезпечності!

Даний матеріал опирається на Правила пристрою електроустановок (ПУЕ), які є головним документом, що регламентує питання електричних мереж.

Електричні установки, до яких відноситься практично всі офісна оргтехніка, надає для людини можливу небезпеку, оскільки в процесі експлуатації або проведення профілактичних робіт людина може торкнутися частин, що перебувають під напругою. Проходячи через людину, електричний

струм впливає на неї складним чином, викликаючи електричний, електролітичний, механічний й біологічний вплив. Кожен з перерахованих впливів струму може призвести до електричної травми, тобто ушкодженню організму, викликаному впливом електричного струму або дуги (ГОСТ 12.1.009-776).

Умови електробезпечності залежать і від параметрів навколишнього середовища виробничих приміщень - вологість, температура й так далі. Винятково важливе значення для припинення електротравматизму має правильна організація обслуговування діючих електроустановок, тобто суворе виконання ряду організаційних і технічних заходів, установлених «Правилами технічної експлуатації електроустановок споживачів» й «Правилами техніки безпеки при експлуатації електроустановок споживачів» (ПТЕ й ПТБ).

Для попередження поразки електричним токовищем при експлуатації електроустановок використають технічні засоби захисту, до яких відносять:

- електричну ізоляцію струмоведучих частин;
- захисне заземлення;
- занулення;
- вирівнювання потенціалів;
- захисне відключення;
- електричний поділ мережі;
- мала напруга;
- подвійну ізоляцію.

Фізичний зміст ізоляції як захисної міри, полягає в обмеженні значення сили струму, що протікає через тіло людини при різних обставинах, що виникають у процесі експлуатації встаткування. В електроустановках до 1 кВ, мінімальне значення опору ізоляції повинне бути не менш 0,5 МОм. Захисне заземлення - це основна технічна міра, застосовувана в мережах з ізольованою нейтраллю. Під ним розуміють навмисне електричне з'єднання з «землею» або її еквівалентом металевих неструмоведучих частин, які можуть виявитися під

напругою. Всі підлягаючі заземленню елементи ЕОМ приєднують до контурушини окремими заземлюючими провідниками.

У мережах напруги до 1 кВ захист персоналу від поразки електричним струму здійснюється зануленням. Зануленням називається навмисне електричне з'єднання з нульовим захисним провідником металевих неструмоведучих частин, які можуть виявитися під напругою (ГОСТ 12.1.009-76).

Захист відключенням являє собою швидкодіючий захист, що забезпечує автоматичне відключення електроустановки від мережі при виникненні в ній небезпеки поразки людини токовищем (ГОСТ12.4.155-85). Захисне відключення може застосовуватися як самостійний захисний засіб, так і разом із заземленням і із зануленням.

Згідно ГОСТ 12.1.019-79 під електробезпекою розуміють систему організаційних і технічних заходів і засобів, що забезпечують захист людей від шкідливого і небезпечного впливу електричного струму, електричної дуги і статичної електрики. На відміну від інших джерел небезпеки, електричний струм не можна виявити без спеціального обладнання та приладів, тому вплив його на людину найчастіше несподіваний.

Проходячи через організм людини, електричний струм робить можливим функціонування нервової системи та м'язів, оскільки електричні сигнали передаються по нервових волокнах, а також скорочення м'язів відбувається завдяки електричній активності. Однак при сильному впливі електричного струму на організм людини можуть виникнути небезпечні наслідки, такі як серцева аритмія, опіки, пошкодження органів і тканин. Тому, використовуючи електрику, необхідно дотримуватися всіх необхідних запобіжних заходів і безпеки. В результаті термічного впливу здійснюється розігрів організму і виникають опіки ділянок тіла, в результаті електролітичного впливу розкладається кров і інші органічні рідини в організмі. Біологічний вплив проявляється в порушенні і роздратуванні тканин і мимовільному судорожному скороченні м'язів.

Основною причиною отримання трав від напруги є:

- контакт з оголеними проводами;
- взаємодія з комплектуючими комп'ютера;
- використання не справного обладнання;
- несправність захисних засобів, якими потерпілий стосувався струмоведучих частин;
- несподіване виникнення напруги через пошкодження ізоляції там, де в нормальних умовах його бути не повинно;
- замикання фаз на землю тощо;
- поява напруги на струмопровідних частинах обладнання в результаті помилкового включення тоді, коли на ньому виконують роботу.

