

Міністерство освіти і науки України  
 Національний технічний університет  
 «Дніпровська політехніка»  
Навчально-науковий інститут  
електроенергетики  
 (інститут)

Факультет інформаційних технологій  
 (факультет)

Кафедра інформаційних технологій та комп'ютерної інженерії  
 (повна назва)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**  
**кваліфікаційної роботи ступеня бакалавра**

**студента** Підплетька Андрія Васильовича  
 (піб)

**академічної групи** 123-19з-1  
 (шифр)

**спеціальності** 123 Комп'ютерна інженерія  
 (код і назва спеціальності)

**за освітньо-професійною програмою** 123 Комп'ютерна інженерія  
 (офіційна назва)

**на тему** “Комп'ютерна система дніпровської філії мережі магазинів електроніки ТОВ»АЛЮ»з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі..

(назва за наказом ректора)

| Керівники                     | Прізвище, ініціали | Оцінка за шкалою |               | Підпис |
|-------------------------------|--------------------|------------------|---------------|--------|
|                               |                    | рейтинговою      | інституційною |        |
| кваліфікаційної роботи        | доц.Ткаченко С.М   |                  |               |        |
| розділів:                     |                    |                  |               |        |
| розробка апаратної частини    | доц. Бешта Д.О.    |                  |               |        |
| розробка корпоративної мережі | ас. Панферова Я.В. |                  |               |        |

|                  |  |  |  |  |
|------------------|--|--|--|--|
| <b>Рецензент</b> |  |  |  |  |
|------------------|--|--|--|--|

|                       |                    |  |  |  |
|-----------------------|--------------------|--|--|--|
| <b>Нормоконтролер</b> | проф. Цвіркун Л.І. |  |  |  |
|-----------------------|--------------------|--|--|--|

Дніпро  
 2023

**ЗАТВЕРДЖЕНО:**  
завідувач кафедри

2

інформаційних технологій

та комп'ютерної інженерії

(повна назва)

\_\_\_\_\_ Гнатушенко В.В.  
(підпис) (прізвище, ініціали)  
\_\_\_\_\_ квітня 2023 року

**ЗАВДАННЯ**  
**на кваліфікаційну роботу ступеня**  
**бакалавр**

**студента** Підплетька А.В.

(прізвище та ініціали)

**академічної групи** **123-19з-1**

(шифр)

**спеціальності** 123 «Комп'ютерна інженерія»

**за освітньо-професійною програмою інженерія»** 123 «Комп'ютерна інженерія»

(офіційна назва)

**на тему** «Комп'ютерна система дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 №256-с

| Розділ                              | Зміст  | Термін виконання |
|-------------------------------------|--|------------------|
| Стан питання та постановка завдання | Комп'ютерна система ТОВ «АЛЛО». З'ясувати принципи та структуру системи управління мережею підприємства. Запропонувати план програмної реалізації системи управління мережею підприємства. | 10.05.2023       |
| Розробка апаратної частини          | Розробка, технічні вимоги, розробка апаратної частини системи та загальної архітектури мережі підприємства.  | 17.05.2023       |
| Розробка корпоративної мережі       | Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, її безпека та функціонування.   | 24.05.2023       |
| Розробка компонента системи         | Хмарна реалізація захисту корпоративної мережі ТОВ «АЛЛО», рекомендації по захисту віртуалізованих середовищ.  | 31.05.2023       |

**Завдання видано**

\_\_\_\_\_

(підпис керівника)

доц. Ткаченко С.М.

(прізвище, ініціали)

Дата видачі 11.04.2023

Дата подання до екзаменаційної комісії

14.06.2023

**Прийнято до виконання**

\_\_\_\_\_

Підплетько А.В.

## Реферат

Пояснювальна записка: 97 с., 54 рис., 40 табл., 6 дод., 33 джерел.

ПРИНЦИПИ, РОЗРОБКА, АПАРТНА ЧАСТИНА,  
ВИБІР І ОБҐРУНТУВАННЯ, КОРПОРАТИВНА МЕРЕЖА,  
БЕЗПЕКА, VLAN, ХМАРНА РЕАЛІЗАЦІЯ ЗАХИСТУ

Об'єкт розробки – Комп'ютерна система дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи – створення комп'ютерної системи дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Розглянуто основні принципи побудови та діяльності компанії.

Розкрито основні поняття та організацію системи управління мережею підприємства.

Сформульовано методичні пропозиції щодо забезпечення ефективної роботи системи управління мережею підприємства.

Розроблена комп'ютерна система може бути застосована та використана в діяльності Дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО». Ці дії включають налаштування, створення та захист корпоративної мережі.

Розроблена мережа виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Результати перевірки наведені у вигляді таблиць та графіків, також вони наводяться у пояснювальній записці та додатка

## Зміст

|   |           |
|---|-----------|
| <b>Перелік скорочень, умовних познач, одиниць і термінів</b>  | <b>6</b>  |
| <b>Вступ</b>  | <b>7</b>  |
| <b>1 Стан питання і постановка завдання</b>   | <b>10</b> |
| 1.1 Характеристика підприємства та умов застосування КС   | 10        |
| 1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства                 | 10        |
| 1.3 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань | 12        |
| 1.4 Розробка схеми організаційної структури підприємства  | 17        |
| 1.5 Постановка завдання   | 21        |
| <b>2 Розробка апаратної частини комп'ютерної системи підприємства</b>   | <b>24</b> |
| 2.1 Технічні вимоги до комп'ютерної системи   | 24        |
| 2.1.1 Вимоги до системи в цілому  | 24        |
| 2.1.1.1 Вимоги до структури і функціонуванню системи  | 24        |
| 2.1.1.2 Показники призначення   | 24        |
| 2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню                               | 24        |
| 2.1.1.4 Вимоги до патентної чистоти   | 25        |
| 2.1.2 Вимоги до функцій, які виконує КС   | 25        |
| 2.1.3 Вимоги до видів забезпечення КС   | 26        |
| 2.1.3.1 Вимоги до інформаційного забезпечення   | 26        |
| 2.1.3.2 Вимоги до програмного забезпечення  | 26        |
| 2.2 Розробка апаратної частини комп'ютерної системи   | 27        |

|  |           |
|--|-----------|
| 2.2.1 Розробка топологічної схеми розміщення структурних підрозділів підприємств               | 27        |
| 2.2.2 Розробка загальної архітектури мережі підприємства                                       | 32        |
| 2.2.3 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи | 32        |
| 2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства      | 39        |
| <b>3 Розробка корпоративної мережі</b>   | <b>42</b> |
| 3.1 Розрахунок схеми адресації корпоративної мережі  | 42        |
| 3.2 Розробка топологічної схеми корпоративної мережі   | 43        |
| 3.3 Розрахунок налаштувань маршрутизації корпоративної мережі                                  | 59        |
| 3.4 Налаштування та перевірка роботи комп'ютерної системи                                      | 63        |
| 3.4.1 Базове налаштування конфігурації пристроїв Cisco базові команди та налаштування          | 63        |
| 3.4.2 Налаштування маршрутизаторів корпоративної мережі  | 64        |
| 3.4.3 Налаштування роботи Інтернет   | 66        |
| 3.4.4 Перевірка роботи комп'ютерної системи  | 68        |
| 3.5 Захист інформації в комп'ютерній системі від несанкціонованого доступу                     | 70        |
| 3.5.1 Розробка методів для захисту інформації в комп'ютерній системі                           | 70        |
| 3.5.2 Налаштування мереж VLAN  | 71        |
| 3.5.3 Налаштування параметрів безпеки комутаторів  | 72        |
| <b>4 Розробка компонента системи</b>   | <b>75</b> |
| 4.1 Хмарна реалізація захисту корпоративної мережі   | 75        |
| 4.2 Рекомендації захисту віртуалізованих середовищ в публічній хмарі                           | 86        |
| <b>Висновки</b>  | <b>92</b> |
| <b>Перелік посилань</b>  | <b>94</b> |

## **Перелік скорочень, умовних познач, одиниць і термінів**

ЕОМ – Електронно-обчислювальна машина

ПК – Персональний комп'ютер

КМ – Корпоративна (комп'ютерна) мережа

ЛКМ – Локальна комп'ютерна мережа

ОС – Операційна система

ПЗ – Програмне забезпечення

СЗІ – Система захисту інформації

СУБД – Система управління базами даних

ТОВ – Товариство з обмеженою відповідальністю

## Вступ

**Актуальність дослідження.** Сьогодні розвиток комп'ютерної мережі має значний вплив на діяльність практично кожного підприємства. В результаті він використовується для спілкування між співробітниками в офісі (підприємстві, будівлі), а також між спільнотами в різних містах або країнах. Ефективне управління підприємством неможливе без постійного контролю за інформаційним потоком, без безпосередньої оперативної координації діяльності підрозділів і співробітників.

Як правило, усі, за винятком небагатьох компаній будь-якого профілю, вже мають комп'ютери та офісне обладнання, але якщо процес їх придбання та встановлення відбувався нерегулярно, то, як правило, його ефективність і завершеність були б знижені. Крім того, в існуючих мережах захист інформації не є пріоритетним. Будь-яка організація складається з взаємопов'язаних структурних компонентів (підрозділів), кожен з яких може мати свою унікальну характеристику. Компоненти пов'язані функціями та інформацією, тобто кожен з них служить окремій меті в контексті одного бізнес-процесу. Крім того, ці компоненти взаємодіють з іншими системами, і їх взаємодія також може бути як інформаційною, так і функціональною.

У міру зростання та розвитку організації її керівництво неминує захоче створити найбільш гнучку та ефективну систему управління мережею всього підприємства, а також його складових частин.

Важливо визнати, що для організацій, які мають багато віддалених філій і підприємств, правильне вирішення цих питань допоможе успішно управляти компанією, скоротити часові та фінансові витрати. Світовий досвід великих корпорацій і компаній свідчить про те, що таким рішенням є створення єдиної інформаційної системи, яка базується на корпоративній мережі.

Як відомо, в умовах множинних інформаційних потоків, які з кожним роком зростають, без сучасних комп'ютерів та комп'ютерних мереж майже неможливо уявити безпосередню взаємодію між банківськими установами, торговими компаніями, державними установами та іншими організаціями. В іншому випадку довелося б залучити великий штат спеціалізованих процесорів документів і кур'єрів, а надійність і швидкість системи все ще залежали б від зв'язку, який надається за нижчою швидкістю, і комп'ютерних мереж. Зрештою, кожна хвилина затримки в передачі важливої інформації може призвести до значних фінансових збитків.

Останнім часом ідея динамічного адміністрування все частіше документується в зарубіжній літературі. Його дизайн відповідає загальній моделі мережевого та системного адміністрування - перехід від контролю окремих ресурсів до більш цілеспрямованого підходу до управління запитами інформаційних технологій і задоволення цих запитів. Цей метод передбачає наявність інструментів, які можуть аналізувати поведінку користувачів. Отримані на цьому етапі результати повинні слугувати основою для адміністрування взаємодії між основними об'єктами адміністрування – користувачами, додатками та мережею. Термін «активний» означає постійне спостереження за поведінкою користувальницьких додатків і оперативну реакцію на цю поведінку, якщо очікуваний користувачем рівень обслуговування не досягається. Для найбільш ефективного реагування на виникаючі проблеми прихильники концепції активного адміністрування виступають за використання аналітичних інструментів підтримки прийняття рішень.



**Метою дослідження** є створення комп'ютерної системи дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

**Практичне значення дослідження** полягає в тому, що розроблена комп'ютерна система дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі може бути практично реалізованою та використовуватися в його діяльності.

## **1 Стан питання і постановка завдання**

### **1.1 Характеристика підприємства та умов застосування КС**

Мережа магазинів роздрібної торгівлі електроніки ТОВ «АЛЛО» є організацією, що надає різного роду інформацію. Ця інформація надається у кількох видах, наприклад: інформація для бухгалтерії (співробітники, купівля-продаж продукції), електронний перелік продукції, ресурси Інтернету.

Діяльність мережі магазинів електроніки ТОВ «АЛЛО» можна умовно розділити на завдання купівлі-продажу електроніки та роботу бухгалтерії.

Ці завдання включають оперативність отримання інформації про покупців, інформацію про співробітників організації.

Також кожен відвідувач може, користуючись послугами інтернету, переглядати продукцію в наявності, замовляти продукцію, надсилаючи свою заявку на поштову адресу організації.

Таким чином, для нормального функціонування мережі магазинів електроніки ТОВ «АЛЛО» необхідна оперативна взаємодія всіх її складових.

Отже, так як інформація про доступну продукцію в магазинах, на складах та її електронний перелік буде зберігатися в базі даних, то для того, щоб робота даної мережі магазинів була якомога оперативнішою та злагодженою, необхідно зв'язати комп'ютери кожної будівлі (філії) локальною обчислювальною мережею, які у свою чергу будуть пов'язані між собою.

### **1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства**

Філії мережі матимуть базу, отриману з оптових складів та інших магазинів, що містить інформацію про продукцію, що є в наявності, для отримання оперативної інформації операторами. Крім того, на одному із серверів мережі зберігатиметься база даних з інформацією про всю

продукцію. Щодня оператори філій надсилатимуть на цей сервер БД інформацію про купівлю-продаж продукції. Також в базу цього сервера з БД про всю продукцію надходитиме інформація про клієнтів, які залишили замовлення на той чи інший товар. Ця інформація надходитиме відразу після здійснення замовлення. До головного серверу організації матиме доступ і директор мережі магазинів у разі знаходження в одній з філій. Це забезпечить необхідну мобільність мережі.

Філії матимуть можливість взаємодії одна з одною для отримання інформації про наявність необхідної інформації, яка відсутня в іншій філії мережі.

Запит до бази даних здійснюватиметься за необхідності, у разі відсутності необхідної продукції в іншій філії мережі.

Філії обмінюються різномірною документацією (документи Word, Excel, PDF) невеликого розміру для чого вони використовують електронну пошту.

Для зручності роботи запит повинен виконуватися не більше 1 секунди, тому підрахунок трафік буде вестися в Мбітах в секунду.

Будемо проводити розрахунок приблизних значень швидкостей передачі даних через мережу. Так як для визначення таких показників потрібні певні математичні прийоми та моделі системи, що виходить за рамки даного предмета, вважатимемо, що вихідні значення уже відомі.

Розрахуємо максимальну швидкість, яку має забезпечувати локальна мережа.

$50\ 000\ \text{кбайт} * 1000\ \text{записів} = 50\ 000\ 000\ \text{кбайт} = 48828,125\ \text{Мбайт} = 13,56\ \text{Мбіт/с}$

Виходячи з викладеного вище, необхідно забезпечити швидкість передачі порядку 100 Мбіт/с.

### **1.3 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань**

В даний час існує кілька підстандартів технології Fast Ethernet:

#### **1. 100Base-TX**

Конфігурація пасивної зірки функціонує як конфігурація. Для створення мережі використовується кабель UTP5 або STPType1. Кількість пар кабелю - 2. Максимальна довжина сегмента - 100 метрів. Для підключення мережевого кабелю до адаптерів і концентраторів використовуються 8-контактні інтерфейси RJ-45 [1]. Максимальна кількість точок, які можуть бути підключені до сегмента – 1024. Максимальна кількість учасників мережі – 3072 учасника.

#### **2. 100Base-T4**

Топографія зірки функціонує як рельєф. Для створення мережі використовується пара перекреслених UTP, UTP4 і UTP5. Кількість пар кабелів - 4 (3 - передача даних, 1 - виявлення колізій). Максимальна довжина відрізка – 100 метрів. Для підключення мережевого кабелю до адаптера та концентратора використовуються 8-контактні інтерфейси RJ-45. Максимальна кількість точок, які можуть бути підключені до сегмента – 1024. Максимальна кількість учасників мережі – 3072 учасника.

#### **3. 100Base-TF**

Максимальна довжина сегмента може становити 400 метрів в напівдуплексному режимі (для гарантованого виявлення зіткнень) або 2 кілометри в повнодуплексному режимі по одномодовому оптоволокну і до 32 кілометрів по багатомодовому.

#### **Gigabit Ethernet**

1. 1000BASE-T, IEEE 802.3ab – перший стандарт для 1 Гбіт/с Ethernet. Приймається 5-й або 6-й розряд. У передачі даних беруть участь всі 4 пари. Швидкість передачі даних становить 250 Мбіт/с на пару.

2. 1000BASE-TX, - протокол Ethernet 1 Гбіт/с, який є стандартним для подвійного дроту категорії 6. Практично не використовується.

3. 1000Base-X — це загальний термін для Gigabit Ethernet, який використовує оптичне волокно як середовище для передачі даних, включає 1000BASE-SX, 1000BASE-LX і 1000BASE-CX.

4. 1000BASE-SX, IEEE 802.3z – протокол Ethernet 1 Гбіт/с, використовує кілька режимів оптоволокна та має максимальну відстань передачі сигналу 550 метрів без повторювача.

5. 1000BASE-LX, IEEE 802.3z – протокол Ethernet 1 Гбіт/с, використовує кілька режимів оптоволокна та має максимальну відстань передачі сигналу 550 метрів без повторювача. Підходить для роботи на великих відстанях при використанні одномодового волокна (до 10 кілометрів).

6. 1000BASE-CX – технологія Gigabit Ethernet для коротких відстаней (до 25 метрів), це досягається за допомогою спеціального кабелю, відомого як екрановані кручені пари (STP), який має хвильовий опір 150 Ом. Підпорядкований протоколу 1000BASE-T і більше не актуальний.

7. 1000BASE-LH (Long Haul) - технологія 1гб/с Gigabit Ethernet, використовує одномодовий оптичний кабель, відстань між відправником і одержувачем обмежена 100 кілометрами без повторювача.

### 10 Gigabit Ethernet

Новий протокол 10 Gigabit Ethernet було вдосконалено за допомогою семи фізичних стандартів середовища для LAN, MAN і WAN. Наразі це визначено поправкою IEEE 802.3ae, яка є частиною стандартного процесу перегляду IEEE 802.3.

1. 10GBASE-CX4 – використовується технологія 10гб/с Gigabit Ethernet, яка підходить для роботи на коротких відстанях (до 15 метрів), мідний кабель CX4 і роз'єми InfiniBand.

2. 10GBASE-SR – технологія 10Гб/с Gigabit Ethernet, яка підходить для коротких відстаней (до 26 або 82 метрів, в залежності від типу кабелю), використовується багатомодове волокно. Він також дозволяє подолати відстань до 300 метрів за допомогою нового оптичного волокна (2000 МГц/км) у багатомодовому режимі [2].

3. 10GBASE-LX4 – використовує стратегію економії довжини хвилі для забезпечення відстані до 300 метрів у кількох оптоволоконних режимах. Він також дозволяє подолати відстань до 10 кілометрів при використанні одномодового оптичного волокна на відстані.

4. 10GBASE-LR і 10GBASE-ER - їх характеристики підтримують відстань до 10 і 40 кілометрів відповідно.

5. 10GBASE-SW, 10GBASE-LW і 10GBASE-EW - ці протоколи використовують фізичний інтерфейс, який сумісний з інтерфейсом OC-192/STM-64 SONET. Вони подібні до стандартів 10GBASE-SR, 10GBASE-LR і 10GBASE-ER відповідно, оскільки використовують той самий тип кабелю та однакову відстань передачі.

6. 10GBASE-T, IEEE 802.3ap-2006 – ця версія була прийнята в червні 2006 року після 4 років розробки. Використовує екрановану кабельну пару. Дистанція обмежена 100 метрами.

#### Технології WLAN

Ці технології описуються стандартами 802.11 (відомі під торговою маркою WIFI) та 802.16 (WiMax).

Раніше технології WIFI проектувалися для мобільних користувачів у рамках ЛОМ:

802.11 a (1999 р): 54 Мбіт/с; 5ГГц

802.11 b (1999 р): 11 Мбіт/с; 2.4 ГГц

802.11g (2001р): 54 Мбіт/с; 2.4 ГГц

Основні характеристики та специфікації описуються для вбудованих антен, але можуть працювати із зовнішніми антенами, що сприяє збільшенню

діаметра. За архітектурою бездротові локальні мережі можуть працювати в 2 режимах [3]:

1. з фіксованою структурою (з базовою станцією – AP: Access Point).  
(Рис. 1.1 (ліворуч))

2. без базової станції: Ad Нос (з довільною структурою) (Рис. 1.1 (рисунок) праворуч))

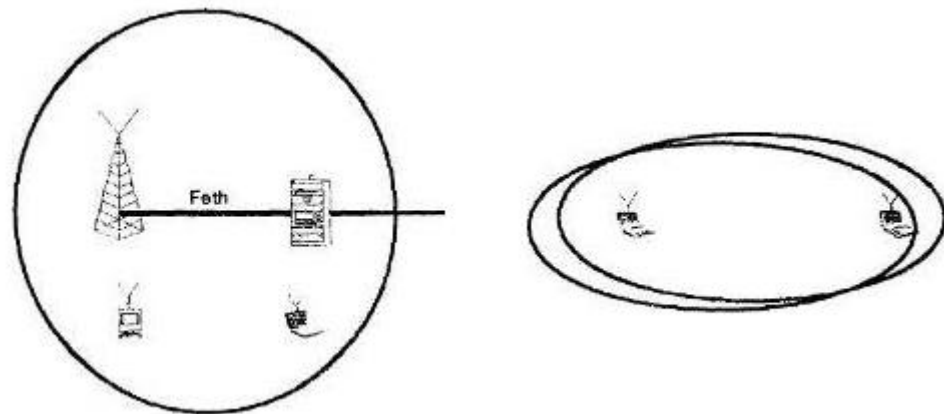


Рисунок 1.1 – Топології побудови WLAN засобами WiFi

### Технології доступу до Інтернету

В наш час конкурентоспроможними є 2 технології доступу до Інтернету ADSL/ADSL2+ та FTTB (Fiber to the Building).

### Технологія волоконно-оптичних кабелів.

Коли доступ до Інтернету надається через оптоволоконний канал, оператори зв'язку можуть використовувати різні технології у своїй мережі (SDH – синхронна цифрова ієрархія, PDH – плезіохронна цифрова ієрархія, оптичний Ethernet та інші), але на рівні кінцевого користувача це не має особливого значення, оскільки всі сучасні оптичні технології мають схожий профіль надійності. Найважливішими атрибутами користувача в цьому контексті є швидкість доступу до мережі через цей канал і тип інтерфейсу, який використовується для підключення пристроїв користувача. Використання оптоволоконного середовища є вигідним, оскільки воно

забезпечує найбільший ступінь надійності, гнучкості та найвищу швидкість передачі.