Експлуатація комп'ютерної мережі передбачає використання ПК в якості пристроїв доступу до неї. Джерелом напруги живлення ПК і *Wi-Fi*-роутерів є мережа змінного струму з напругою 220 В, на яку поширюється ГОСТ 25861-83. Згідно з вимогами для попередження уражень струмом необхідно:

- чітко і в повному обсязі виконувати правила виконання робіт і правила технічної експлуатації;
- виключити можливість доступу оператора до частин обладнання, що працює під небезпечною напругою, неізольованих частин, призначеним для роботи при малому напрузі і не підключеним до захисного заземлення;
- застосовувати ізоляцію, служить для захисту від ураження електричним струмом, виконану із застосуванням міцного суцільного або багатошарового ізоляційного матеріалу, товщина якого обумовлена типом забезпечується захисту;
- підводити електроживлення до ПК від розетки будівлі за допомогою спеціальної вилки з занулюючим контактом;
- захистити від перевантажень по струму, розраховуючи на потужність, споживану від мережі; а також захистити від короткого замикання обладнання, вбудоване в мережу будинку;

- надійно підключити до заземлюючих затискачів металеві частини, доступні для оператора, які в результаті пошкодження ізоляції можуть опинитися під небезпечною напругою;
- перевірити, що захисний заземлювальний провідник не має вимикачів і запобіжників, а також надійно ізольований.

Мікроклімат в офісі. Згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» встановлено такі норми допустимих параметрів мікроклімату для робіт в офісних приміщеннях (категорія робіт – легка 1а): під час холодного періоду року температура повітря повинна бути не менше +21-25 °С, а температура поверхонь не менше + 19-24 °С; відносна вологість повітря до 75% зі швидкістю руху повітря 0,1 м/*с*.

В літній сезон температура приміщення повинна бути в межах + 22-28 °С, температура поверхонь не вище + 19-24 °С, відносна вологість повітря 40-60 %, а швидкість руху повітря 0.1 м/*с*. З цим кліматом може стабільно працювати сервер та співробітники.

Висновок до п'ятого розділу:

В результаті проведеного дослідження, присвяченого монтажним роботам під час прокладання мереж, можна зробити низку висновків щодо безпеки та ефективності процесу. Практичні аспекти монтажних робіт, пов'язані з ризиками отримання різних травм.

Правильне планування та облік особливостей розташування обладнання дозволяють знизити ризики травм та забезпечити ефективну та безпечну роботу мережевої інфраструктури.

ЗАГАЛЬНІ ВИСНОВКИ

При розробці дипломної роботи було на прикладі показано створення і оптимізація цієї мережі. На даний момент це оптимальне рішення для нових підприємств та гарна оптимізація вже для фінансових гігантів. Так як ця мережа вимагає особливого догляду адміністратор зможе підтримувати стабільність роботи сервера для все користувачів і так-же невід'ємним плюсом є те, що ця мережа може бути обслужена з дому використовую віддалений доступ. Купівля клієнтів від фірми дасть можливість швидко виправити технічні помилки.

У першій частині диплома ми побачили різноманітність топологій і способів будови мережі що дало нам чітке розуміння як наша мережа буде влаштована і як прокладена.

У другій частині було приділено увагу до основних вимог мережі для її установки в будівлі. І до основних принципів роботи мережі і протоколів щоб було приблизне поняття про роботу мережі.

У третій частині буквально по слайдом був розібраний процес створення мережі, так само було приділено увагу на основні помилки які часто з'являються при створенні мережі.

Цей дипломний проект дав мені чітке уявлення, що з себе представляє віртуалізація мереж, її плюси і мінуси.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. С.М. Платунова Адміністрування мережі в *windows server* 2012.
2. Посібник з технологій об’єднання мереж 4-е видання. *Cisco Systems*, 2005. -1040 с.
3. Т.Т. Газизов Інформаційні мережі, Віртуалізація мережі. *URL*: *https://koi.tspu.ru/koi_books/gazizov2/6_Virtyalnie_localnie_ceti.htm* (дата звернення: 30.01.2023).
4. Пролетарський А.В. (ред.) - Технології комутації та маршрутизації в локальних комп'ютерних мережах (Комп'ютерні системи та мережі) – 2013.
5. Практичне керівництво для адміністраторів і професійних користувачів / Мауфер Т. 2005.
6. Мережі ЕОМ і телекомунікації / В.К. Мищенко. Курс лекцій, 2004 р. *Building Wireless Community Networks. Help for Network Administrators / Rob Flickenger. - O’Reilly Publishing*, 2002.
7. Практичне керівництво для адміністраторів і професійних користувачів / Мауфер Т. 2005.
8. Закон України «Про Національну програму інформатизації». URL: *https://zakon.rada.gov.ua/laws/show/74* (дата звернення: 22.11.2022).
9. Закон України «Про Концепцію Національної програми інформатизації». *URL*: *https://zakon.rada.gov.ua//laws/show/75/98-вр* (дата звернення: 30.01. 2023).
10. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». *URL*: *https://zakon.rada.gov.ua/laws/z0508-18* (дата звернення: 30.01.2023).
11. Додонов О. Г., Ланде Д.В. Живучість інформаційних систем. – К.: Наук. думка, 2011. – 246 с.

12. Мар’їна О. Контент-стратегія бібліотек у цифровому середовищі Бібліотечний вісник. 2016. №4. С.8–12. *URL: http://nbuv.gov.ua/UJRN//bv_2016* (дата звернення: 30.01.2023).

13. Додонов О.Г. До питання живучості корпоративних інформаційних систем / О.Г. Додонов, Д.В. Флейтман //, Київ, 2004, – 130 с.

14. Вігуржинська С.Ю., Колесник В.І. Дипломне проектування економічної частини проекту: Методичні вказівки для студентів, що навчаються за спеціальностями 05010101 – «Інформаційні управляючі системи та технології»; 05010102 – «Інформаційні технології проектування»; 05010201 – «Комп’ютерні системи та мережі»; 05010203 – «Спеціалізовані комп’ютерні системи» / С.Ю. Вігуржинська, В.І. Колесник. – Одеса: НВЦ ОНАХТ «Технолог», 2016. – 23 с.

15. Сахарова С.В., Соломицький М.Ю., Барабаш Т.М. Системи доступу користувача. Частина перша. Розробка мережі доступу користувача: Методичні вказівки до курсового проектування / С.В. Сахарова, М.Ю. Соломицький, Т.М. Барабаш. – Одеса: 2018. – 47 с.

ДОДАТКИ

Додаток А Графічний матеріал

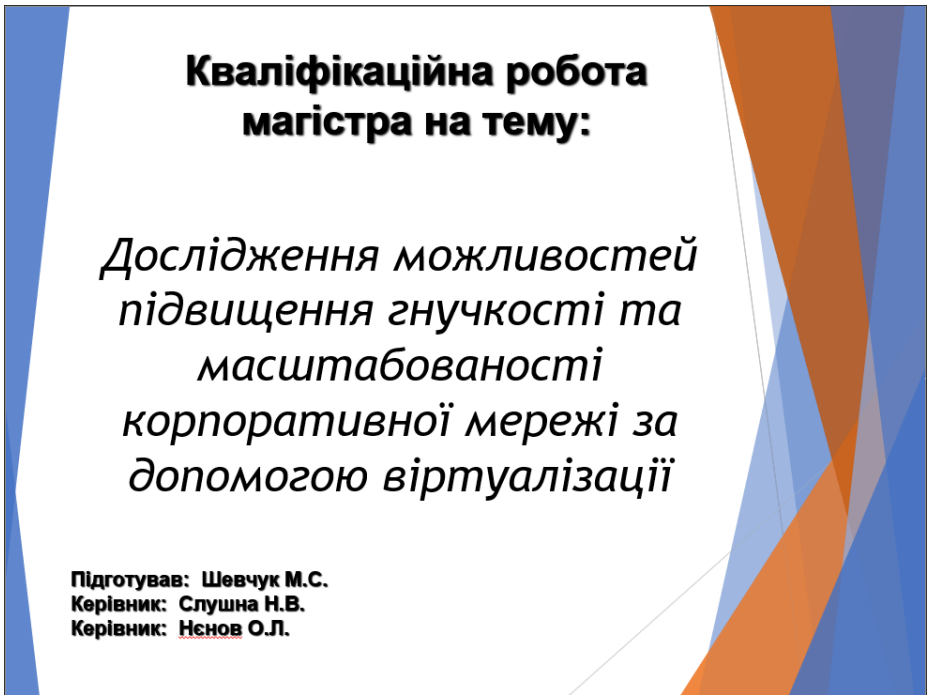

Рисунок А.1 – Слайд №1

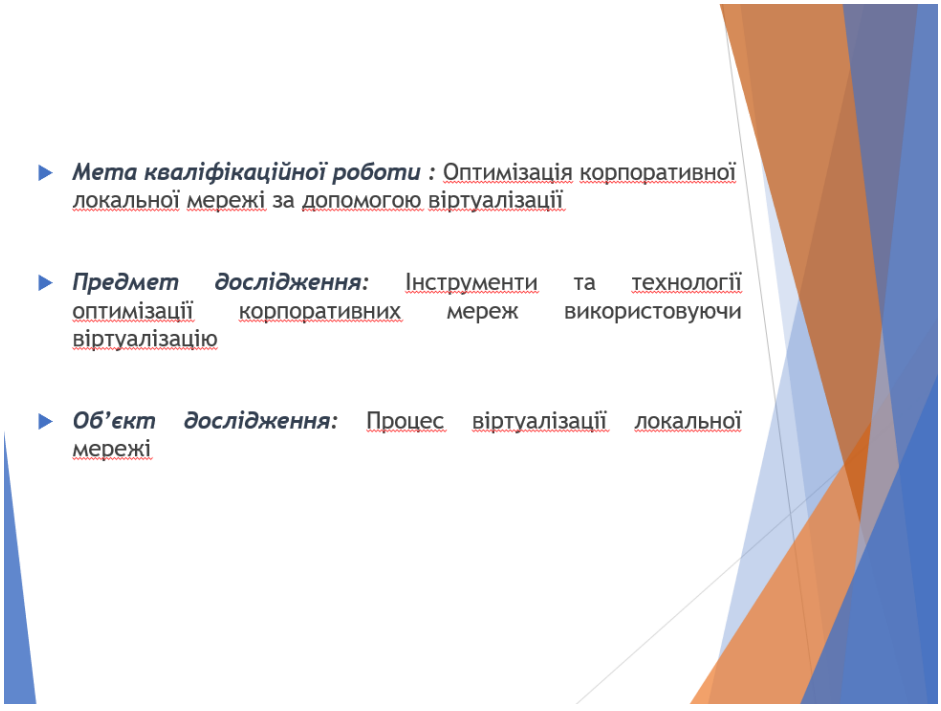

Рисунок А.2 – Слайд №2

Головні поняття

- ***Віртуалізація мереж*** *- це одне з рішень, що дозволяє значно підвищити гнучкість та масштабованість корпоративних мереж, а також покращити їх продуктивність та надійність. Віртуалізація дозволяє об'єднати ресурси декількох серверів у єдине віртуальне середовище, де ресурси можуть бути ефективніше розподілені та керовані. Це може суттєво скоротити витрати на обладнання та експлуатацію мережі.*

- ***Cloud Service Provider, CSP*** *- це компанія або організація, яка надає доступ до хмарних обчислювальних ресурсів, таких як віртуальні сервери, зберігання даних, мережеві ресурси та інші сервіси через Інтернет.*