#### xDSL.

Останнім часом для забезпечення високої швидкості та надійності каналу, організованого мідним дротом, став популярним термін xDSL. На основі загальної технології DSL (цифрова абонентська лінія) було випробувано багато різних підходів для різних цілей: HDSL, MSDSL, SDSL, ADSL та інші. Як правило, технології xDSL використовуються, коли швидкість не викликає занепокоєння і телефон просто відпускають. SDSL і ADSL є найпопулярнішими технологіями, оскільки вони не вимагають дорогого обладнання від провайдера і при цьому забезпечують високу якість каналу. Обидві ці технології не забезпечують гарантованої швидкості передачі інформації, вони автоматично змінюються фізичними властивостями використовуваного мідного дроту. Основна відмінність між ними: ADSL пропонує різну швидкість передачі та прийому інформації, а SDSL ідентичний (від англійських слів Asymmetric і Symmetric) [5].

Приватні користувачі зазвичай підключаються до Інтернету через ADSL. Зазвичай використовуються стандартні телефони, перша причина полягає в тому, що вони можуть бути використані для забезпечення високого ступеня надійності та швидкості передачі даних, друга причина полягає в тому, що мідний кабель майже завжди доступний у місті (зазначаються винятки). На обсяг швидкості передачі даних впливає довжина та якість телефонної лінії.

В обох випадках виконується зв'язок з Інтернетом(постійний).

#### VPN (Virtual Private Network – віртуальна приватна мережа)

Залишається ще одна невирішена проблема: зв'язок магазинів та оптових складів. Негативним фактором є велика відстань та значна кількість магазинів, що робить застосування оптоволокна накладним. Тому найбільш оптимальним рішенням для об'єднання локальних мереж магазинів в єдину локальну мережу є технологія віртуальних приватних мереж (VPN).



Існують різні варіанти побудови VPN.

VPN на базі брандмауерів

VPN на базі маршрутизаторів

VPN на основі програмного забезпечення

VPN на базі мережної ОС

VPN на базі апаратних засобів

Виходячи зі значень, отриманих при розрахунку трафіку в пункті 1.2, можна дійти висновку у тому, що оптимальною технологією для побудови локальних мереж даної мережі магазинів електроніка ТОВ «АЛІО» є технологія Fast Ethernet.

Для побудови ЛОМ буде використано саме технологію FastEthernet 100 Base TX, оскільки дана технологія передбачає передачу даних по двох неекранованих витих парах категорії 5, у той час як для 100 Base – Т4 потрібно 4 пари кабелю категорії 3, 4 або 5, три з них потрібні передачі або прийому пакетів, а четверта пара призначена для прослуховування каналу. Оскільки неможливо виділити пари передачі або прийому даних, 100Base – Т4 неспроможна забезпечувати дуплексний режим.

Буде реалізована топологія зірка в кожному підрозділі, з центральним елементом, крім того в таких підприємствах, важливо передбачити резерви для відновлення даних після неминучих зламів та інших несправностей обладнання.

Локальна мережа підприємства має вихід в Інтернет, для цього буде використано технологію ADSL для доступу до Інтернету. Доступ віддалених з'єднань здійснено за допомогою VPN (Virtual Private Network).

#### **1.4 Розробка схеми організаційної структури підприємства**

Дніпровська філія мережі магазинів електроніки ТОВ «АЛІО» заснована у 1998 році. Сьогодні це одна з найвідоміших і найдинамічніших у сфері електроніка торгових фірм, яка встановила надійні партнерські

відносини з багатьма провідними виробниками техніки. Сьогодні ТОВ «АЛЛО» - це українська група компаній, в яку входить онлайн та класичний ритейл, маркетплейс та дистриб'юція електроніки. Офіс компанії перебуває у Дніпрі.

Основний вид діяльності ТОВ «АЛЛО» – роздрібна торгівля комп'ютерами, комплектуючими, електронно-обчислювальною технікою, радіоелектронним обладнанням, тощо.

Проаналізуємо структуру підприємства для детального ознайомлення. Організаційно-управлінська структура Дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» представлена на рисунку 1.2.

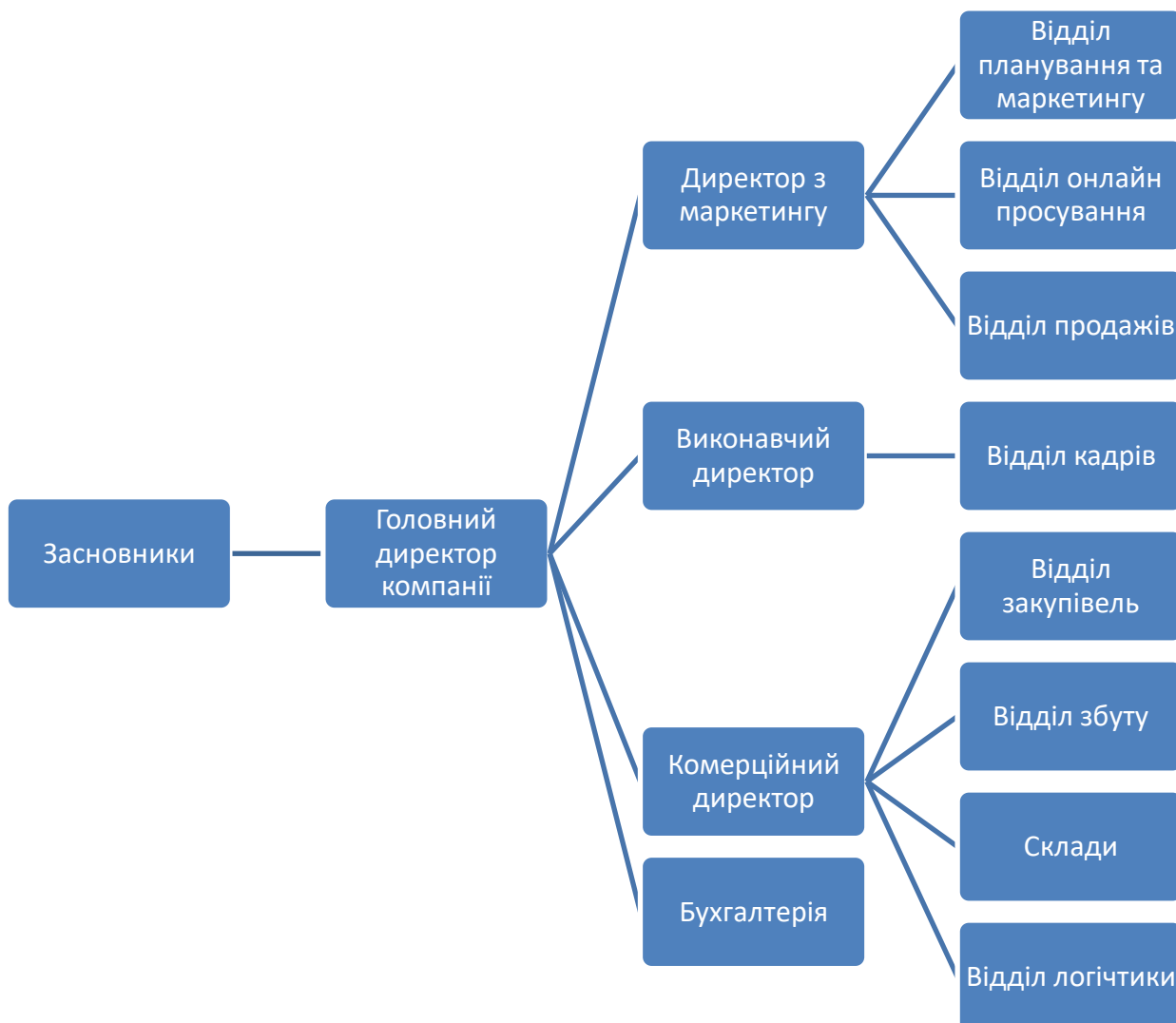


Рисунок 1.2 – Організаційна структура підприємства ТОВ «АЛЛО»

Вищим корпоративним органом є загальні збори учасників. Можливі чергові або позачергові зустрічі.

Органом контролю за фінансово-господарською діяльністю товариства є ревізійна комісія.

Керівництво поточною діяльністю покладається на єдиний виконавчий орган, до складу якого входить дирекція товариства. Органом управління є директор, який відповідає за діяльність підприємства в цілому. Єдиний виконавчий орган, який не має спроможності самостійно приймати рішення, не має повноважень діяти від імені корпорації, натомість він представляє інтереси компанії, здійснює операції, ліцензує працівників, розпоряджається справами та дає вказівки, обов'язкові для всіх працівників.

У магазині ведеться облік усіх товарів, замовлень та клієнтів.

З базою даних магазину можуть працювати такі групи користувачів:

- Директор
- Бухгалтер
- Маркетолог/менеджер
- Адміністратор-консультант
- Продавець-касир
- Клієнт

Під час роботи з базою даних директор може переглядати всю інформацію про діяльність усіх підрозділів.

При роботі з базою даних бухгалтер може переглядати всю фінансову документацію та інформацію щодо каси.

Під час роботи з базою даних маркетолог/менеджер може виконувати такі завдання:

- переглядати інформацію про чеки
- додавати інформацію про чеки
- редагувати або додавати інформацію про замовлення
- переглядати будь-яку інформацію

Під час роботи з базою даних адміністратор-консультант може виконувати такі завдання:

- вносити зміни в особисті дані клієнтів та працівників

- додавати або видаляти інформацію про товари
- редагувати або додавати інформацію про замовлення
- переглядати будь-яку інформацію

Під час роботи з базою даних продавець-касир може:

- переглядати інформацію про замовлення
- переглядати інформацію про наявність товару на складі

Під час роботи з базою даних клієнт може:

- переглядати інформацію про замовлення
- отримати інформацію про товари, що його цікавлять.

### **1.5 Постановка завдання**

Головною метою даної роботи є розробка комп'ютерної системи дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Головною вимогою, що висуваються до мереж, є забезпечення користувачам потенційної можливості доступу до ресурсів всіх комп'ютерів, об'єднаних у мережу. Всі інші вимоги – продуктивність, надійність, сумісність, керованість, прозорість, розширюваність та масштабованість – пов'язані з якістю виконання основного завдання.

Висока продуктивність мережі потрібна для нормальної роботи більшості сучасних програм. Продуктивність мережі визначається такими технічними показниками:

- Час реакції – інтегральна або узагальнена характеристика мережі з точки зору користувача, що є проміжком часу від його звернення до якогось мережного ресурсу до моменту отримання відповіді на це звернення [4, 6];
- Пропускна здатність – це максимальна потужність обробки трафіку, яка визначається стандартом технології, пов'язаної з

мережею. Пропускна здатність – це максимальний обсяг даних, який може передати мережа або її компонент за одиницю часу.

- Час затримки – інтервал часу між надходженням на вхід будь-якого компонента або всієї мережі даних та часу їхнього виходу;
- Варіація затримки – зміна (довільне) часу затримки, що носить випадковий характер, що може спричинити істотне зниження якості мережевих сервісів [6].

Однією з первісних цілей створення розподілених систем, до складу яких входять комп'ютерні мережі, був вищий ступінь надійності, ніж окремі комп'ютери.

Інший атрибут використовується для оцінки надійності складних систем:

- готовність або коефіцієнт готовності означає час, протягом якого система може бути використана;
- збереження даних та їх захист від спотворень;
- узгодженість даних, наприклад, якщо підвищення надійності на кількох файлових серверах зберігається кілька копій даних, необхідно постійно забезпечувати їх ідентичність, тобто синхронізувати;
- можливість доставки даних.

Безпека – здатність системи захистити дані від несанкціонованого доступу.

Відмовостійкість – здатність системи приховати від її користувачів відмову її окремих компонентів.

Сумісність або інтегрованість означає, що мережа здатна включати найрізноманітніше програмне та апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, що підтримують різні стеки комунікаційних протоколів, і працювати апаратні засоби і додатки від різних виробників.

Керованість – здатність мережі до централізованого управління станом її компонентів, виявлення, вирішення проблем, а також віддаленого конфігурування компонентів. Мережа повинна бути досить легко керованою, щоб її можна було переналаштовувати для задоволення постійно змінюваних потреб організації.

Прозорість - це здатність мережі приховувати від користувача свій склад, тобто мережа представляється користувачеві як єдиний традиційний комп'ютер зі складною системою зв'язків, а не як набір окремих комп'ютерів, з'єднаних складною системою кабелів.

Розширюваність — це здатність легко додавати окремі компоненти мережі (користувачів, комп'ютерів, програм, служб), збільшувати довжину сегментів у мережі та замінювати наявне обладнання більш потужними версіями.

Масштабованість — це здатність мережі збільшити кількість учасників і довжину їхніх з'єднань, зберігаючи високу продуктивність.

## **2 Розробка апаратної частини комп'ютерної системи підприємства**

### **2.1 Технічні вимоги до комп'ютерної системи**

#### **2.1.1 Вимоги до системи в цілому**

##### **2.1.1.1 Вимоги до структури і функціонуванню системи**

Комп'ютерну систему дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» можна поділити на два напрямки:

- система моніторингу всіх комп'ютерів, об'єднаних у мережу;
- система керування доступом до ресурсів всіх комп'ютерів, об'єднаних у мережу.

Вимоги до узгодженості пристроїв у мережі:

- можливість для кожного пристрою зв'язуватися та взаємодіяти з іншими пристроями;
- забезпечення рівноправного доступу до фізичного середовища для всіх пристроїв, що колективно використовують його.

##### **2.1.1.2 Показники призначення**

Комп'ютерна система Дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» повинна мати здатність обслуговувати 500 користувачів для підсистеми оперативної діяльності та не менше 100 користувачів для інших підсистем з часом відгуку системи, характерним для весь ланцюг:

- для операцій навігації за екранними формами системи – трохи більше 5 сек;
- для операцій формування доступу – не більше 10 сек.

Період часу, виділений на аналітичні звіти, залежить від їх складності та може займати декілька хвилин.

##### **2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню**

Вимоги до надійності та достовірності:



- відсутність електроживлення повинна тільки викликати перехідну помилку;
- відсутність працездатності КС не повинна перевищувати 0,02% від часу роботи на рік, що відповідає 20 хвилинам на рік.

Усі технічні рішення, використані при створенні системи, а також при визначенні необхідного апаратного забезпечення, повинні відповідати чинним нормам і правилам щодо техніки безпеки, пожежної безпеки та захисту навколишнього середовища під час експлуатації.

Система повинна бути розроблена для функціонування в складі комплексу програмно-технічної інфраструктури магазинів електроніки ТОВ «АЛЛО», а також поділу ІТ-інфраструктури магазинів електроніки ТОВ «АЛЛО» на внутрішню та зовнішню. Технічний та фізичний захист апаратних компонентів системи, зберігання даних, джерела живлення, резервування ресурсів, поточне обслуговування здійснюються засобами технічної та організаційної інфраструктури ІТ-департаменту ТОВ «АЛЛО».

Для типової роботи системи, що розробляється, необхідно гарантувати безперебійне джерело живлення. Під час роботи система повинна дотримуватися відповідних правил щодо зберігання носіїв та роботи комп'ютерів, необхідно враховувати температуру та вологість.

#### **2.1.1.4 Вимоги до патентної чистоти**

Весь процес інсталяції, а також інсталяція окремих частин процесу не повинні вимагати додаткових витрат на придбання ліцензій на програмне забезпечення сторонніх розробників.

#### **2.1.2 Вимоги до функцій, які виконує КС**

Комп'ютерна система дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» має забезпечувати захист від несанкціонованого доступу

(НСД) на рівні не нижче встановленого вимогами, що висуваються до категорії 1Д щодо класифікації чинного керівного документа НД ТЗІ 1.4-001-2000 [8-14].

Система, що будується, повинна гарантувати обмеження доступу на рівні окремих програмних компонентів і структур даних. Складові частини підсистеми НРД повинні пропонувати:

- ідентифікацію користувача;
- перевірку повноважень користувача під час роботи з системою;
- розмежування доступу користувачів на рівні завдань та інформаційних масивів.

Система, що розробляється, повинна використовувати "сліпі" паролі (при наборі пароля його символи не показуються на екрані або замінюються одним типом символів; кількість символів не відповідає довжині пароля).

### **2.1.3 Вимоги до видів забезпечення КС**

#### **2.1.3.1 Вимоги до інформаційного забезпечення**

Інформаційні вимоги:

- забезпечення використання «прозорого» режим обслуговування;
- при повному завантаженні мережі не повинно відбуватися блокування передачі даних;
- мінімальна швидкість передачі 100 Мбіт/с.

#### **2.1.3.2 Вимоги до програмного забезпечення**

Модернізація КС передбачає заміну наявного обладнання на нове, що відповідає вимогам передових світових технологій у сфері телекомунікацій та автоматизації управління [15], а саме:

- підтримувати можливість зберігання в єдиній базі даних великих обсягів інформації (комплексність, єдність БД), забезпечувати

- можливості функціонального розширення та нарощування потужності (розширюваність та масштабованість);
- підтримувати розподілену обробку інформації, доступом до ресурсів системи як у локальній мережі, і через Internet;
  - використовувати єдину систему класифікації та кодування (уніфікованість);
  - мати вбудовані засоби оперативної аналітичної обробки даних;
  - функціонувати в гетерогенних середовищах та на різних апаратних платформах (багатолатформність);
  - забезпечувати взаємодію та сумісність з різними програмними продуктами, які вже використовуються на підприємстві (відкритість та інтегрованість);
  - забезпечувати високу надійність та стійкість до збоїв;
  - забезпечувати несуперечність та повноту збереженої інформації (цілісність);
  - забезпечувати належний рівень захисту та конфіденційності переданих даних (безпека);
  - підтримувати можливість модернізації у процесі експлуатації [4].

## **2.2 Розробка апаратної частини комп'ютерної системи**

### **2.2.1 Розробка топологічної схеми розміщення структурних підрозділів підприємства**

Процес модернізації КС передбачає її часткове переоснащення, проте в даному випадку доводиться розглядати варіант повної заміни існуючої мережі у виробничих цехах та організації нової обчислювальної мережі між будинком офісу та будинком з розміщенням у ньому складу, розташованих на значній відстані один від одного.

На рисунку 2.1 представлено карту розташування будівель, ЛОМ яких вирішено з'єднати в єдину обчислювальну мережу для створення загального інформаційного простору організації ТОВ «АЛЛО».

На рисунках 2.2, 2.3, 2.4 представлені плани будівлі офісу першого, другого поверху та складу із існуючою ЛОМ.



Рисунок 2.1 – Карта розташувань будівель

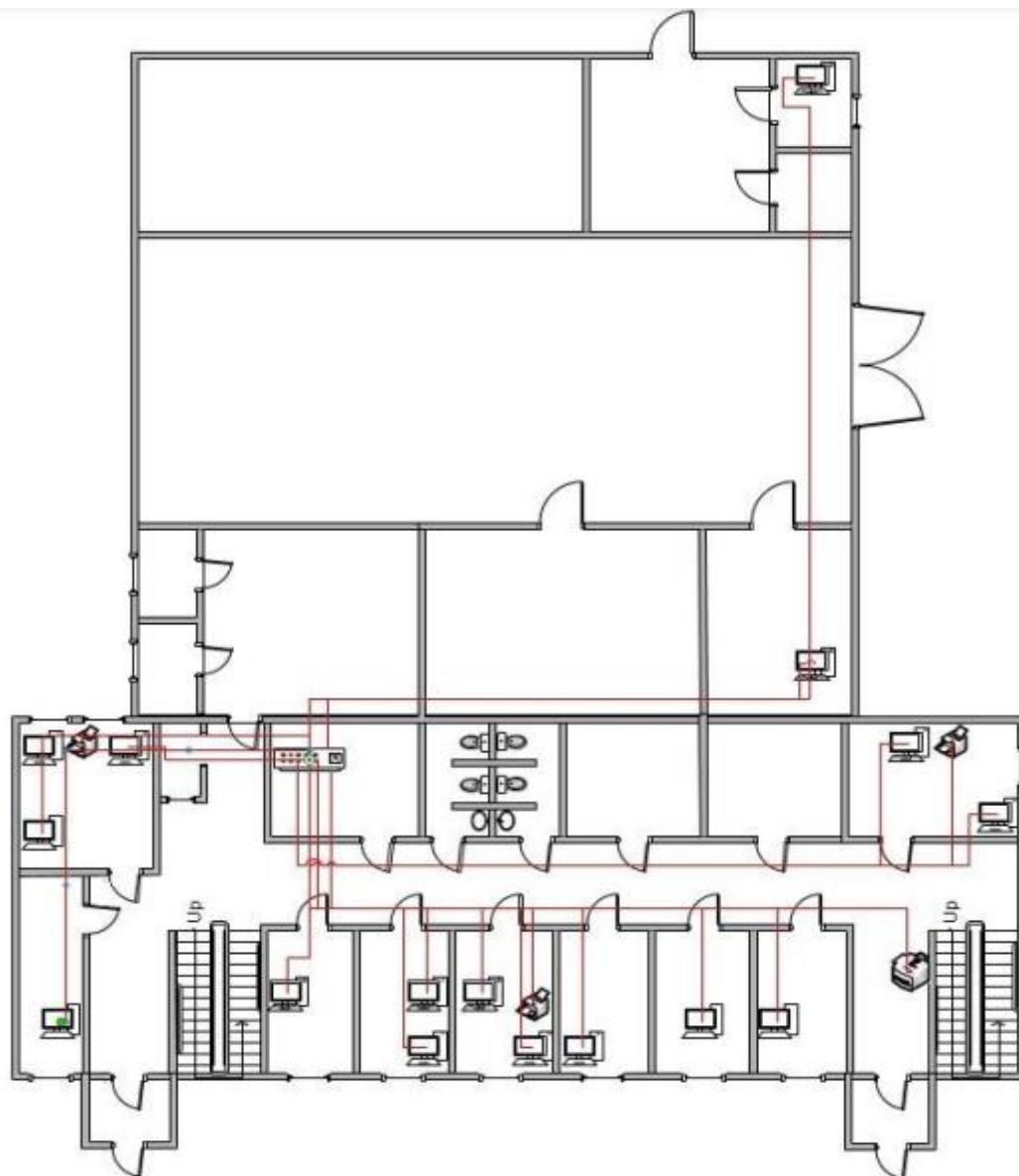


Рисунок 2.2 – План розміщення першого поверху

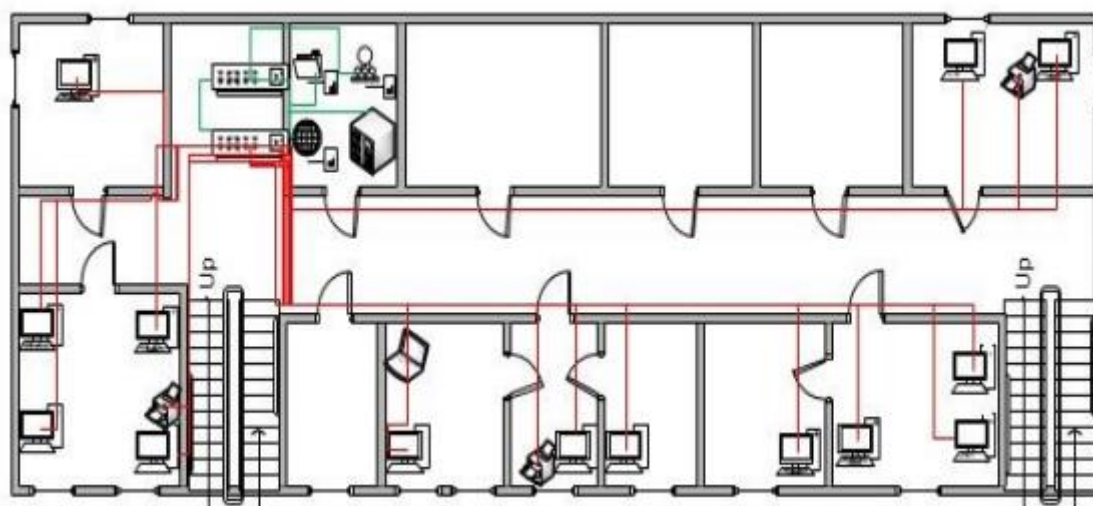


Рисунок 2.3 – План розміщення другого поверху

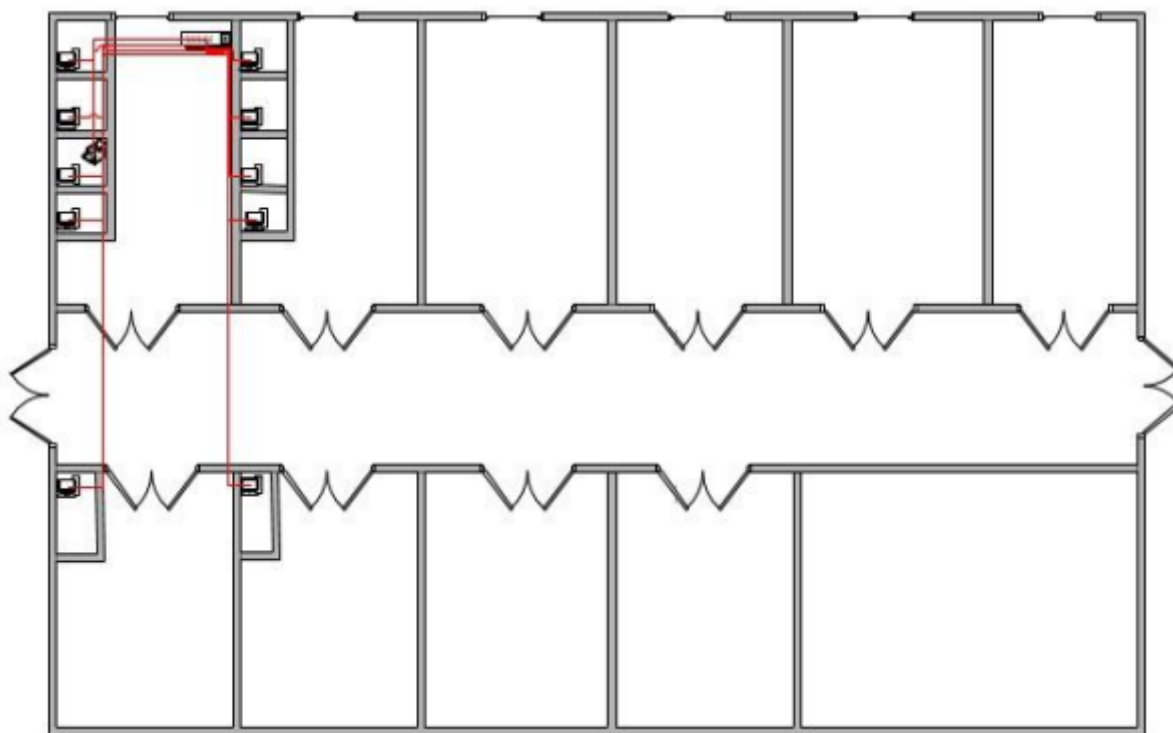


Рисунок 2.4 – План розміщення робочих місць складу

Необхідно вибрати способи розміщення КС (рисунок 2.5, 2.6). на рисунку 2.5 продемонстровано можливість розміщення КС, розташованої на віддаленні один від одного, за допомогою зв'язуючого кабель каналу передачі даних.

На рисунку 2.6 продемонстровано розміщення точок доступу та відстань між ними у прямій видимості.

На рисунках 2.5 та 2.6 видно, що ЛОМ розташовані на великій відстані одна від одної, що призводить до неможливості підключення кабельним способом.

Метод підключення двох окремо розміщених ЛОМ за методом точок доступу.

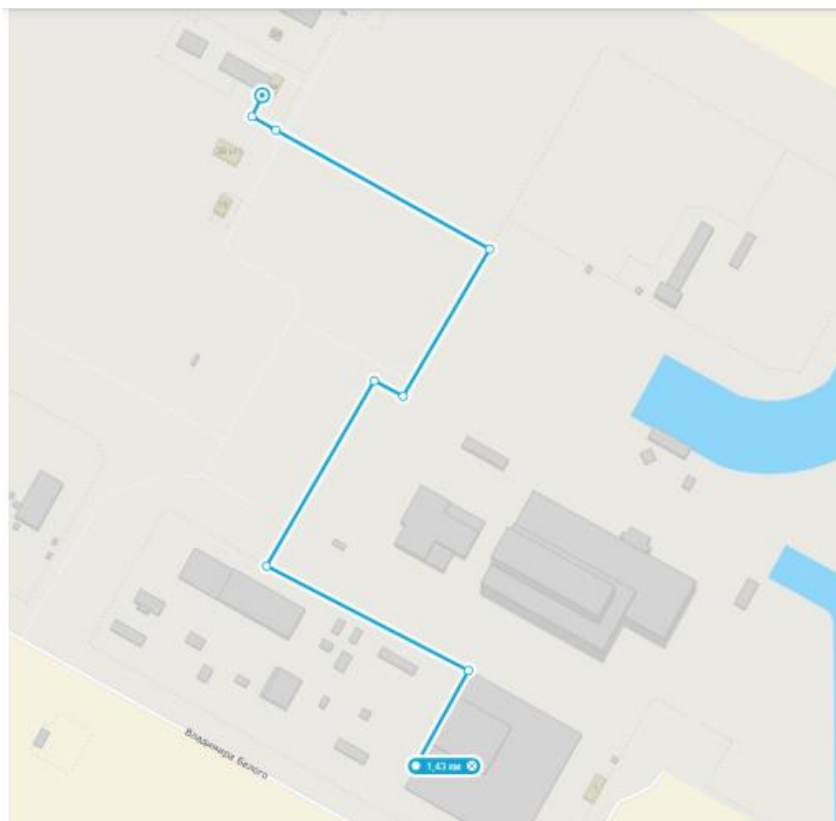


Рисунок 2.5 – Можливість розміщення КС, розташованої на віддаленні один від одного, за допомогою зв'язуючого кабель каналу передачі даних

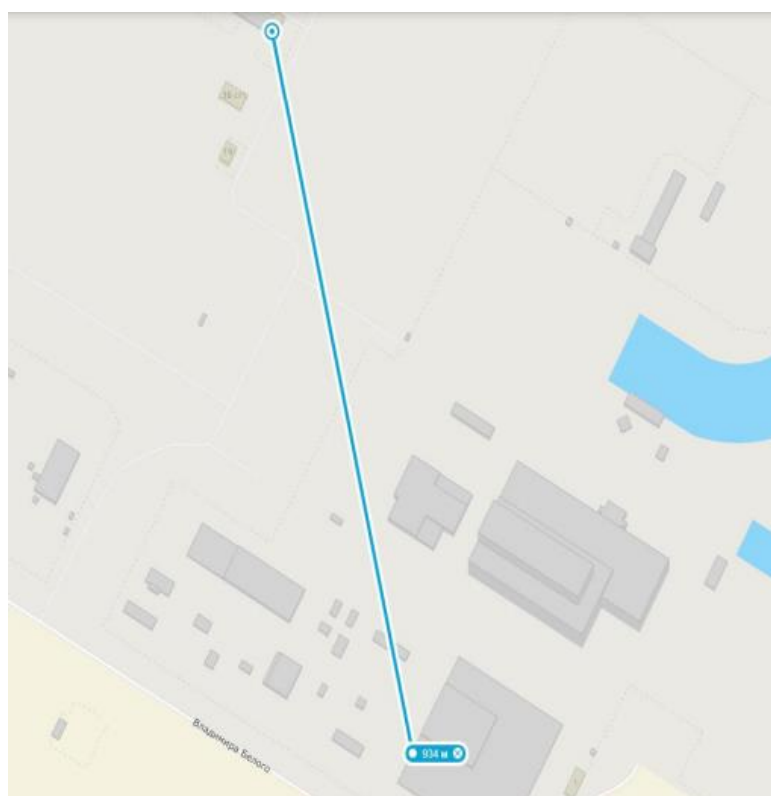


Рисунок 2.6 – Розміщення точок доступу та відстань між ними у прямій видимості

### **2.2.2 Розробка загальної архітектури мережі підприємства**

Для виконання проекту об'єднання ЛОМ складу та будівлі офісу організації ТОВ «АЛЛО» в єдину мережу та модернізації існуючої ЛОМ будівлі складу знадобиться наступне обладнання:

- сервер,
- комп'ютери для робочих місць користувачів,
- джерела безперебійного живлення,
- багатофункціональні пристрої,
- бездротові точки доступу,
- кабель,
- шафа монтажна,
- комутатор та програмне забезпечення.

При проектуванні КМ філії ТОВ «АЛЛО» були виявлені недоліки існуючої інформаційної структури мережі організації, що призвело до необхідності модернізації обладнання, що використовується, зокрема:

- сервера для адміністрування мережі з низькою обчислювальною потужністю, встановленого в серверній кімнаті;
- використовуваних системних блоків на складу організації з програмним забезпеченням, що не підтримується;
- використання комутаційного обладнання з недостатньою пропускною спроможністю.

### **2.2.3 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи**

Вибір сервера.



Основні вимоги, яких необхідно дотримуватись при виборі типу та конфігурації сервера:

- надійність;
- гарантоване зберігання даних;
- необхідність зростання під зростання навантаження;
- забезпечити безперебійну роботу.

Проаналізувавши КС ТОВ «АЛЛО» визначено, що необхідний сервер першого рівня. До представленої категорії зараховуються сервери настільного виконання для невеликого офісу.

Сервери початкового рівня використовуються:

- для невеликих підприємств, яким необхідно економічно перейти від однорангової мережі до мережі на основі сервера;
- підходить як файловий сервер, сервер друку та сервер електронної пошти для малого підприємства, якому потрібно підвищення продуктивності.

Порівнявши технічні характеристики серверів, наведених у таблиці 2.1, було обрано сервер PRIMERGY TX300 S8 [16].

Можливості сервера:

- можливості максимального розширення у майбутньому;
- оптимізовано для бізнесу – додатків, хмарних обчислень та віртуалізації, а також для додатків, що потребують великого обсягу обчислень;
- розширена масштабованість – до 24 модулів DIMM із загальним обсягом пам'яті 1536 ГБ, до 24 жорстких дисків та 10 роз'ємів PCIe.

Виконаємо порівняння кількох серверів у таблиці 2.1.

Таблиця 2.1 – Порівняння характеристик різних серверів

|  |                     |                         |                           |
|--|---------------------|-------------------------|---------------------------|
|  | IBM System x3100 M4 | HP ProLiant ML350e Gen8 | FUJITSU PRIMERGY TX300 S8 |
|--|---------------------|-------------------------|---------------------------|

|                                |   |   |   |
|--------------------------------|---|---|---|
| Тип процесора:                 | E3-1270 - 3.40 GHz  | E5-2407 - 2.20 GHz  | Intel Xeon processor E5-2600 v2   |
| Об'єм оперативної пам'яті, Gb: | 4   | 4   | Від 4 до 1536   |
| Розмір жорсткого диска:        | 500 ГБ  | 500 ГБ  | HDD SAS, 5 с, 4 ТБ, 7200 об./хв., гарячої заміни  |
| Слоти                          | RJ-45 (Ethernet):<br>2Графічний:<br>1Оптичний привід:<br>DVD-ROM USB: 6 | RJ-45 (Ethernet): 2<br>Графічний:<br>1Оптичний привід:<br>DVD-ROM USB :10 | 2 порти Ethernet<br>10/100/1000 Мбіт/с<br>(прискорення<br>введення/виводу)Привід<br>DVDROMUSB 3.0: 10 |

Вибір робочих місць користувачів.

Для користувачів було обрано персональні комп'ютери з технічними характеристиками, порівняння наведено у таблиці 2.2.

Виконавши порівняння технічних характеристик робочих станцій було обрано Intel Pentium Intel Core i3-4130 3.4GHz, оскільки продуктивність цієї станції вище, ніж в інших.

Таблиця 2.2 – Порівняння характеристик робочих станцій

|               |   |  |   |
|---------------|---|--|---|
| Зображення    |  |  |  |
| Процесор      | Intel Core i3 3400<br>МГц   | IntelPentium G620<br>2.60GHz   | Intel Pentium Intel<br>Core i3-4130 3.4GHz  |
| Пам'ять       | 2048 Мб   | 1024 Мб  | 4096 Мб   |
| Тип пам'яті   | DIMM DDRIII   | DDR-III  | DDR-IV DIMM   |
| Відеокарта    | Інтегрована Intel HD<br>Graphics 2500   | Інтегрована  | Intel HD Graphics<br>4000   |
| Жорсткий диск | 500 Гб  | 500 Гб   | 1 Тб  |

Вибір комутаторів.

Комутаційне обладнання відноситиметься до активного мережного обладнання. Насправді є ядром КМ тобто вузлами, що поєднують її сегменти. Для цього проекту організації ЛОМ були обрані комутатори виробника D-Link, які зарекомендували себе з найкращого боку [17].

Для наочності нижче наведено таблицю 2.3, де можна побачити характеристики різних комутаторів.




Таблиця 2.3 – Порівняння показників комутаторів

| Назва               | D-Link DGS-1100-24                      | 3Com 4500G                    | Zyxel -4526                  |
|---------------------|---|-------------------------------|------------------------------|
| Кількість портів    | 24 порти 10/100BASE-TX з підтримкою PoE | 24 порти 10/100/1000 Мбіт/сек | 24 порт 10/100/1000 Мбіт/сек |
| Комутаційна матриця | 12,8 Гб/с                               | 10 Гб/с                       | 10 Гб/с                      |
| Матриця MAC-адрес   | 16000 записів                           | 8192 записів                  | 8000 записів                 |

Вибір джерела безперебійного живлення.

Джерело безперебійного електроживлення (далі – ДБЖ) – це автоматичний пристрій, головна функція якого – живлення включеного навантаження за рахунок енергії акумуляторних батарей за відсутності напруги мережі або виходу його параметрів за можливі межі. Крім цього ДБЖ може виконувати функції фільтра та стабілізатора (Таблиця 2.4).

Таблиця 2.4 – Порівняння ДБЖ

| Зображення                          |  |  |  |
|-------------------------------------|---|--|---|
| Назва                               | APC by Schneider Electric Symmetra LX 8kVA Exp to 16kVA                             | Riello MSM10   | Borri RT 030-60   |
| Час роботи при повному навантаженні | 57.4 хв   | 35 хв  | 60 хв   |
| Вихідна потужність                  | 8000 ВА / 5600 Вт   | 10000 ВА / 8000 Вт   | 3000 ВА / 2400 Вт   |
| Вхідна напруга                      | 155-480 В   | 180-264 В  | 160-280 В   |

Щоб забезпечити безперебійну працездатність мережі, серверів і комутаторів, необхідно встановити ДБЖ. Для того щоб вибрати ДБЖ

необхідно підрахувати споживану потужність мережного обладнання в серверній:

- 1 файловий сервер та Proху-сервер – 1000 Вт;
- 4 комутатори – 18 Вт;
- загальна споживана потужність дорівнює 509 Вт.

Вихідна потужність ДБЖ визначається як добуток напруги (у вольтгах, V) на силу струму (в амперах, A).

Потужність, споживана навантаженням, визначається як добуток вихідної потужності ДБЖ (у вольт-амперах, ВА) на коефіцієнт потужності навантаження (PowerFactor, PF).

З цього випливає, що максимальна потужність, споживана навантаженням, для цього ДБЖ дорівнюватиме:  $8000 \times 0,7 = 5600$  Вт. Цього достатньо для забезпечення електроживленням існуючого устаткування. Потужність ДБЖ взята трохи вище, ніж було б необхідно для того, щоб у майбутньому не довелося при нарощуванні обчислювальних та комунікаційних потужностей замінювати ДБЖ іншим [18], більш потужним, а також при запасі потужності збільшиться час автономної роботи обладнання. Порівнявши і підрахувавши необхідну потужність, вибираємо APC by Schneider Electric Symmetra LX 8kVA Exp to 16kVA.

Вибір бездротової точки доступу

Для з'єднання двох ЛОМ підприємства, розташованих на відстані рівній 934 метри у прямій видимості, була обрана точка доступу Ubiquiti NanoStation M2, в кількості 2 штук.

Точка доступу Ubiquiti NanoStation M2 призначена для розміщення поза будівлею. Цей пристрій забезпечує користувачам швидкість передачі даних до 150 Мбіт/с у режимі бездротового зв'язку, а дальність дії точки доступу становить 15 кілометрів. Апаратна частина девайсу представлена високопродуктивним процесором та потужною інтегрованою антеною, яка покликана забезпечити стабільність з'єднання та відмінний сигнал [19].

Ubiquiti NanoStation M2 оснащена LAN-портом, що дозволяє підключати пристрої для здійснення IP-відеоспостереження.

Вибір типу кабельних систем.

Для зв'язку комутаційного устаткування з обчислювальними пристроями мережі організації необхідно забезпечити зв'язок з-поміж них. Для цього нам потрібні сполучні кабелі.

В даний час, практично всі мережі проектуються на базі кабелю кручений пари, так як коаксіальний кабель вже застарів і не забезпечує необхідну швидкість передачі.

Кабель кручена пара (UTP, FTP) - це певний тип кабельних провідників, що складаються з однієї або декількох переплетених між собою двох жил. Кожен провідник такої пари має власну ізоляцію, а кількість витків намагаються зробити невеликою. Скручування пар таких кабелів необхідно здійснювати для зменшення перешкод, що наводяться на провідники.

Кабель вита пара UTP, категорія 5e, 4 пари, solid UTP4-C5e-SOLID-XX представлений рисунку 2.7.



Рисунок 2.7 – Вита пара solid UTP4-C5e-SOLID-XX

Вибір монтажної шафи

Для встановлення обчислювального обладнання мережі потрібна спеціалізована монтажна шафа. Для проекту ЛОМ організації ТОВ «АЛЛО» було обрано, DEPO Rack 650G3 Міні датацентр. Монтажна шафа, що замикається, забезпечує захист від пилу для використовуваного обладнання і обмежує доступ персоналу до обладнання.

Основні переваги:

- жорсткість конструкції завдяки великій кількості точок кріплення;
- зручний доступ для сервісного обслуговування обладнання з розбирання дверей та бічних панелей;
- широкий кабельний простір;
- модульність та гнучкість дизайну;
- максимальний ступінь захисту від пошкоджень;
- підведення кабелів з 4-х сторін через щіткові введення підлоги та стелі.



Рисунок 2.8 – Монтажна шафа DEPO Rack 650G3 міні-ЦОД

Основні вимоги, встановлені для операційної системи:

- виконувати основні функції ефективного керування ресурсами;
- забезпечити простий у використанні інтерфейс та програми.

Операційні системи для робочих станцій.

Для робочих станцій у вибраному корпусі організації буде встановлена операційна система Windows 7.

Для коректної установки операційної системи на комп'ютер він повинен мати такі мінімальні характеристики:

- процесор із частотою не менше 1 ГГц;
- 1 гігабайт оперативної пам'яті (2 гігабайти для 64-бітної версії);
- відеоадаптер з об'ємом не менше 128 мегабайт (необхідний для включення інтерфейсу Aero) та підтримкою DirectX9;

- 16 гігабайт вільного простору на жорсткому диску (20 гігабайт для 64-бітної версії) [19].

#### 2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Обсяг вихідного трафіку з найбільшої локальної мережі в Дніпрі мережі електроніки АЛЛО визначається наступним чином. Загальна кількість користувачів – 100. Максимальна пропускна здатність мережі на рівні доступу становитиме:

$$P_{p.p} = \mu * l * N * 8 = 155 * 650 * 100 * 8 = 80,6 \text{ (Мбіт/с)},$$

де  $N$  – кількість вузлів в мережі.

Отриманий чисельний результат вказує на відсутність перевантажень.

Комутатор рівня доступу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000Мбіт/с [20]. Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 1000\ 000\ 000 / (650 * 8) = 20830 \text{ пакетів/с}$$

Максимальне завантаження знаходимо:

$$N = 20830 / 155 = 134 \text{ джерел}$$

Інтенсивність вихідного трафіку від всіх користувачів дорівнює:

$$\lambda = N * \mu = 100 * 155 = 15500 \text{ (пакетів/с)}$$

Коефіцієнт затримки:

$$\rho = \lambda / \mu_{\text{вих}} = 15500 / 20830 = 0,74$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \rho (1 - \rho) = 0,74 (1 - 0,74) = 0,02$$

Середня затримка кадру, пов'язана з чергою М/М/1, дорівнює:

$$T = 1 / (\mu - \lambda) = 1 / (20830 - 15500) = 3,2 * 10^{-6} \text{ с}$$

Середня довжина черги:

$$L_{\text{чер}} = \rho^2 / (1 - \rho) = 0,0038 / (1 - 0,74) = 0,001$$

Середній час перебування пакета в черзі:

$$T_{\text{оч}} = L_{\text{чер}} \lambda = 0,001 \cdot 15500 = 8 \text{ мкс}$$

Пропускна здатність каналу:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = b / l$$

$$b = \lambda * l = 15500 * 650 * 8 = 59520000 \text{ біт/с} = 59,5 \text{ Мбіт/с}$$

Що є нормою.

Загальна структура мережі наведена на рисунку 2.9.