Рисунок А.3 – Слайд №3

Віртуальна мережа

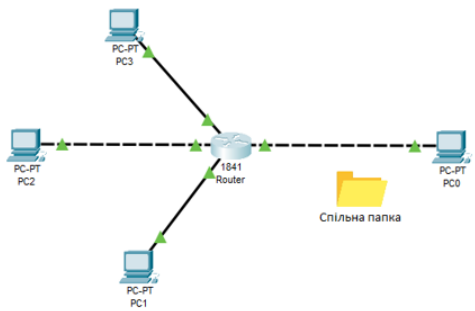

Рисунок А.4 – Слайд №4

Рисунок А.5 – Слайд №5

Рисунок А.6 – Слайд №6

Віртуальна мережа

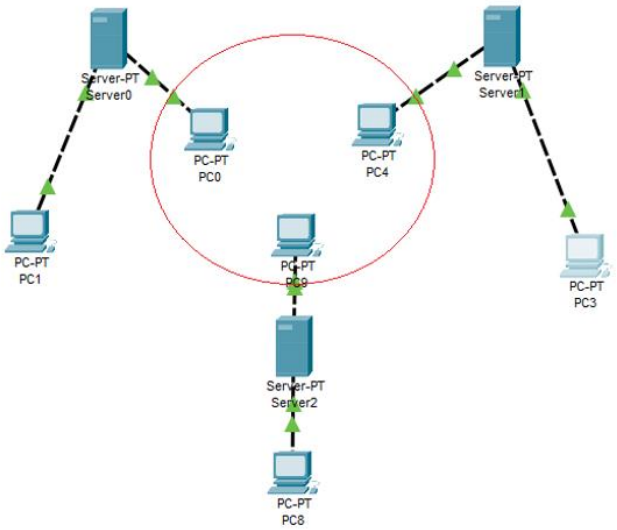

Рисунок А.7 – Слайд №7

Висновки

При розробці дипломної роботи на прикладі показано оптимізацію та працездатність цієї мережі. Дана мережа - оптимальне рішення для нових підприємств та офісних центрів. Цей дипломний проект дав мені ясне уявлення, що являють собою віртуальні мережі та постачальники хмарних послуг.

Рисунок А.8 – Слайд №8

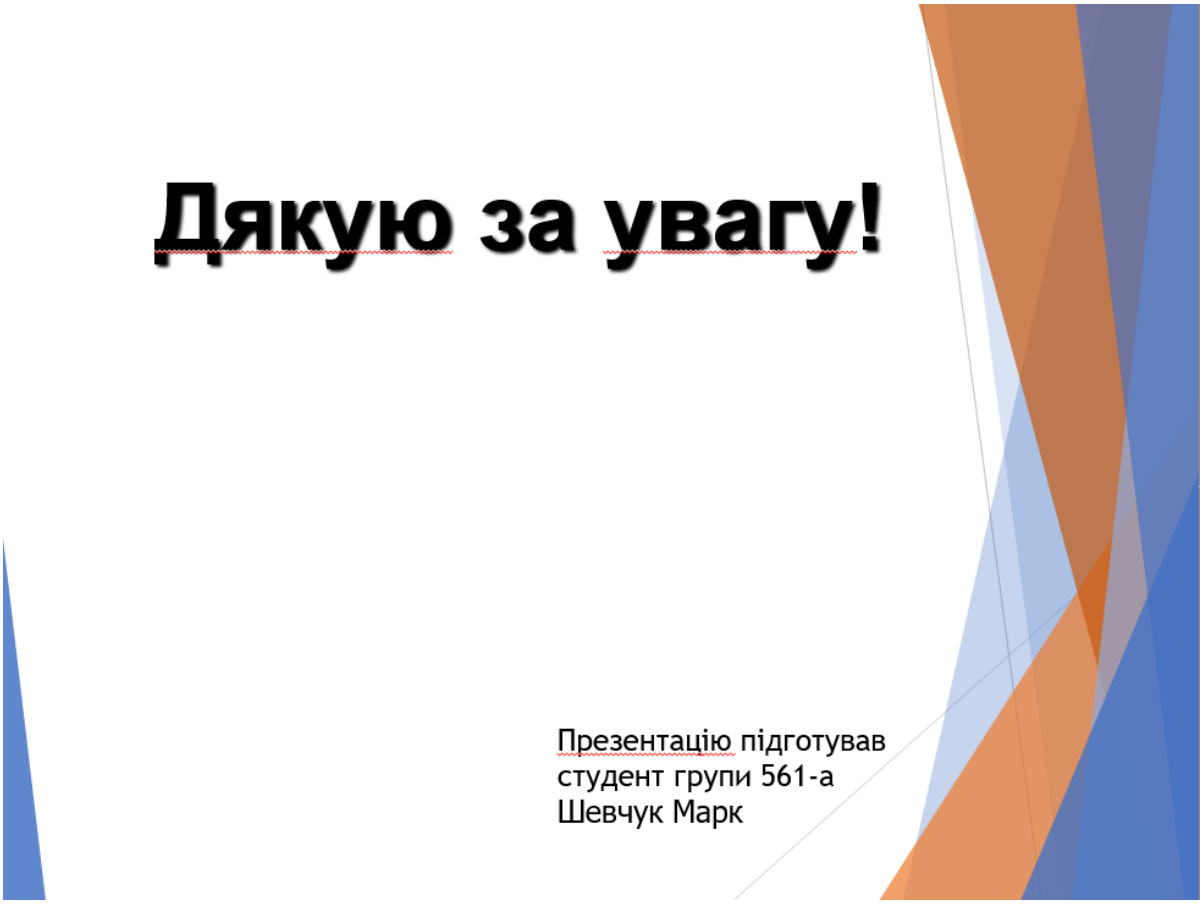

Рисунок А.9 – Слайд №9