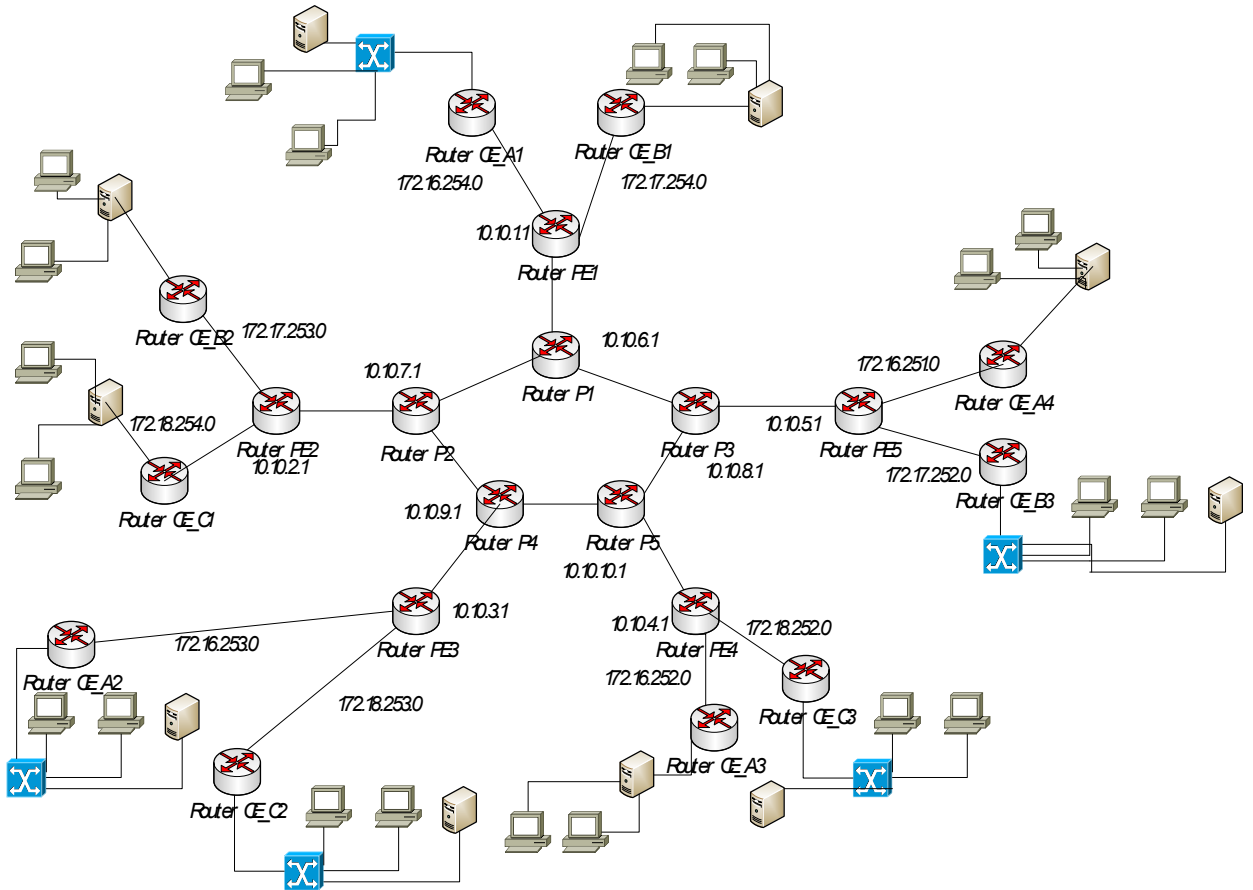


Рисунок 2.9 – Структура мережі

## 3 Розробка корпоративної мережі

### 3.1 Розрахунок схеми адресації корпоративної мережі

Сформуємо структурну схему КМ дніпровської філії мережі магазинів електроніки ТОВ «АЛІО» та виведемо основні показники.

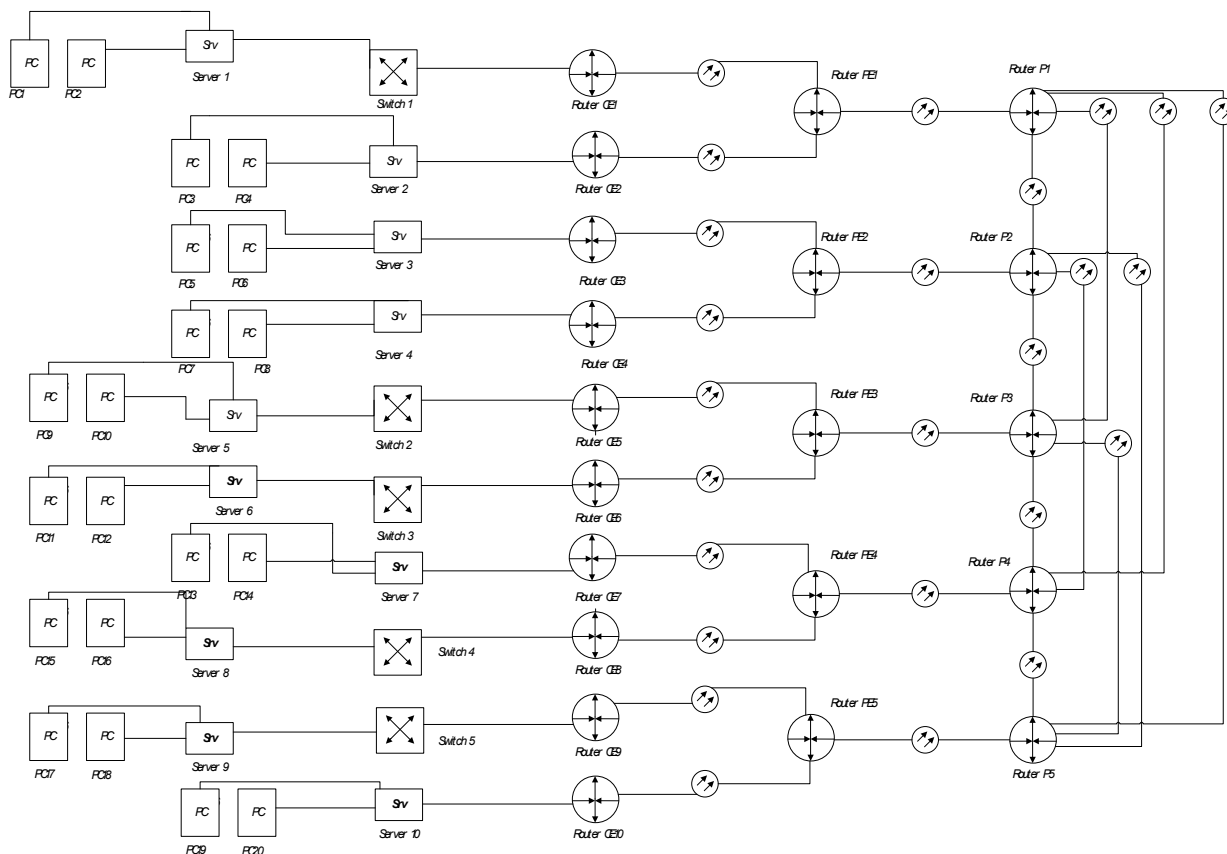


Рисунок 3.1 – Топологічна схем структурна дніпровської філії мережі магазинів електроніки ТОВ «АЛІО»

Виділимо три сегменти

```
class-map match-all class2
match ip precedence 3
class-map match-all class3
match ip precedence 1
class-map match-all class1
match ip precedence 5
```

Кожному припишемо інтерфейсні адреси

```

interface Loopback0
ip address 10.10.6.1 255.255.255.255
!
interface Serial1 / 0
description *** Router_P2 ***
bandwidth 10240
ip unnumbered Loopback0
tag-switching ip
serial restart-delay 0
max-reserved-bandwidth 90
service-policy output Isp

interface FastEthernet2 / 0
ip vrf forwarding vrf1
ip address 172.16.254.1 255.255.255.252
duplex auto
speed auto

interface FastEthernet2 / 1
ip vrf forwarding vrf2
ip address 172.17.254.1 255.255.255.252
duplex auto
speed auto
!
router ospf 100
log-adjacency-changes
network 10.10.1.1 0.0.0.0 area 0

```

### 3.2 Розробка топологічної схеми корпоративної мережі

Проведемо вимірювання на всіх 4 етапах і внесемо дані в відповідні таблиці. Згідно зі схемою мережі маємо 4 нарядки (A1), (A2), (A3) (A4).

Виконаємо дослідження ділянки мережі A1 - A4. На першому етапі будемо перевіряти частину A4 з головного офісу, використовуючи пакети різного розміру [21] і занесемо результати в таблицю 3.1:

```

Ping 172.16.251.2 size 100 repeat 100
Ping 172.16.251.2 size 6000 repeat 100
Ping 172.16.251.2 size 12000 repeat 100
Ping 172.16.251.2 size 18000 repeat 100

```

Таблиця 3.1 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 13                       | 49                    | 84                        |
| 6000          | 69                       | 116                   | 188                       |
| 12000         | 140                      | 185                   | 276                       |
| 18000         | 184                      | 234                   | 314                       |

На другому етапі припустимо, що стався обрив кабелю на ділянці P1-P3 і повторимо дії виконані на першому етапі. Також зауважимо що в перебігу 10-15 секунд ring не проходив, так як маршрутизатори реагували на зміни в мережі [22]. Отримані дані занесемо в таблицю 3.2.

Таблиця 3.2 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці P1-P3

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 36                       | 62                    | 98                        |
| 6000          | 80                       | 140                   | 210                       |
| 12000         | 182                      | 225                   | 318                       |
| 18000         | 199                      | 303                   | 433                       |

На третьому етапі припустимо, що на ділянці PE5-P3, відбувається обмін даними. Для цього виконаємо команду ring з маршрутизатора PE5:

*Ping 10.10.8.1 size 18000 repeat 500*

Виконаємо вимірювання і занесемо їх в таблицю 3.3.

Таблиця 3.3 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (PE5-P3)

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 12                       | 53                    | 120                       |
| 6000          | 110                      | 162                   | 272                       |
| 12000         | 169                      | 208                   | 355                       |
| 18000         | 212                      | 273                   | 503                       |

На четвертому етапі припустимо, що ділянка між маршрутизаторами PE1-PE5 також використовує інший клієнт, нехай це буде клієнт В. Для цього з маршрутизатора клієнта В виконаємо:

*Ping 172.17.252.2 size 18000 repeat 500*

Виконаємо вимірювання і занесемо їх в таблицю 3.4.

Таблиця 3.4 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (PE1-PE5) двома клієнтами

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 29                       | 58                    | 137                       |
| 6000          | 107                      | 172                   | 208                       |
| 12000         | 168                      | 241                   | 365                       |
| 18000         | 203                      | 284                   | 516                       |

Далі виконаємо ці ж дії, але для ділянок мережі А1-А3 і А1-А4, внесемо дані в відповідну таблиці для подальшого аналізу. Вимірювання для ділянки мережі А1-А3 будуть в таблицях 3.5, 3.6, 3.7, 3.8, а для ділянки А1-А4 в таблицях 3.9, 3.10, 3.11, 3.12.

Таблиця 3.5 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 33                       | 65                    | 98                        |
| 6000          | 104                      | 170                   | 245                       |
| 12000         | 176                      | 266                   | 368                       |
| 18000         | 240                      | 382                   | 496                       |

Таблиця 3.6 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці Р1-Р3

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 40                       | 65                    | 100                       |
| 6000          | 120                      | 207                   | 368                       |
| 12000         | 237                      | 335                   | 405                       |
| 18000         | 320                      | 427                   | 529                       |

Таблиця 3.7 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (PE4-P5)

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 32                       | 77                    | 176                       |
| 6000          | 153                      | 197                   | 273                       |
| 12000         | 205                      | 292                   | 395                       |
| 18000         | 292                      | 410                   | 564                       |

Таблиця 3.8 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (PE1-PE4) двома клієнтами

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 32                       | 80                    | 156                       |
| 6000          | 117                      | 195                   | 269                       |
| 12000         | 192                      | 297                   | 462                       |
| 18000         | 296                      | 420                   | 576                       |

Таблиця 3.9 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 40                       | 72                    | 108                       |
| 6000          | 115                      | 174                   | 260                       |
| 12000         | 183                      | 260                   | 378                       |
| 18000         | 258                      | 395                   | 482                       |

Таблиця 3.10 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці P1-P2

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 48                       | 83                    | 120                       |
| 6000          | 123                      | 181                   | 278                       |
| 12000         | 242                      | 316                   | 422                       |
| 18000         | 342                      | 428                   | 535                       |

Таблиця 3.11 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (PE3-P4)

| Розмір пакета | Мінімальне | Середнє значення | Максимальне |
|---------------|------------|------------------|-------------|
|---------------|------------|------------------|-------------|

|       | значення (мс) | (мс) | значення (мс) |
|-------|---------------|------|---------------|
| 100   | 45            | 80   | 151           |
| 6000  | 163           | 205  | 302           |
| 12000 | 216           | 286  | 391           |
| 18000 | 304           | 414  | 545           |

Таблиця 3.12 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (PE1-PE3) двома клієнтами

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 45                       | 88                    | 169                       |
| 6000          | 160                      | 210                   | 334                       |
| 12000         | 236                      | 300                   | 409                       |
| 18000         | 312                      | 423                   | 599                       |

Після виконаних вимірів постоїмо графіки отриманих даних. На першому графіку, рисунок 3.2 відобразимо залежність часу затримки від розміру пакета, використовуючи дані таблиці 3.1. З рисунка 3.2 можна зробити висновок, що залежність лінійна, тобто затримка буде поступово збільшуватися з ростом розміру пакета.

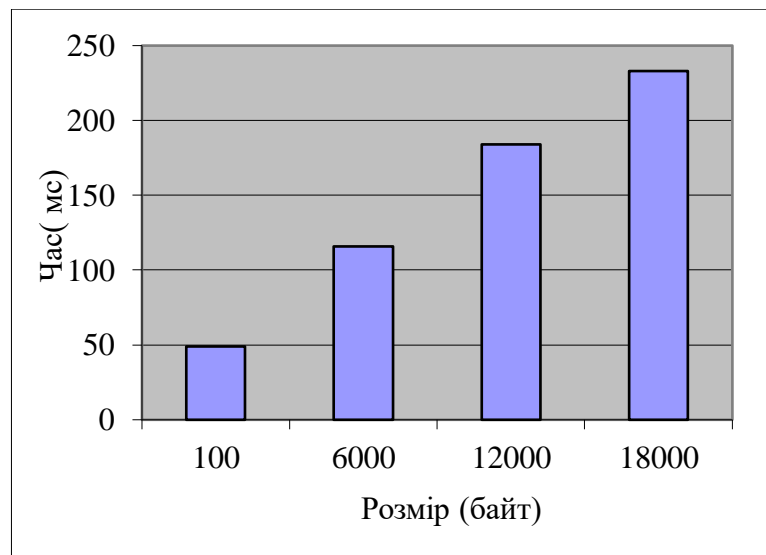


Рисунок 3.2 – Залежність часу затримки від розміру пакета

На наступній діаграмі, рисунок 3.3, відобразимо тимчасову затримку на всіх чотирьох етапах, дані для графіка візьмемо з таблиць 3.1, 3.2, 3.3 і 3.4 при відправці пакета максимального розміру - 18000 байт.

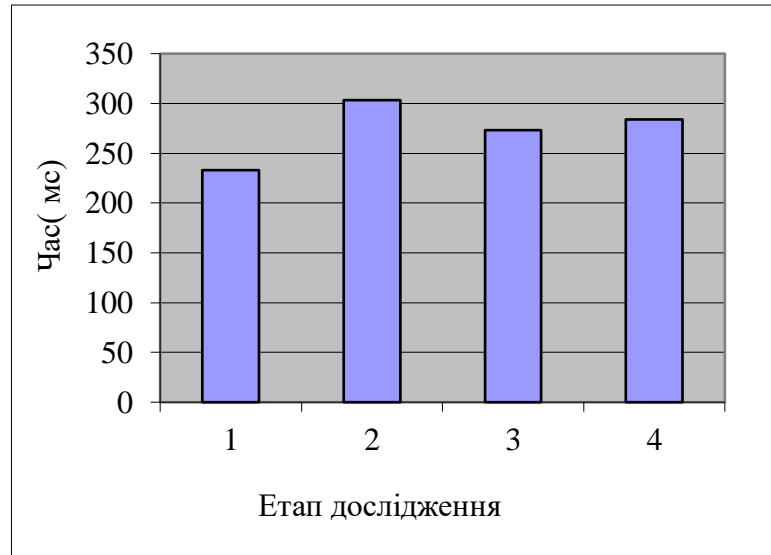


Рисунок 3.3 – Час затримки на всіх чотирьох етапах

З рисунку 3.3 можна зробити висновок, що при завантаженості однієї з ділянок мережі провайдера або при спільному використанні одного каналу двома клієнтами час затримки зростає незначно. Тимчасова затримка при обриві одного з кабелів провайдера більше за всіх інших, що пов'язана з проходженням більшої кількості маршрутизаторів і зі збільшенням відстані між клієнтами [23-25].

Тепер обчислимо середню затримку для кожного з чотирьох етапів при відправці пакета максимального розміру - 18000 байт. І занесемо отримані дані в таблицю 3.13

Таблиця 3.13 – Середнє значення тимчасової затримки на кожному з етапів

| Етап дослідження | Середнє значення тимчасової затримки (мс) |
|------------------|---|
| 1                | 335                                       |
| 2                | 385                                       |
| 3                | 366                                       |
| 4                | 375                                       |



Використовуючи дані таблиці 3.13 можна побудувати графік, рисунок 3.4.

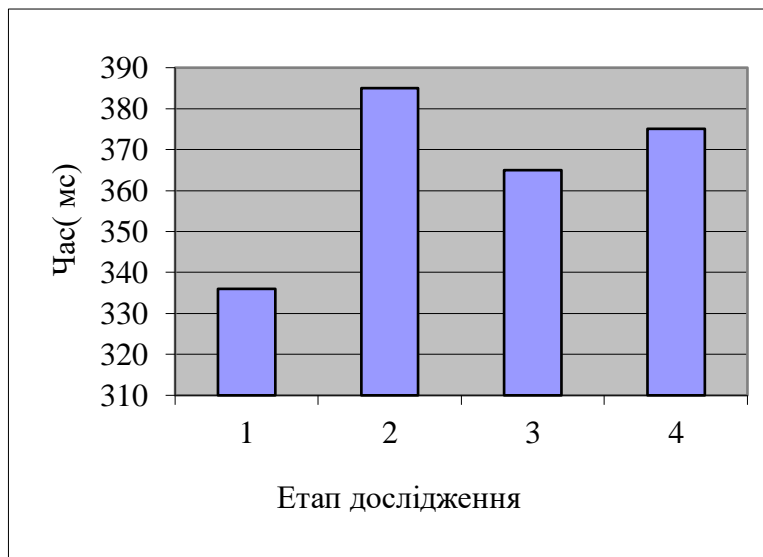


Рисунок 3.4 – Середній час затримки на кожному з етапів

Проведемо вимірювання на всіх 4 етапах і внесемо дані в відповідні таблиці.

Виконаємо дослідження ділянки мережі В1 - В2. На першому етапі будемо пінгувати В2 з головного офісу клієнта, використовуючи пакети різного розміру і занесемо результати в таблицю 3.14:

*Ping 172.17.252.2 size 100 repeat 100*

*Ping 172.17.252.2 size 6000 repeat 100*

*Ping 172.17.252.2 size 12000 repeat 100*

*Ping 172.17.252.2 size 18000 repeat 100*

Таблиця 3.14 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 12                       | 51                    | 100                       |
| 6000          | 75                       | 137                   | 204                       |
| 12000         | 155                      | 204                   | 275                       |
| 18000         | 168                      | 261                   | 393                       |

На другому етапі припустимо, що стався обрив кабелю на ділянці P1-P3 і повторимо дії виконані на першому етапі. Також зауважимо що в перебігу 10-15 секунд ring не проходив, так як маршрутизатори реагували на зміни в мережі. Отримані дані занесемо в таблицю 3.15.

Таблиця 3.15 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці P1-P3

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 18                       | 60                    | 97                        |
| 6000          | 98                       | 145                   | 202                       |
| 12000         | 179                      | 232                   | 299                       |
| 18000         | 205                      | 294                   | 404                       |

На третьому етапі припустимо, що на ділянці PE5-P3, відбувається обмін даними. Для цього виконаємо команду ring з маршрутизатора PE5:

*Ping 10.10.8.1 size 18000 repeat 500*

Таблиця 3.16 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (PE5-P3)

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 24                       | 51                    | 88                        |
| 6000          | 100                      | 165                   | 253                       |
| 12000         | 155                      | 225                   | 344                       |
| 18000         | 192                      | 286                   | 469                       |

На четвертому етапі припустимо, що ділянку між маршрутизаторами PE1-PE5 також використовує інший клієнт, нехай це буде клієнт А. Для цього з маршрутизатора клієнта А, виконаємо:

*Ping 172.16.251.2 size 18000 repeat 500*

Виконаємо вимірювання і занесемо їх в таблицю 3.17.

Таблиця 3.17 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (PE1-PE5) двома клієнтами

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 28                       | 54                    | 120                       |
| 6000          | 88                       | 118                   | 184                       |
| 12000         | 157                      | 234                   | 325                       |
| 18000         | 228                      | 299                   | 462                       |

Далі виконаємо ці ж дії, але для ділянок мережі В1-В3, внесемо дані у відповідні таблиці для подальшого аналізу. Вимірювання для ділянки мережі В1-В3 будуть в таблицях 3.18, 3.19, 3.20 і 3.21.

Таблиця 3.18 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 16                       | 44                    | 84                        |
| 6000          | 96                       | 155                   | 237                       |
| 12000         | 143                      | 213                   | 662                       |
| 18000         | 184                      | 269                   | 416                       |

Таблиця 3.19 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці P1-P2

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 32                       | 53                    | 84                        |
| 6000          | 93                       | 154                   | 232                       |
| 12000         | 176                      | 266                   | 353                       |
| 18000         | 208                      | 306                   | 522                       |

Таблиця 3.20 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (PE2-P2)

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 24                       | 47                    | 101                       |
| 6000          | 89                       | 126                   | 241                       |
| 12000         | 140                      | 218                   | 336                       |
| 18000         | 208                      | 272                   | 425                       |

Таблиця 3.21 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (PE1-PE2) двома клієнтами

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 24                       | 56                    | 108                       |
| 6000          | 93                       | 140                   | 221                       |
| 12000         | 149                      | 215                   | 312                       |
| 18000         | 224                      | 295                   | 405                       |

Після виконаних вимірів постоїмо графіки отриманих даних. На першому графіку, рисунок 3.5 відобразимо залежність часу затримки від розміру пакета, використовуючи дані таблиці 3.14. З рисунка 3.5 можна зробити висновок, що залежність лінійна, тобто затримка буде поступово збільшуватися з ростом розміру пакета.

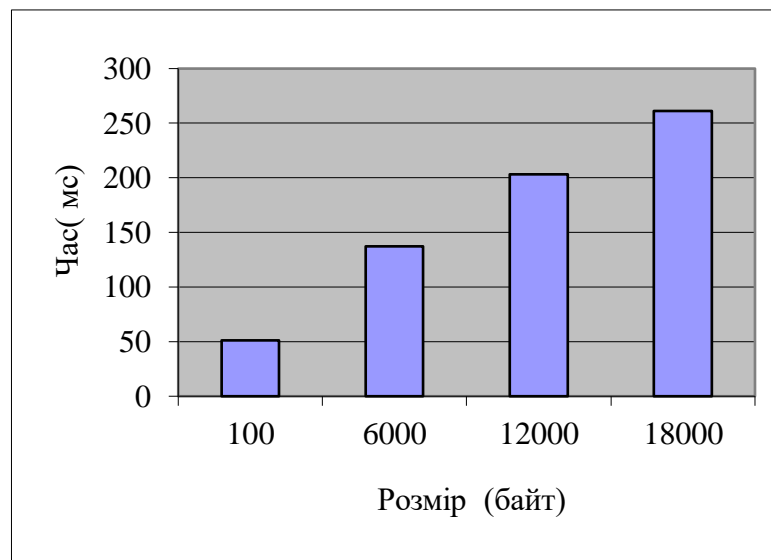


Рисунок 3.5 – Залежність часу затримки від розміру пакета

На наступній діаграмі, рисунок 3.6, відобразимо тимчасову затримку на всіх чотирьох етапах, дані для графіка візьмемо з таблиць 3.14, 3.15, 3.16 і 3.17 при відправці пакета максимального розміру - 18000 байт.

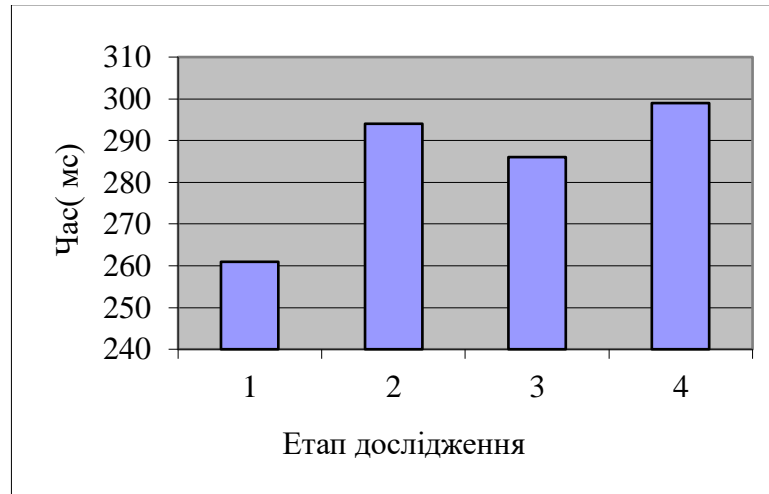


Рисунок 3.6 – Час затримки на всіх чотирьох етапах

З рисунка 3.6 можна зробити висновок, що при завантаженості однієї з ділянок мережі провайдера або при спільному використанні одного каналу двома клієнтами час затримки зростає незначно. Тимчасова затримка при обриві одного з кабелів провайдера більше ніж при проходженні пакета без перешкод, що пов'язана з проходженням більшої кількості маршрутизаторів і зі збільшенням відстані між клієнтами [26].

Тепер обчислимо середню затримку для кожного з чотирьох етапів при відправці пакета максимального розміру - 18000 байт. І занесемо отримані дані в таблицю 3.22.

Таблиця 3.22 – Середнє значення тимчасової затримки на кожному з етапів

| Етап дослідження | Середнє значення тимчасової затримки (мс) |
|------------------|---|
| 1                | 265                                       |
| 2                | 300                                       |
| 3                | 279                                       |
| 4                | 297                                       |

Використовуючи дані таблиці 3.22 можна побудувати графік, рисунок 3.7.

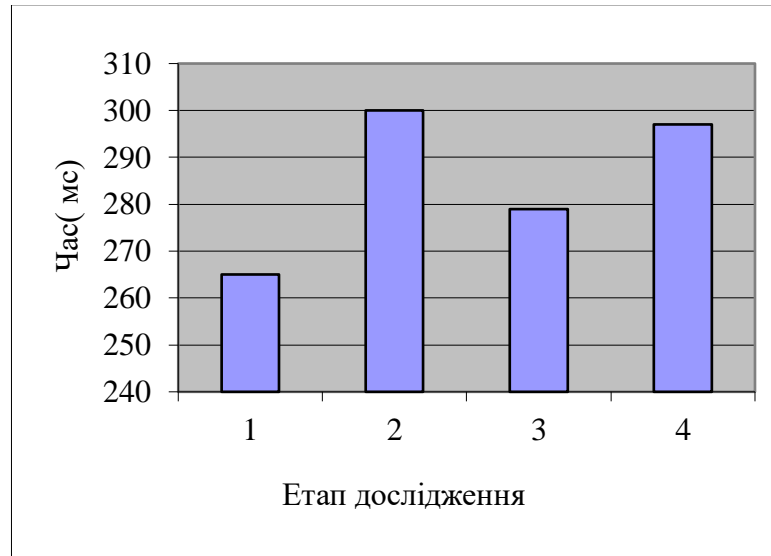


Рисунок 3.7 – Середній час затримки на кожному з етапів

Проведемо вимірювання на всіх 4 етапах і внесемо дані в відповідні таблиці.

Виконаємо дослідження ділянки мережі С1 - С2. На першому етапі будемо пінгувати філія клієнта С2 з головного офісу клієнта, використовуючи пакети різного розміру і занесемо результати в таблицю 3.23:

*Ping 172.18.253.2 size 100 repeat 100*

*Ping 172.18.253.2 size 6000 repeat 100*

*Ping 172.18.253.2 size 12000 repeat 100*

*Ping 172.18.253.2 size 18000 repeat 100*

Таблиця 3.23 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 12                       | 40                    | 84                        |
| 6000          | 69                       | 104                   | 188                       |
| 12000         | 97                       | 139                   | 205                       |
| 18000         | 136                      | 200                   | 262                       |

На другому етапі припустимо, що стався обрив кабелю на ділянці Р2-Р4 і повторимо дії виконані на першому етапі. Також зауважимо що в

перебігу 10-15 секунд ping не проходив, так як маршрутизатори реагували на зміни в мережі. Отримані дані занесемо в таблицю 3.24.

Таблиця 3.24 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці P2-P4

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 36                       | 71                    | 120                       |
| 6000          | 108                      | 175                   | 235                       |
| 12000         | 187                      | 251                   | 340                       |
| 18000         | 260                      | 326                   | 382                       |

На третьому етапі припустимо, що на ділянці PE3-P4, відбувається обмін даними. Для цього виконаємо команду ping з маршрутизатора PE3:

*Ping 10.10.9.1 size 18000 repeat 500*

Таблиця 3.25 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (PE3-P4)

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 15                       | 69                    | 156                       |
| 6000          | 61                       | 111                   | 180                       |
| 12000         | 124                      | 174                   | 241                       |
| 18000         | 145                      | 195                   | 280                       |

На четвертому етапі припустимо, що ділянка між маршрутизаторами PE2-PE3 також використовує інший клієнт. Для цього з маршрутизатора клієнта PE3, виконаємо:

*Ping 10.10.2.1 size 18000 repeat 500*

Виконаємо вимірювання і занесемо їх в таблицю 3.26.

Таблиця 3.26 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (PE2-PE3) двома клієнтами

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 28                       | 57                    | 116                       |

|       |     |     |     |
|-------|-----|-----|-----|
| 6000  | 64  | 121 | 196 |
| 12000 | 91  | 158 | 211 |
| 18000 | 160 | 216 | 301 |

Далі виконаємо ці ж дії, але для ділянок мережі С1-С3, внесемо дані в відповідні таблиці для подальшого аналізу. Вимірювання для ділянки мережі С1-С3 будуть в таблицях 3.27, 3.28, 3.29 і 3.30.

Таблиця 3.27 – Залежність часу затримки від розміру пакета

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 28                       | 50                    | 88                        |
| 6000          | 73                       | 111                   | 172                       |
| 12000         | 102                      | 170                   | 221                       |
| 18000         | 180                      | 231                   | 352                       |

Таблиця 3.28 – Залежність часу затримки від розміру пакета при обриві кабелю на ділянці Р2-Р4

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 32                       | 60                    | 88                        |
| 6000          | 109                      | 157                   | 264                       |
| 12000         | 164                      | 246                   | 327                       |
| 18000         | 196                      | 289                   | 436                       |

Таблиця 3.29 – Залежність часу затримки від розміру пакета при завантаженості однієї з ділянок мережі (РЕ4-Р5)

| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 32                       | 59                    | 108                       |
| 6000          | 127                      | 154                   | 236                       |
| 12000         | 166                      | 235                   | 344                       |
| 18000         | 208                      | 297                   | 364                       |

Таблиця 3.30 – Залежність часу затримки від розміру пакета при використанні одного і того ж каналу (РЕ2-РЕ4) двома клієнтами



| Розмір пакета | Мінімальне значення (мс) | Середнє значення (мс) | Максимальне значення (мс) |
|---------------|--------------------------|-----------------------|---------------------------|
| 100           | 32                       | 70                    | 116                       |
| 6000          | 108                      | 155                   | 213                       |
| 12000         | 173                      | 235                   | 320                       |
| 18000         | 240                      | 303                   | 389                       |

Після виконаних вимірів постоїмо графіки отриманих даних. На першому графіку, рисунок 3.8 відобразимо залежність часу затримки від розміру пакета, використовуючи дані таблиці 3.23. З рисунка 3.8 можна зробити висновок, що залежність лінійна, тобто затримка буде поступово збільшуватися з ростом розміру пакета.

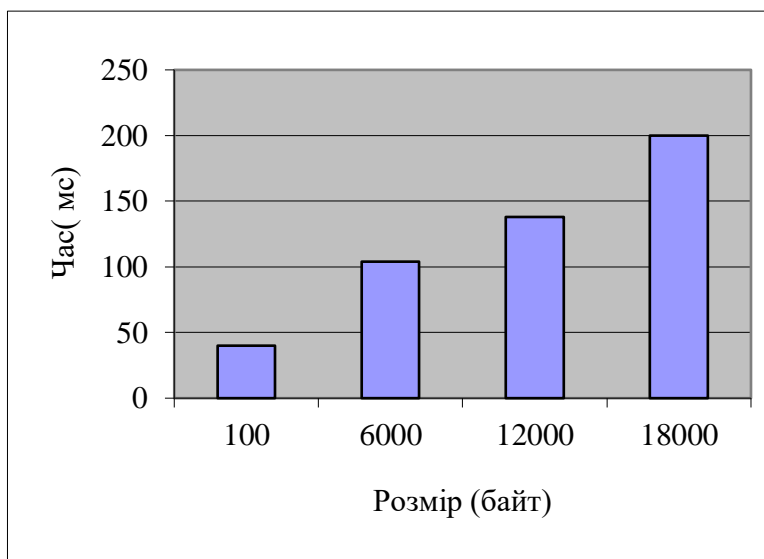


Рисунок 3.8 – Залежність часу затримки від розміру пакета

На наступній діаграмі, рисунок 3.9, відобразимо тимчасову затримку на всіх чотирьох етапах, дані для графіка візьмемо з таблиць 3.23, 3.24, 3.25 і 3.26 при відправки пакета максимального розміру - 18000 байт.

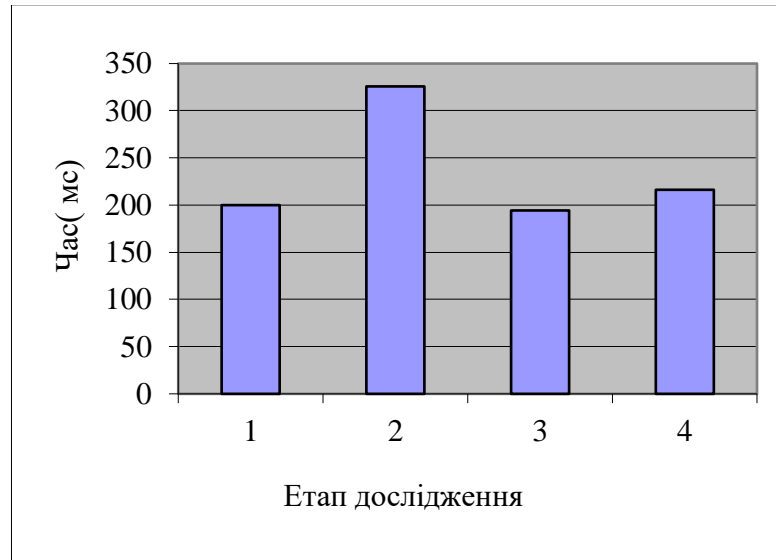


Рисунок 3.9 – Час затримки на всіх чотирьох етапах

З рисунка 3.9 можна зробити висновок, що при завантаженості однієї з ділянок мережі провайдера або при спільному використанні одного каналу двома клієнтами час затримки зростає незначно. Тимчасова затримка при обриві одного з кабелів провайдера більше ніж при проходженні пакета без перешкод, що пов'язана з проходженням більшої кількості маршрутизаторів і слідчо збільшенням відстані між клієнтами.

Тепер обчислимо середню затримку для кожного з чотирьох етапів при відправці пакета максимального розміру - 18000 байт. І занесемо отримані дані в таблицю 3.31.

Таблиця 3.31 – Середнє значення тимчасової затримки на кожному з етапів

| етап дослідження | Середнє значення тимчасової затримки (мс) |
|------------------|---|
| 1                | 216                                       |
| 2                | 306                                       |
| 3                | 247                                       |
| 4                | 259                                       |

Використовуючи дані таблиці 3.31 можна побудувати графік, рисунок 3.10.

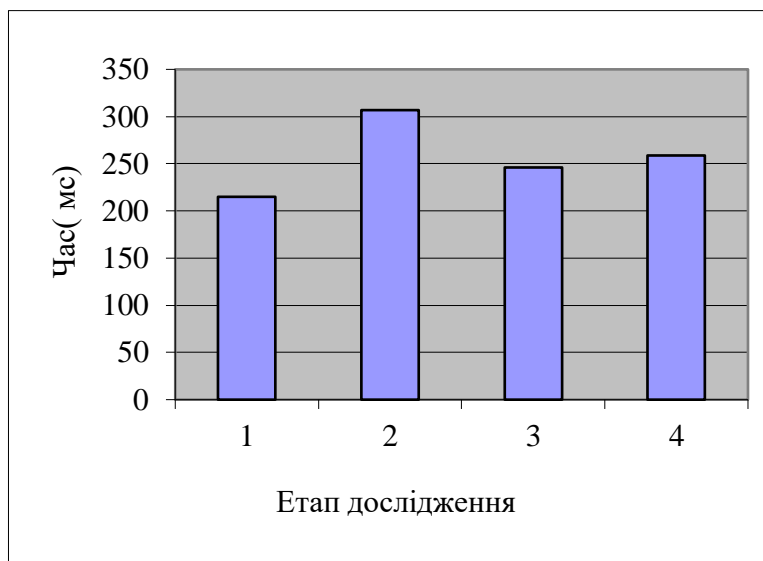


Рисунок 3.10 – Середній час затримки на кожному з етапів

### 3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Зведемо дані з таблиць 3.13, 3.22 і 3.31 в один графік і відобразимо його на рисунку 3.11

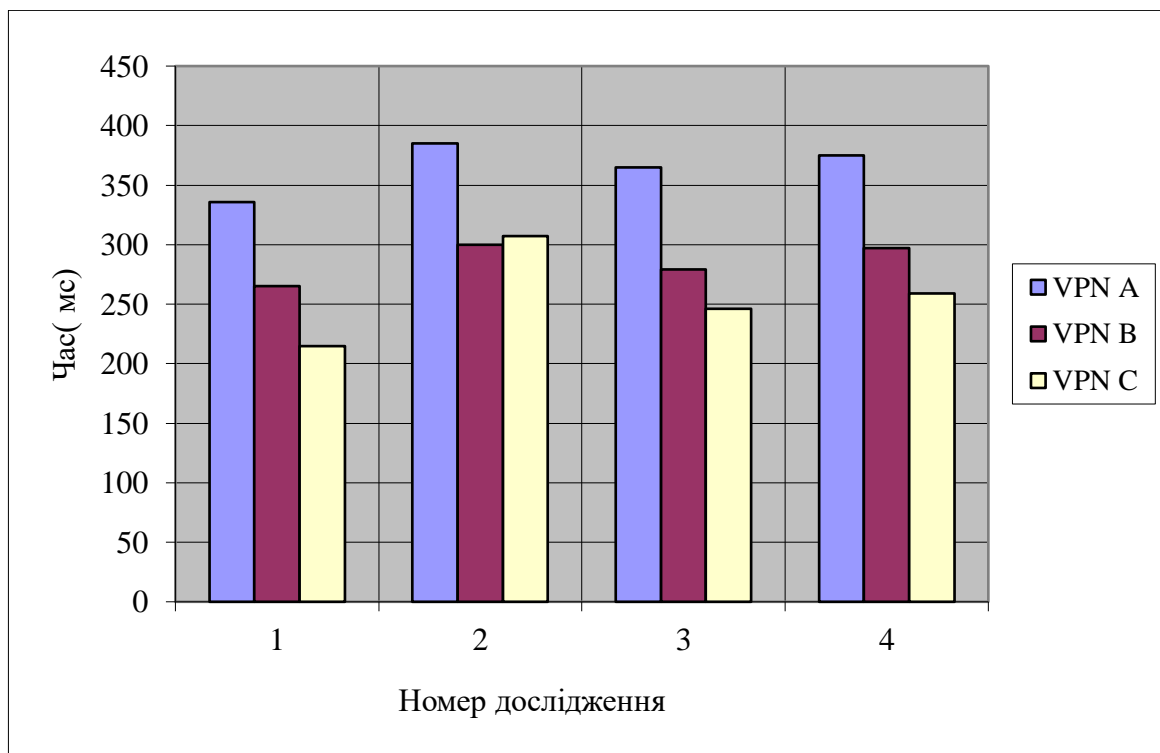


Рисунок 3.11 – Середній час затримки на кожному з етапів кожного клієнта

З отриманого графіка можна зробити висновок, що середня тимчасова затримка на кожному етапі приблизно однакова і досить мала, щоб якось вплинути на передачу даних в мережі.

Знаючи дані попередніх розділів можна розрахувати середню тимчасову затримку передачі даних в мережі для кожного клієнта віртуальної приватної мережі [27]. Для цього використовуємо дані таблиць 3.13, 3.22 і 3.31 і обчислимо для кожної середнє значення. Результат помістимо в таблицю 3.32.

Таблиця 3.32 – Середнє значення тимчасової затримки для кожного клієнта

| клієнт | Середнє значення тимчасової затримки (мс) |
|--------|---|
| А      | 370                                       |
| В      | 286                                       |
| С      | 257                                       |

Використовуючи дані таблиці 3.32 побудуємо графік і відобразимо його на рисунку 3.12

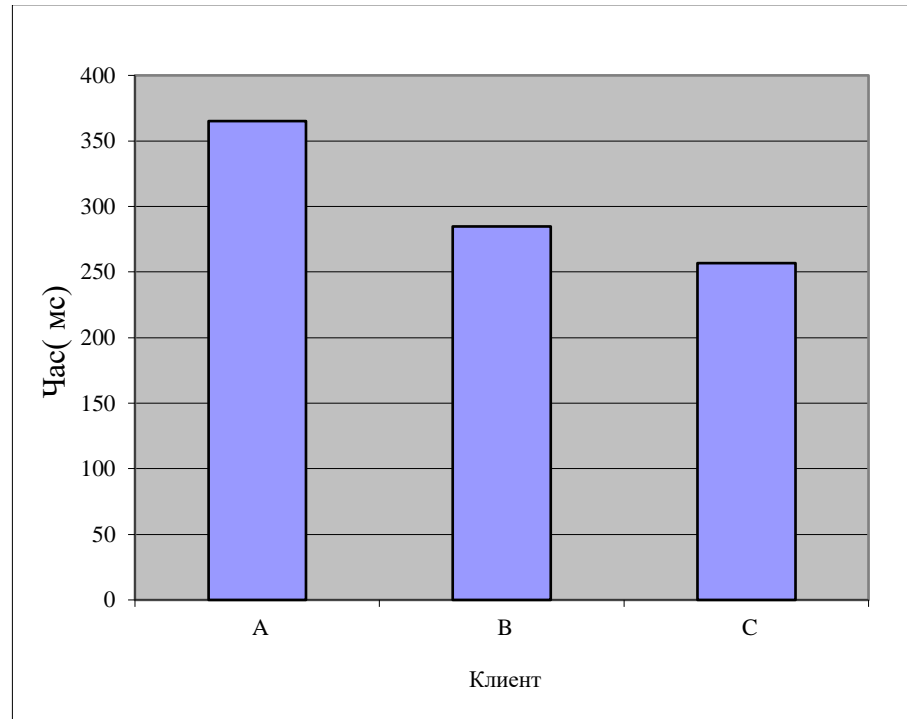


Рисунок 3.12 – Середня тимчасова затримка для кожного клієнта

Проаналізуємо результати отриманого графіка для цього побудуємо таблицю 3.33 використовуючи дані QoS і знаючи підрахувавши кількість маршрутизаторів. Для того щоб дізнатися середнє значення маршрутизаторів на шляху від однієї філії до іншої скористаємося формулою 3.1 [28]

$$N = (n1 + n2 + \dots + nk) / k \quad (3.1)$$

де  $n1$  - кількість маршрутизаторів на першому шляху;

$nk$  - кількість маршрутизаторів на  $k$ -му шляху;

$k$  - максимально можлива кількість шляхів виходять з головного офісу до клієнта.

Тоді для VPN A можна підрахувати що

$$n1 = PE1 + P1 + P3 + PE5 \text{ тобто } n1 = 4$$

$$n2 = PE1 + P1 + P3 + P5 + PE4 \text{ тобто } n2 = 5$$

$$n3 = PE1 + P1 + P2 + P4 + PE3 \text{ тобто } n3 = 5$$

Значить  $N = (4 + 5 + 5) / 3 = 4.7$ . Аналогічно можна розрахувати значення  $N$  для  $B$  і для  $C$ .

Таблиця 3.33 – Параметри мереж

| клієнт | Швидкість доступу певна QoS (Кбіт / сек) | Максимальне число пакетів в черзі | Середнє число маршрутизаторів на шляху | Середня затримка в мережі |
|--------|--|-----------------------------------|--|---------------------------|
| A      | 384                                      | 900                               | 4,7                                    | 365                       |
| B      | 512                                      | 600                               | 4                                      | 285                       |
| C      | 640                                      | 900                               | 4,5                                    | 257                       |

З таблиці 3.33 можна зробити висновок, що середня затримка в мережі не може залежати тільки від середнього числа маршрутизаторів на шляху. Це значення можна розглядати тільки як один з факторів впливає на тимчасову затримку в мережі.

Тепер, на основі отриманих даних, можна порівняти розрахункову швидкість передачі даних зі швидкістю певної QoS [29]. Для цього скористаємося формулою 3.2.

$$V = S / T, \quad (3.2)$$

де  $V$  - швидкість передачі даних;

$S$  - розмір переданих даних;

$T$  - час, за який передалися дані.

тоді

$$V_A = (18000 * 8) / 0,365 = 382 \text{ Кбіт / сек}$$

$$V_B = (18000 * 8) / 0,285 = 505 \text{ Кбіт / сек}$$

$$V_C = (18000 * 8) / 0,257 = 560 \text{ Кбіт / сек}$$

Побудуємо графік, що відображає розрахункову швидкість передачі даних з виділеною швидкістю для кожного клієнта і відобразимо його на рисунку 3.12.

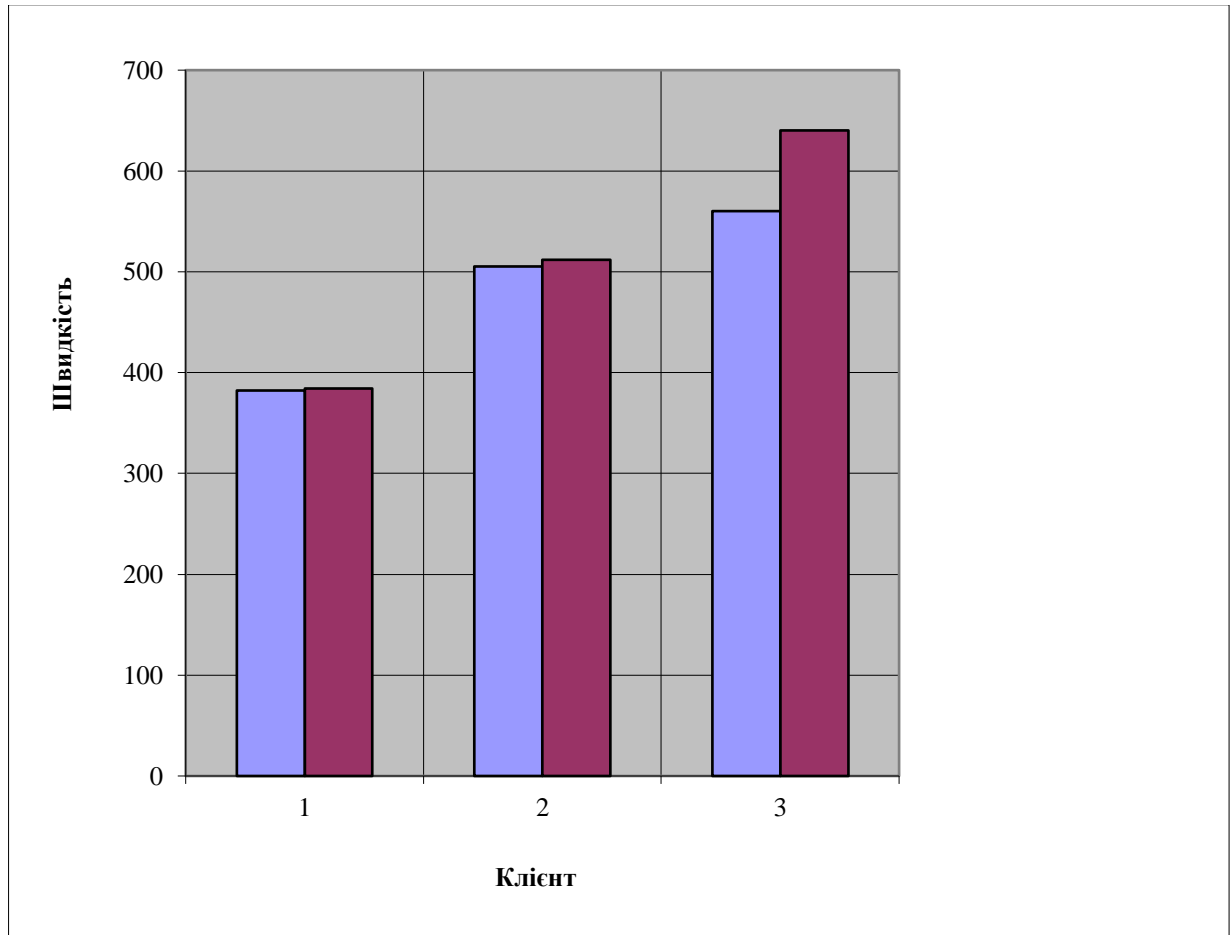


Рисунок 3.12 – Співвідношення експериментальних даних і вимог QoS

Таким чином, з рисунка 3.12 видно, що розрахункові дані швидкості передачі для всіх 3-ох корпоративних клієнтів відповідають вимогам QoS, заданим в технічному завданні. Це підтверджує те, що віртуальна модель мережі була спроектована і налаштована коректно. Швидкості передачі даних 3-ех корпоративних клієнтів не перевищують їхні тарифні плани, а саме Platinum, Gold і Silver. Кожен тарифний план підтримує швидкість доступу до 384 Кбіт / сек - для клієнта А, до 512 Кбіт / сек - для клієнта В і до 768 Кбіт / сек для клієнта С. відповідно [30].

### **3.4 Налаштування та перевірка роботи комп'ютерної системи**

#### **3.4.1 Базове налаштування конфігурації пристроїв**

Cisco базові команди та налаштування

### **show startup-config**

Відображає конфігураційний вміст, який застосовується під час завантаження. Можна скопіювати ці дані в буфер обміну і зберегти файл як бекапу конфігурації. Цей файл потім можна просто вставити (з невеликими застереженнями) з буфера обміну в екран консолі, дати команду `wr mem`, і цим відновити конфігурацію (багато програм, що автоматично зберігають та оновлюють конфігурацію, застосовують саме такий метод) [31].

### **show running-config**

Команда `show running-config` показує поточну конфігурацію пристрою. `Running-configuration` - це конфігурація, завантажена в даний момент в оперативну пам'ять роутера. Коли ви вносите зміни в обладнання, ця конфігурація змінюється. Але після перезавантаження він замінюється на **startup-config**, так що не бійтеся зіпсувати після перезавантаження все повернутись.

### **copy startup-config running-config**

Скасує всі зроблені (якщо були) зміни конфігурації. Те саме відбудеться, якщо вимкнути/включити живлення (перезавантажити пристрій).

### **copy running-config startup-config**

Зберігає в незалежній пам'яті всі зміни, зроблені в конфігурації. Повний аналог команди `write` або `write memory`.

## **3.4.2 Налаштування маршрутизаторів корпоративної мережі**

Щоб налаштувати маршрутизатор, вводимо наступні команди:



```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

Усі методи доступу до налаштувань маршрутизатора повинні бути захищені. Привілейований режим EXEC надає користувачеві повний доступ до пристрою та його налаштувань. Тому необхідно надійно захистити доступ до цього режиму.

Наступні команди дозволяють захистити доступ до користувальницького та привілейованого режимів EXEC, включає Telnet/SSH і шифрує всі паролі в конфігурації.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

Для налаштування інтерфейсів маршрутизатора необхідно ввести такі команди:

```

Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown

```

Для налаштування портів на R1 введіть такі команди:

```

R1> enable
R1# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#

```

```

R1(config)#
*Aug 1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, змінений стан
*Aug 1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, змінений стан
*Aug 1 01:43:57.447: LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, змінений стан
R1(config)#
R1(config)#
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug 1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, змінений стан
*Aug 1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, змінений стан
*Aug 1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, змінений стан
R1(config)#

```

### 3.4.3 Налаштування роботи Інтернет

Мережа складається з компонентів, повний перелік яких наведено на рис. 3.13.

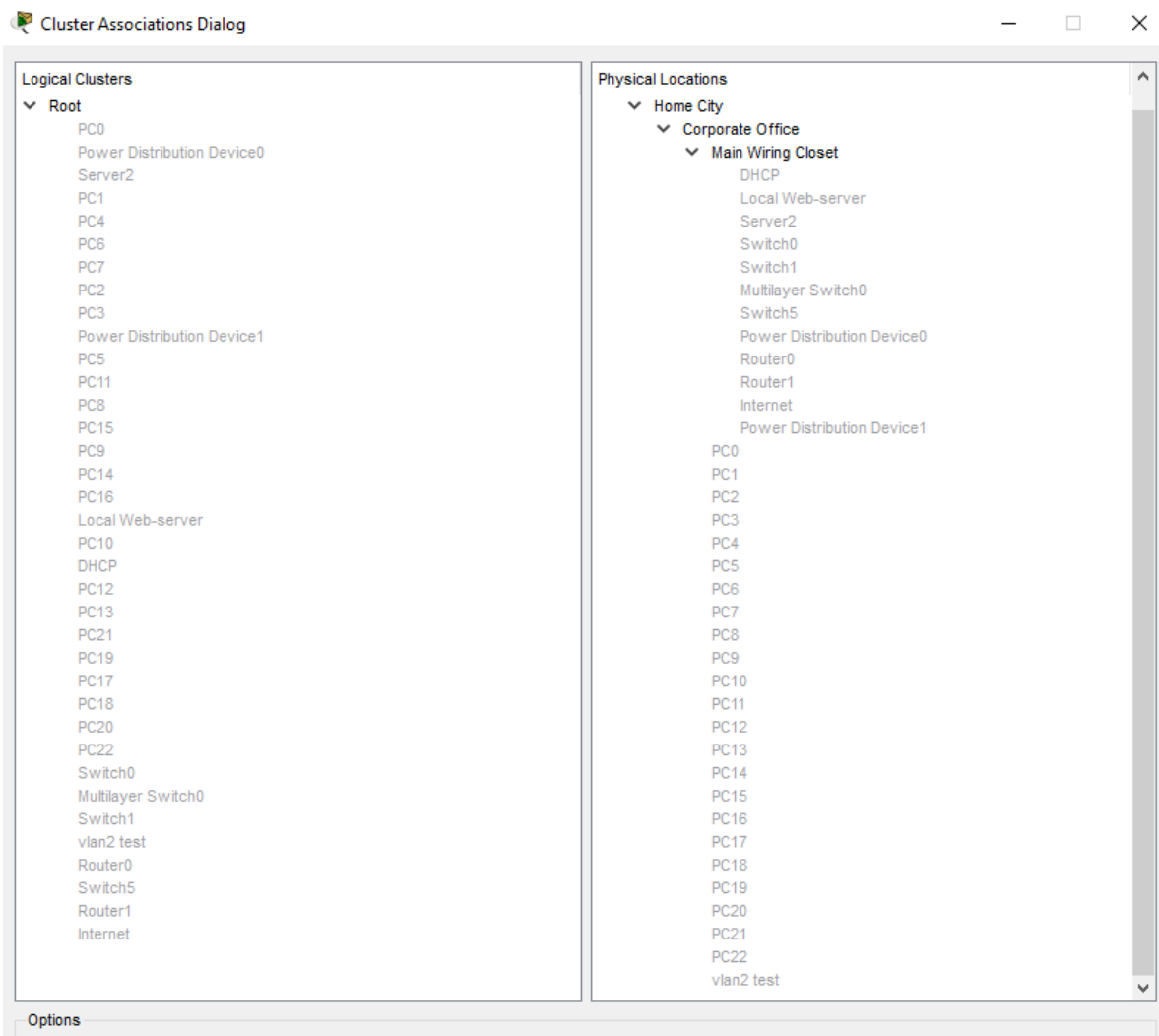


Рисунок 3.13 – Перелік компонентів мережі Інтернет

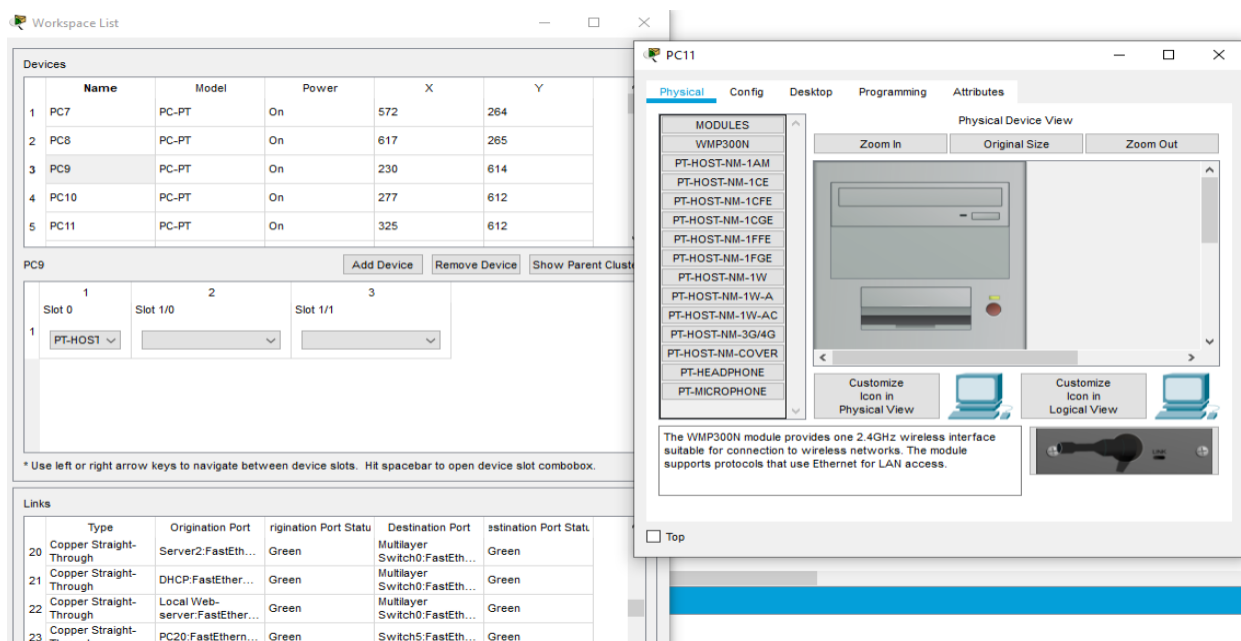


Рисунок 3.14 – Налаштування компонентів мережі Інтернет

Далі здійснимо налаштування мережі Інтернет за кожним окремим компонентом (рис. 3.14).

### 3.4.4 Перевірка роботи комп'ютерної системи

Після проведення налаштувань кожного окремого елемента здійснюємо тестування мережі (рис. 3.15-3.18)

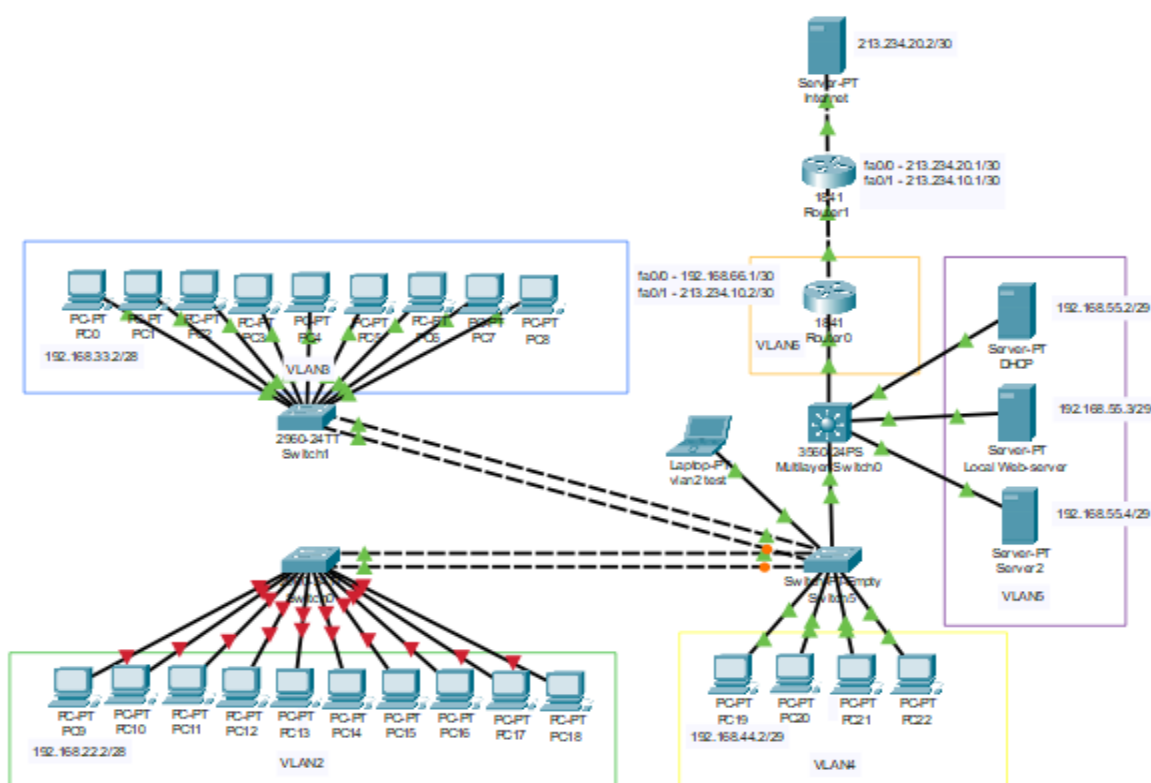
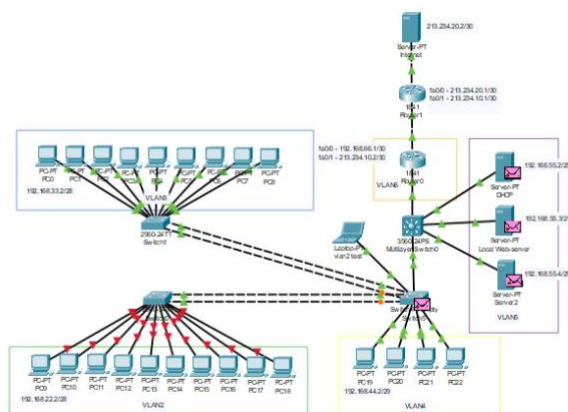


Рисунок 3.15 – Тестування мережі



Simulation Panel

| Vis. | Time(sec) | Last Device        | At Device       | Type |
|------|-----------|--------------------|-----------------|------|
|      | 0.799     | --                 | Multilayer S... | STP  |
|      | 0.800     | Multilayer Swit... | DHCP            | STP  |
|      | 0.800     | Multilayer Swit... | Local Web-s...  | STP  |
|      | 0.800     | Multilayer Swit... | Server2         | STP  |
|      | 0.800     | Multilayer Swit... | Switch5         | STP  |

Reset Simulation  Constant Delay Captured to 0.800 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, LACP, NDR, NETFLOW, NTP, OSPF, OSPFv6, RAgP, RAgP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Рисунок 3.16 – Тестування мережі

Здійснюємо пересилання повідомлень за всіма каналами.

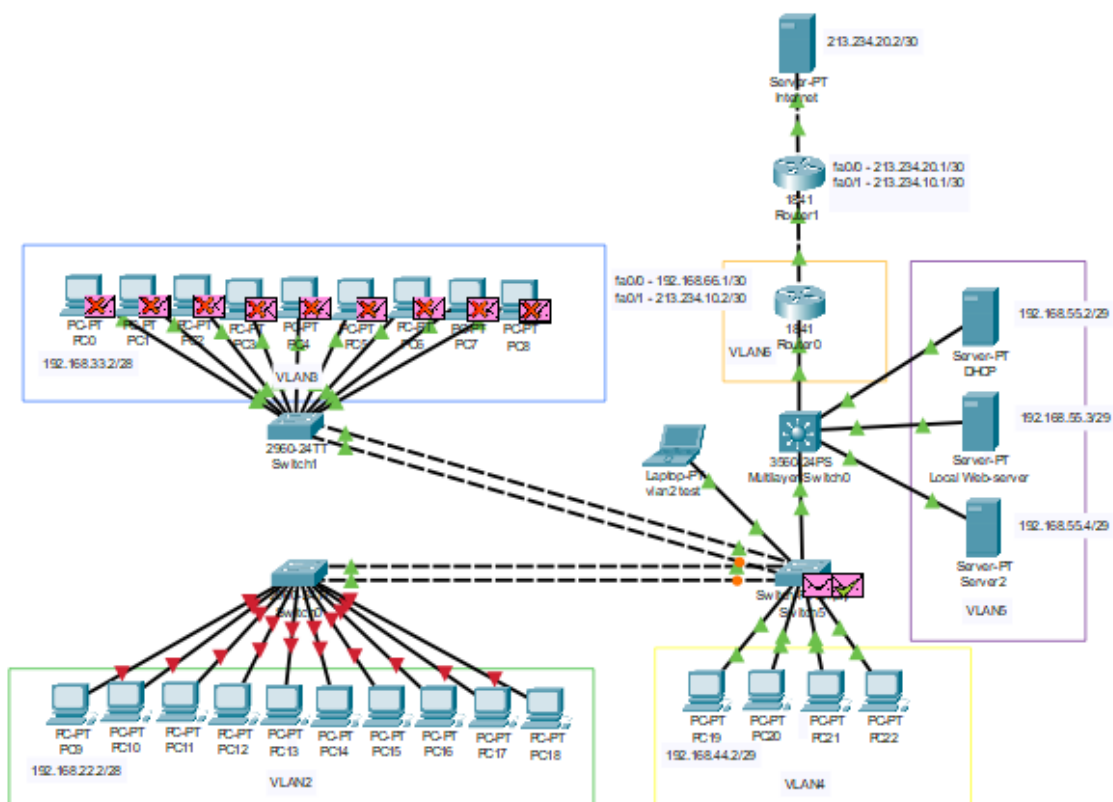


Рисунок 3.17 – Тестування мережі

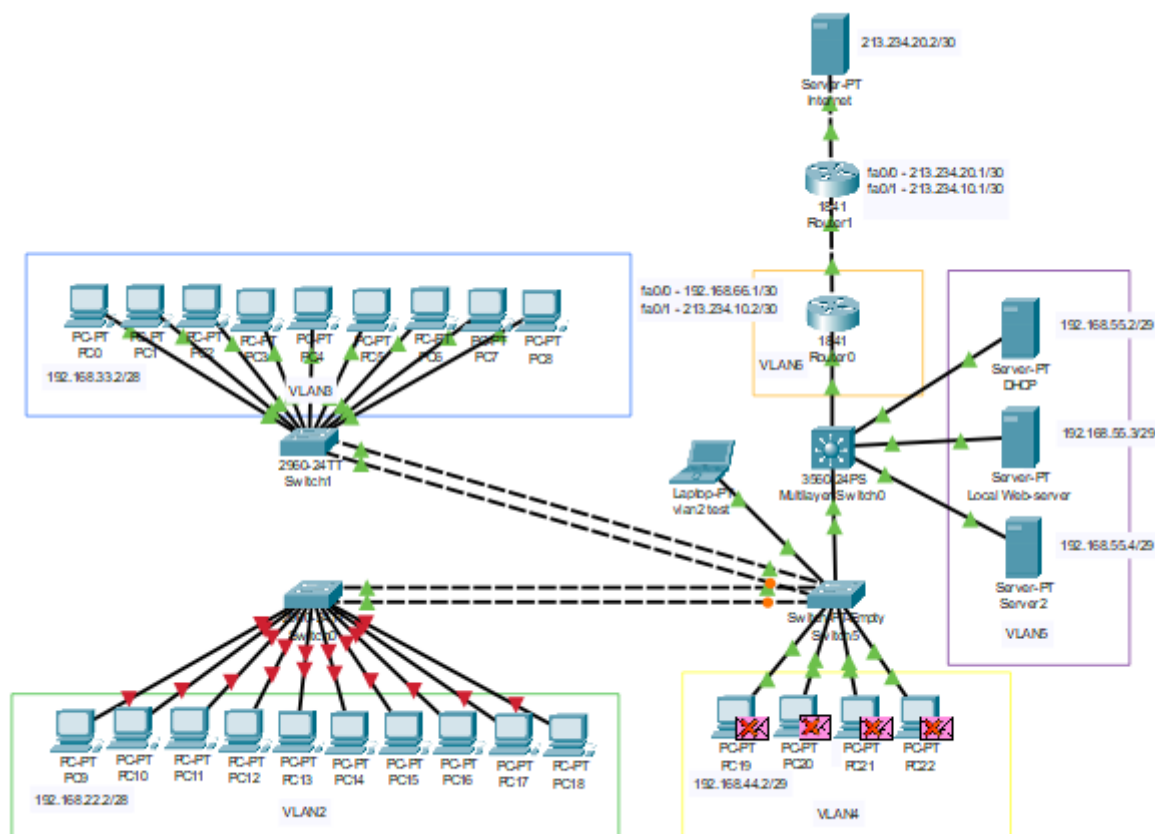


Рисунок 3.18 – Тестування мережі

## 3.5 Захист інформації в комп'ютерній системі від несанкціонованого доступу

### 3.5.1 Розробка методів для захисту інформації в комп'ютерній системі

Організаційні методи захисту інформації включають заходи, заходи та дії, які мають здійснювати посадові особи у процесі створення та експлуатації КМ для забезпечення заданого рівня безпеки інформації.

Методи захисту, які використовуються в організаціях, тісно пов'язані з правовими нормами щодо інформаційної безпеки. Для збереження інформації у відомствах, установах і компаніях (незалежно від форми власності) відповідно до законодавства створюються спеціальні служби безпеки (які зазвичай називаються по-різному). Ці послуги зазвичай залежать від нагляду керівництва. Керівники служб беруть участь у проектуванні та

експлуатації систем захисту інформації. На організаційному рівні делеговано наступні обов'язки з інформаційної безпеки щодо КМ:

- організація робіт із розробки системи захисту інформації;
- обмеження доступу на об'єкт та до ресурсів КМ;
- розмежування доступу до ресурсів КМ;
- планування заходів;
- розробка документації;
- виховання та навчання обслуговуючого персоналу та користувачів;
- сертифікація засобів захисту;
- ліцензування діяльності щодо захисту інформації;
- атестація об'єктів захисту;
- удосконалення системи захисту інформації;
- оцінка ефективності функціонування системи захисту;
- контроль за виконанням встановлених правил роботи в КМ.

Організаційні методи є основою складної системи збереження знань. Тільки за допомогою цих методів можна об'єднати технічні, програмні та криптографічні методи захисту в єдину комплексну систему, яка є законною. під час усунення загроз інформаційній безпеці будуть застосовані спеціальні методи захисту. Найбільш суттєва увага приділяється організаційним заходам при вирішенні питань побудови комплексної інформаційної системи та організації її функціонування.

### **3.5.2 Налаштування мереж VLAN**

Virtual LAN (VLAN) - це Layer 2 broadcast domain. VLAN контролюється комутатором.

Налаштування VLAN:

```

                                ! Створити новий VLAN
vlan 10

! Призначення порту як access port belonging to VLAN 10
interface fa0/1
  switchport mode access
  switchport access vlan 10

! Verify the VLAN exists, and that Fa0/1 has been assigned to it.
show vlan brief
show vlan id 10
show interfaces fa0/1 switchport

```

### 3.5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

Для з'єднання двох комутаторів, що містять VLAN-и, використовуються транки.

Якщо порт налаштований як Trunk, кожен frame цього порту включає додаткову інформацію - tag, визначальну VLAN, до якої належить цей кадр.

Припустимо, що PC1 відсилає broadcast frame. CSW1 приймає broadcast frame і повинен його відправити через транк: для цього SW1 додає до кадру tag, в якому міститься інформація, що даний кадр з VLAN 10. SW2 побачить цей tag, прибере його з кадру, і відправить даний broadcast frame на всі порти в VLAN10 .

```

                                interface fa0/23
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
show interface trunk
show interface fa0/23 switchport

```

Що буде, якщо до порту транка наблизить untagged frame? Комутатор такий кадр прийме і помістить його в Native VLAN.

За промовчаням Native VLAN є VLAN 1.

Inter-VLAN Routing здійснюється пристроєм 3-го рівня, тобто роутером.



Підключення до VLAN-ам можна здійснювати на фізичному рівні, тобто до роутера будуть підключені стільки проводів, скільки у нас є VLAN - ів.

Також можна і на роутері підняти транк, що дозволить здійснювати маршрутизацію при підключеному одному дроті:

**SW1**

```

interface fa 0/3
switchport trunk encapsulation dot1q
switchport mode trunk

```

**R3**

```

interface fa 0/0
no ip address

interface fa 0/0.10
encapsulation dot1q 10
ip address 10.0.0.1 255.255.255.0

```

Spanning Tree Protocol (STP) - протокол, що дозволяє уникнути *Layer2 Loops* у разі надмірних підключень між комутаторами.

SW1 далі розсилає запит на всі порти, включаючи і два транки. Оскільки два комутатори підключені двома зв'язками, відбудеться loop: бродкаст почне бігати по колу.

Через це SW2 це бачитиме, що кадри з джерелом MAC PC 1 будуть з'являтися по черзі з двох портів Fa0/23 і Fa0/24: таке явище називається *MAC address flapping*.

STP або 802.1D дозволяє вимкнути надлишкове підключення, тим самим розірвавши кільце.

Робота STP полягає у взаємодії комутаторів один з одним, - для цього вони обмінюються повідомленнями bridge protocol data units (BPDU).

Алгоритм роботи STP:

– STP вибирає root switch. Всі порти root switch поміщаються в стан *forwarding state*

– Кожен nonroot switch знаходить у себе один порт з найменшою *administrative cost*. Такий порт називається Root Port (RP) і поміщаються у стан *forwarding state*

– У кожному LAN segment знаходиться один Designated Port, комутатор якого має lowest cumulative root path. Цей порт міститься у стан *forwarding state*

– Всі інші порти містяться у стані blocking state

При виборі для STP використовується наступний механізм пріоритетів [25-29]:

1. Lowest root bridge ID
2. Lowest root path cost to root bridge
3. Lowest sender bridge ID
4. Lowest sender port ID

## 4 Розробка компонента системи

### 4.1 Хмарна реалізація захисту корпоративної мережі

Застосування таких хмарних технологій як PaaS і IaaS призводить до зростаючого перенесення даних в хмарні сховища, що викликає необхідність вирішення завдання забезпечення взаємодії додатків між собою і розробки ефективних платформ для інтеграції хмарних додатків і/або хмарних додатків з корпоративними.

Як наголошується в дослідженні [22], більше половини опитаних учасників ІТ бізнесу назвали проблеми в області інтеграції як основну причину відмови від використання SaaS-додатків.

Необхідність вирішення проблем інтеграції хмарних додатків призвело до створення технології інтеграційних хмарних платформ Integration Platform as Service (iPaaS). Основні ключові особливості iPaaS наступні [23]:

- iPaaS об'єднує численні хмарні сервіси з метою інтеграції та управління будь-якою комбінацією внутрішніх і зовнішніх (тобто хмарних) додатків, SOA і хмарних сервісів, процесів і даних всередині і поза організацією;
- iPaaS є еволюцією інтеграційних сервісів, що широко застосовувалися в електронній комерції як доповнення до традиційної інфраструктури додатків.

Ключовими функціями платформи iPaaS є:

- засоби підтримки потоків інтеграції;
- засобів розробки та супроводу життєвого циклу інтеграції;
- управління та моніторинг потоків додатків;
- забезпечення множинності власників додатків.

Огляд сучасного світового стану пропозицій щодо інтеграції наведено в [24]. Там же показано, що основні сучасні рішення реалізують не всі ключові функції платформи iPaaS.

Основні моделі інтеграції

Інтеграція рівня програми передбачає майже миттєве відображення змін серед інтегрованих систем. У більшості випадків такі системи подієво-орієнтовані. Тобто інтеграція полягає в здійсненні невеликих транзакцій, що відбуваються приблизно в той же час, що і дія в основній системі.

Інтеграція даних. Ця модель інтеграції за своєю суттю пакетно-орієнтована. Типовий приклад: синхронізація даних між системами за завданням планувальника. Зазвичай дані переміщуються великими обсягами, при цьому немає жорстких вимог до часу виконання. Така інтеграція виконується у фоновому режимі (щодо бізнес-процесу).

Федеративна інтеграція даних. Можна вважати цю модель інтеграції підтипом інтеграції даних. Відмінність полягає в тому, що дані беруться з федеративного джерела. Тобто, по суті, з безлічі джерел. Такий тип інтеграції характерний для компаній, у яких в парку знаходиться кілька бізнес-систем, дані з яких необхідно консолідувати для отримання загального уявлення про бізнес-процес.

Інтеграція передачею файлів. Як випливає з назви, в цьому випадку інтеграція здійснюється відправкою / отриманням файлів.

При побудові моделі системи хмарних обчислень необхідно врахувати ряд особливостей системи:

- клієнти хмарних систем обслуговують себе самі, тобто надається можливість самостійного отримання доступу до інформаційних сервісів;
- універсальність доступу клієнта до хмарної системи з використанням інформаційно-телекомунікаційних мереж;
- можливість клієнта отримати доступ до інформаційних сервісів з використанням тонких або товстих клієнтів по інформаційно-телекомунікаційному каналу зв'язку;
- висока консолідація обчислювальних ресурсів-об'єднання обчислювальних ресурсів в одній або декількох точках для обслуговування

клієнтів з можливістю динамічного розподілу фізичних і віртуальних ресурсів відповідно до запитів клієнта;

– динамічна масштабованість – можливість оперативної автоматичної зміни продуктивності в залежності від запиту Клієнта [20].

Узагальнена модель системи хмарних обчислень представлена на рис.4.1.

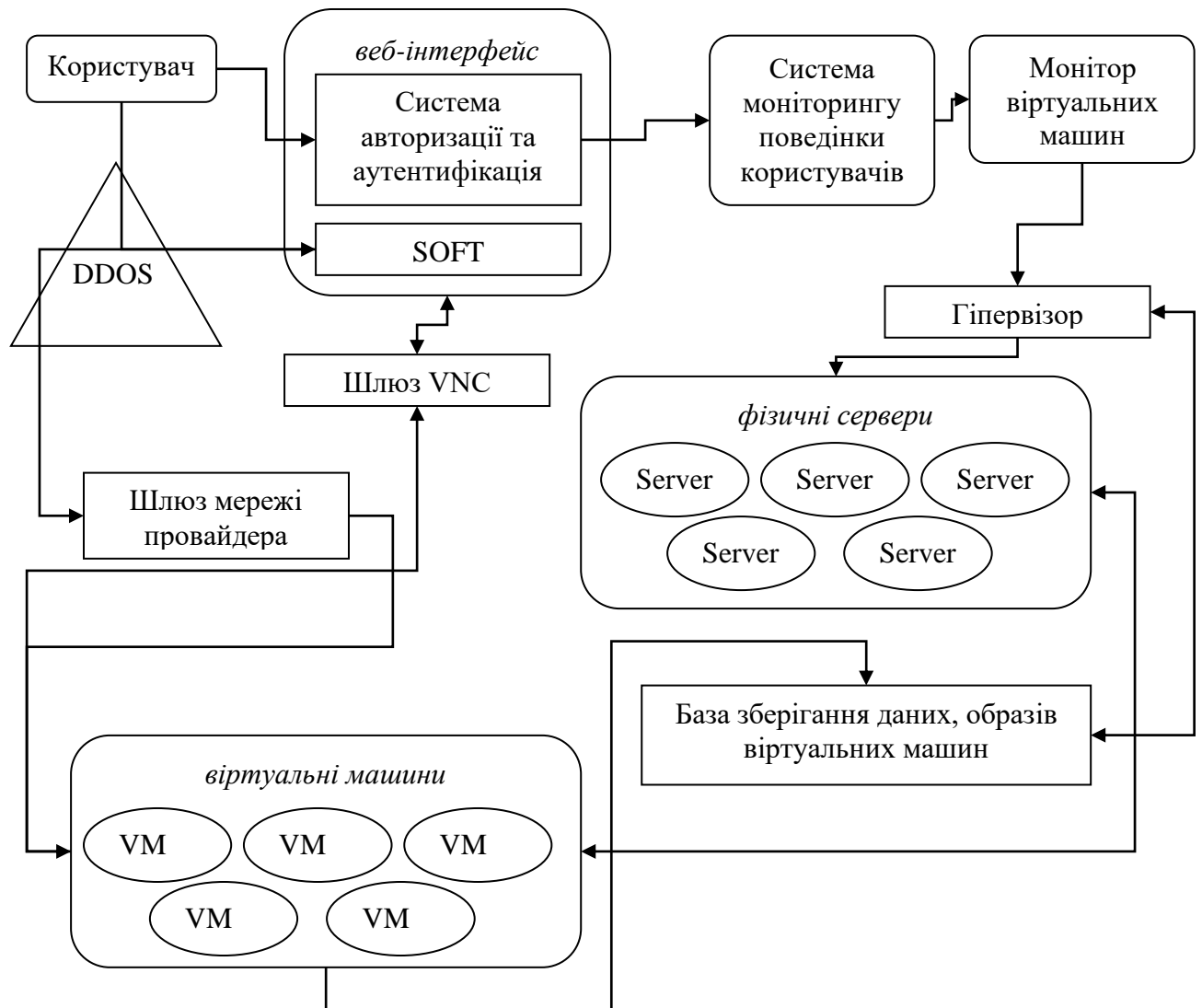


Рисунок 4.1 – Узагальнена модель системи хмарних обчислень

У узагальненій моделі ви можете спостерігати сім різних об'єктів: гіпервізор, монітор віртуальної машини, сховище даних, сховище зображень віртуальної машини, систему авторизації та автентифікації, веб-інтерфейс і систему моніторингу поведінки користувачів.

Система віртуалізації (гіпервізори) — це повна платформа віртуалізації, яка може використовувати апаратні ресурси процесора; зазвичай це реалізується гіпервізорами.

Система керування комп'ютерними ресурсами (монітор віртуальної машини) — це система, яка надає користувачам віртуальні машини, які використовують інструмент моніторингу віртуальної машини, а також розподіляє різні типи ресурсів для користувача, зокрема віртуальні мережі, віртуальне сховище даних і монітор що функціонує як частина системи.

Зберігання даних - користувачеві надається ця послуга для зберігання різних типів даних і багаторазового відтворення цих даних через віддалену веб-службу.

Зберігання образів віртуальних машин - система, яка зберігає образи віртуальних машин у різних форматах, записує доступні користувачеві образи віртуальних машин.

Система авторизації та автентичності - ця система використовується всіма учасниками системи для автентифікації та авторизації дій учасників системи.

Веб-інтерфейс — це інтерфейс, який надає користувачеві доступ.

Система моніторингу поведінки користувачів — це система, яка спирається на обмеження запитів користувачів, а також рекомендації щодо виконання цих запитів у системі хмарних обчислень, ці функції включають потенціал для запобігання несанкціонованому доступу до компонентів системи, зокрема до віртуальної машини, гіпервізора, сховища даних тощо. Модель взаємодії суб'єктів відображена на рис.4.2.

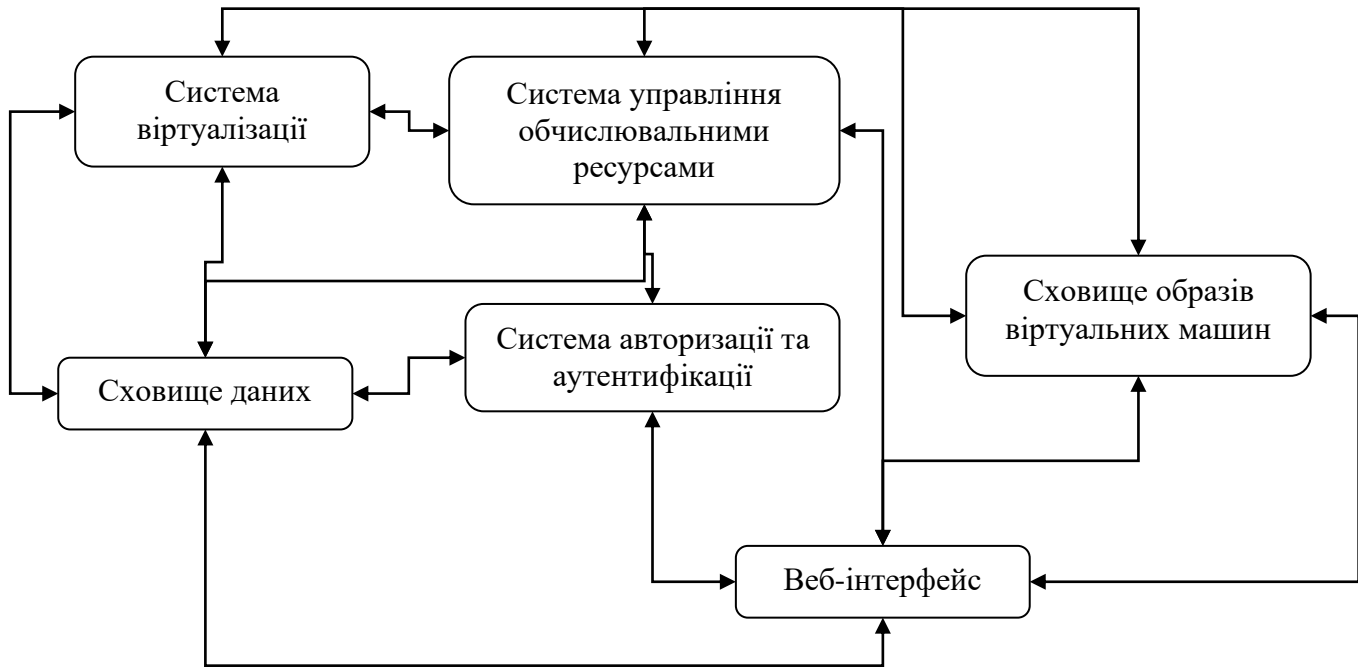


Рисунок 4.2 – Модель взаємодії суб'єктів

З рисунка 4.2 видно, що взаємозв'язок в моделі організовано між усіма елементами системи.

У роботі пропонується модернізована архітектура хмарних обчислень, вона передбачає використання 6 головних діючих акторів (табл.4.1).

Таблиця 4.1 – Актори системи хмарних обчислень

| Актор            | Визначення  |
|------------------|---|
| Користувач       | особа або організація, що використовують ресурси системи хмарних обчислень  |
| Ресурс           | сутність, що відповідає за доступність хмарного ресурсу або послуги для користувача   |
| Аудитор          | особа або організація, що виконує незалежну оцінку наданих ресурсів, послуг, обслуговування інформаційної системи, продуктивність і безпеку реалізація хмари  |
| Брокер           | сутність, що керує використанням і наданням ресурсів і послуг користувачеві. Так само встановлює взаємозв'язок між ресурсом і користувачем  |
| Оператор зв'язку | посередник, що надає послуги підключення між ресурсом і користувачем (канал зв'язку)  |
| Агент безпеки    | сутність, що формує запит від користувача до ресурсу, що визначає процеси необхідні для надання послуги або ресурсу користувачеві, що відповідає за безпечну взаємодію акторів всієї системи в цілому |

В даному випадку модель акторів використовується в якості основи для моделювання системи захисту хмарних обчислень. Ідея композиції систем акторів є важливим аспектом модульності.

На основі узагальненої моделі системи хмарних обчислень з використанням багатоагентного підходу побудуємо модель взаємодії діючих акторів у системі хмарних обчислень.

Модель взаємодії акторів представлена на рис.4.3.

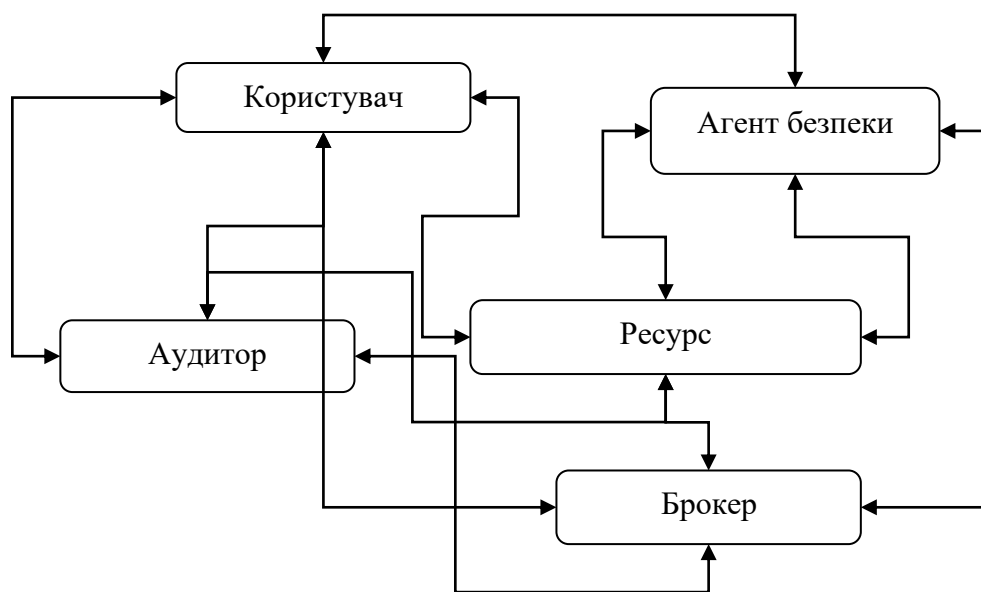


Рисунок 4.3 – Модель взаємодії акторів

Опишемо можливі варіанти сценаріїв взаємодії акторів, введений нами додатковий агент безпеки відповідає за цілісність, конфіденційність і доступність надання ресурсів і сервісів, а так само проводить моніторинг запитів користувачів системи і взаємодії акторів системи.

Сценарій 1: Хмарний користувач запитує послугу або сервіс у хмарного брокера замість прямого запиту з хмарним ресурсом. Запит Користувача формується в агента безпеки і направляється до хмарного брокера, той в свою чергу створює новий сервіс, комбінуючи набір сервісів, послуг і ресурсів. У даній моделі хмарний ресурс не візуалізується



користувачеві безпосередньо, звернення відбувається через хмарного брокера (рис. 4.4).

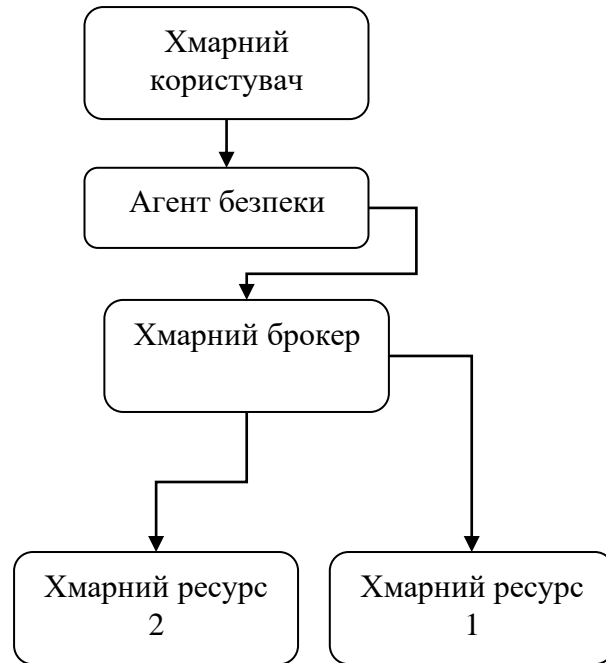


Рисунок 4.4 – Участь хмарного брокера у взаємодії користувача і ресурсу

Сценарій 2: Хмарний оператор зв'язку надає послуги підключення хмарних послуг від хмарного ресурсу до користувача (рис. 4.5).



Рисунок 4.5 – Участь хмарного оператора зв'язку в наданні ресурсів і послуг

Сценарій 3: Хмарний аудитор проводить незалежну оцінку обслуговування та безпеки реалізації хмарних послуг і сервісів (рис.4.6).

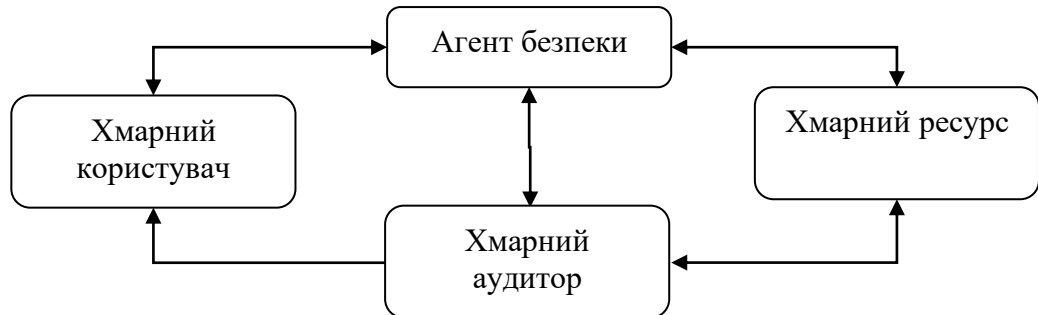


Рисунок 4.6 – Участь хмарного аудитора в оцінці наданих сервісів

Опишемо функції і ролі акторів в системі хмарних обчислень.

Хмарні користувачі поділяються за трьома групами в залежності від необхідних їм додатків (табл.4.2).

Таблиця 4.2 – Приклади і активність користувачів системи хмарних обчислень

| Тип користувача | Активність користувача   | Приклади користувачів  |
|-----------------|--|--|
| SaaS            | особа або організація використовують додатки або сервіси для автоматизації бізнес - процесів       | бізнес користувачі   |
| PaaS            | використовує додатки для розробки, тестування і управління власними проектами розгорнутими в хмарі | адміністратори системи, розробники проектів і додатків, особи, що тестують додатки |
| IaaS            | моніторить і створює сервіси та послуги для управління ІТ інфраструктурою                          | адміністратори систем, системні розробники і адміністратори, it менеджери          |

Хмарний ресурс відповідає за доступність хмарної послуги або сервісу для хмарних користувачів, вирішуючи завдання в різних сервісних моделях (табл. 4.3).

Таблиця 4.3 – Активність ресурсу

| Тип ресурсу | Активність ресурсу   |
|-------------|--|
| SaaS        | управляє, встановлює і підтримує прикладне програмне забезпечення на хмарній інфраструктурі                                |
| PaaS        | надає доступ до інформаційно-технологічних платформ і інструментів для розробки і адміністрування програмного забезпечення |
| IaaS        | управляє і надає обчислювальні ресурси і фізичні потужності системи і мереж, а також управляє хмарною інфраструктурою      |

Хмарний ресурс або сервіс розглядається як розгортання сервісів, узгодження сервісів, хмарний сервіс менеджмент, безпека і приватність (NIST) (рис.4.7).

Хмарний аудитор – особа або організація, що виконує незалежну оцінку надаваних хмарних послуг і сервісів, він може давати оцінку не тільки сервісам, але і безпеці надання послуг, а також дотримання приватності.

Хмарний брокер – сутність, що відповідає за управління і використання надаваних хмарних послуг користувачеві. Основними наданими послугами є: розширення хмарного сервісу, комбінування та забезпечення інтеграції хмарних сервісів, добірка сервісів для користувача.

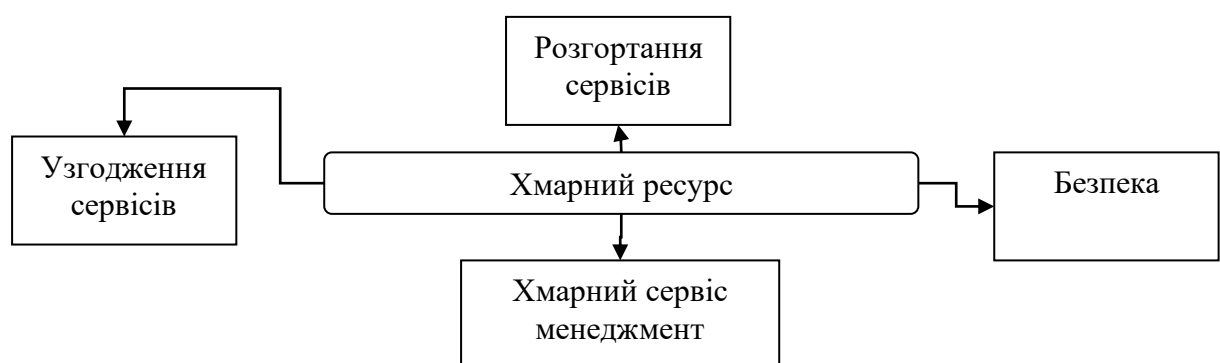


Рисунок 4.7 – Блоки хмарного ресурсу

Хмарний оператор зв'язку є посередником, що надає послуги підключення та доступ через мережеві та телекомунікаційні пристрої зв'язку, також забезпечує доставку послуг і сервісів.

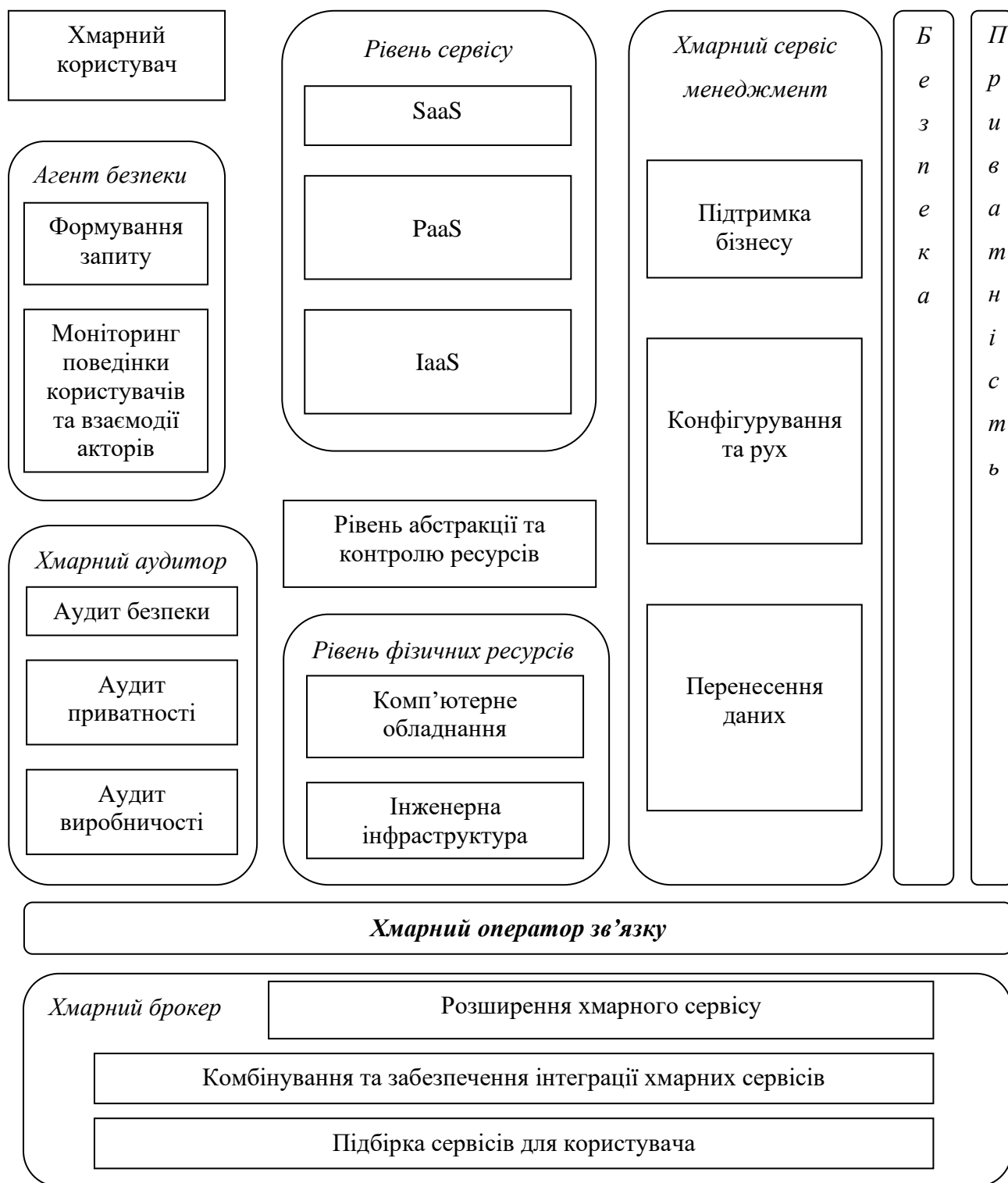


Рисунок 4.8 – Концептуальна структура захисту віртуалізованих середовищ в публічній хмарі

Концептуальна структура захисту віртуалізованих середовищ в публічній хмарі представлена на рис.4.8.

Агент безпеки – сутність, що відповідає за формування запиту від користувача до ресурсу, так само відповідає за моніторинг і адекватність запитів користувачів в системі хмарних обчислень, надає можливі варіанти запитів в разі невірних обраних дій або спроби несанкціонованого доступу до ресурсів системи хмарних обчислень, так само відповідає за взаємодію акторів в системі. Даний актор більш докладно буде описаний нижче.

Опишемо реалізацію актора з підмножиною ментальних властивостей. Ментальні властивості включають в себе: місця, агенти, міграція, з'єднання, повноваження і дозволи (permits). Опишемо перераховані поняття:

Місця – мають на увазі комп'ютерну розподілену мережу як безліч місць. Місце – стаціонарний процес на сервері, гіпервізорі або в мережі, що пропонує послуги вхідному акторові.

Агент. Агенти це комунікаційний додаток займає певне місце. Іноді агенти можуть мігрувати з місця на місце. Агентські процедури виконуються паралельно.

Міграція. Агенту надається можливість мігрувати з місця на місце. Міграція це не помітний для користувача процес не впливає на продуктивність системи. Відмінною рисою міграції є віддалений доступ до послуги або ресурсу.

З'єднання. З'єднання дозволяють агентам обмінюватися інформацією з різних місць.

Повноваження. Дана властивість дозволяють агенту або місцю розпізнавати повноваження іншого агента/місця, причому агент або місце не можуть ні приховувати, ні фальсифікувати свої повноваження. Властивість передбачає перевірку повноважень при переміщенні агента між регіонами мережі, що дозволяє захистити агентів і місця від проникнення вірусів.

Дозвіл. Дана властивість дозволяє управляти призначенням повноважень.

Агент безпеки – це сутність, що відповідає за моніторинг і адекватність запитів користувачів, за коректне відправлення запиту до інших акторів системи і взаємодія АКТР.

Щоб зрозуміти роботу даного актора необхідно проаналізувати поведінку користувача в системі хмарних обчислень.

#### **4.2 Рекомендації захисту віртуалізованих середовищ в публічній хмарі**

Модель моніторингу поведінки користувача та взаємодії акторів у хмарній системі представляє сигнатурну модель пошуку заборонених дій у системі. Запропонований алгоритм аналізу поведінки користувача в системі хмарних обчислень призначений для розробки агента безпеки.

Пропонований підхід підвищить захищеність системи за рахунок підвищення достовірності розпізнавання несанкціонованих запитів і дій користувачів, а також взаємодії акторів в системі хмарних обчислень.

Узагальнена модель поведінки користувача та взаємодії акторів у хмарній системі як цифрового автомата представлена у виразі функцією (4.1).

$$A = \{s, S_0, X, Y, \delta, \lambda\}$$

де  $S$  – поточний технологічний стан системи хмарних обчислень, обумовлений діями користувача,

$S_0$  – початковий стан системи хмарних обчислень,

$X$  – вхідний алфавіт дій користувача,

$Y$  – вихідний алфавіт реакцій системи хмарних обчислень на дії користувача,

$\delta(s, x)$  – функція переходу системи хмарних обчислень,

$\lambda(s, x)$  – функція виходів системи хмарних обчислень.

Для виконання певної процедури в системі користувач дотримується певного алгоритму дій (виконання процедур, введення даних, виконання умов, виведення даних, запит ресурсів і сервісів).

Математична модель системи хмарних обчислень, описана в цій статті, включає всі вхідні та вихідні значення, а також стан і поведінку системи для користувачів.

Так на рисунку представлена структурна схема взаємодії системи хмарних обчислень і підсистеми моніторингу поведінки користувачів і взаємодії акторів, згідно з якою вона контролює всі вхідні і вихідні значення користувача, акторів і системи в цілому, веде звіт по їх роботі, впливає на комп'ютерну підсистему для здійснення дозволених переходів згідно таблиці виходів і переходів (рис.4.9). Користувач виконує дію над комп'ютерною підсистемою під впливом попередніх дій виконаних над нею. Комп'ютерна підсистема виконує дії користувача тільки в разі дозволу підсистеми моніторингу. Контроль здійснюється за попередньо складеною таблицею виходів і переходів.

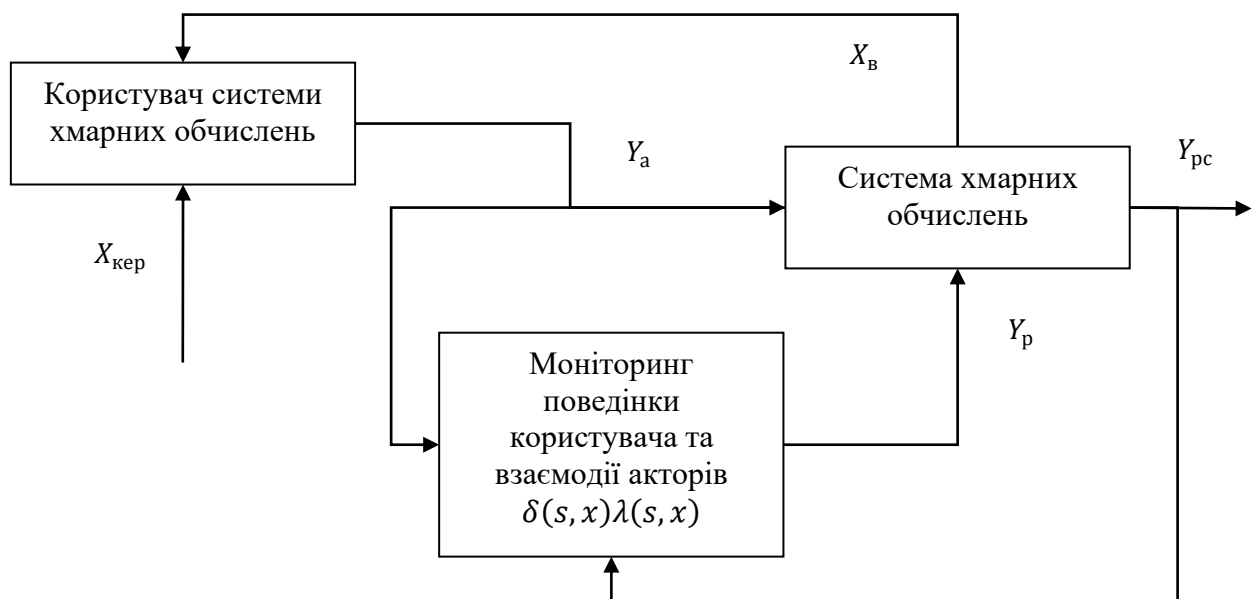


Рисунок 4.9 – Структурна схема взаємодії хмарного користувача і системи хмарних обчислень

де  $X_{кер}$  – керуючий вплив на користувача або актора,  
 $X_B$  – вплив хмарної системи на користувача або актора,  
 $Y_a$  – реакція користувача або актора на системи хмарних обчислень,  
 $Y_p$  – реакція підсистеми поведінки користувача або актора на дії користувача,  
 $Y_{pc}$  – реакція системи хмарних обчислень на дію користувача або актора (результат роботи системи хмарних обчислень).

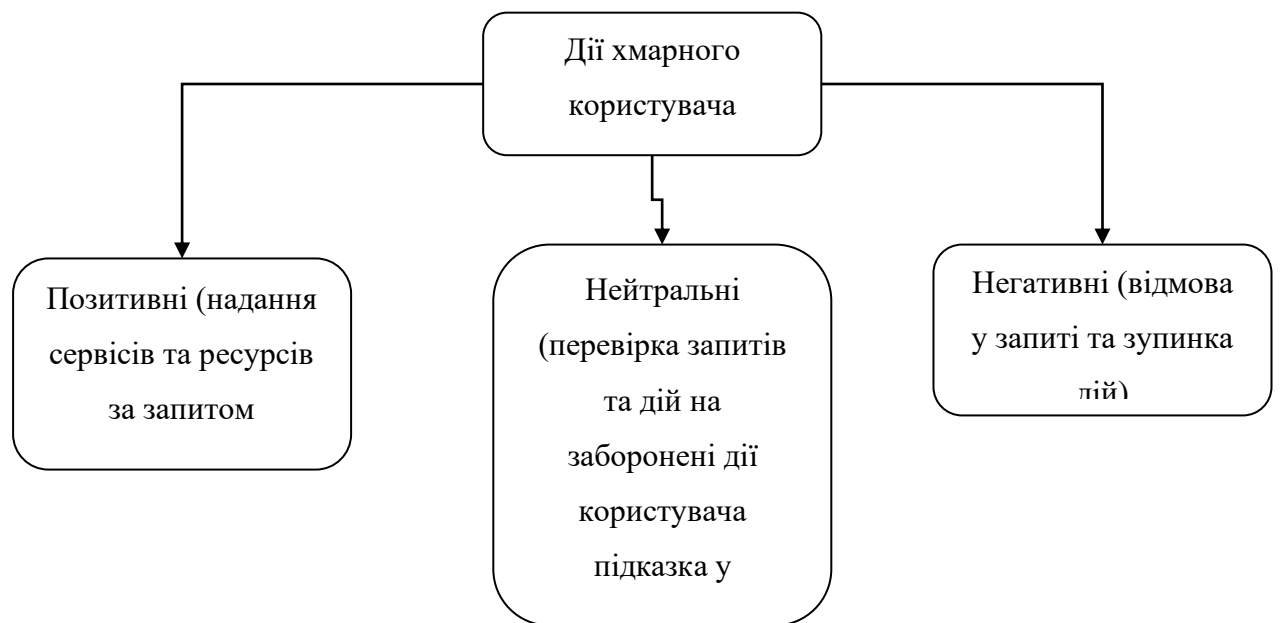


Рисунок 4.10 – Класифікація дій користувача в сигнатурному підході

Класифікація дій користувача в сигнатурному підході представлена на рис.4.10.

Залежно від типу поведінки користувача і його дій, система хмарних обчислень адекватно реагує або підказує, що необхідно зробити або блокує дії користувача. Якщо користувач робить запит на ресурси без будь-яких відхилень – система хмарних обчислень не втручається ( значення 0); в разі коли користувач має намір або не навмисно здійснює заборонену дію – система хмарних обчислень заблокує дії користувача і повідомить



адміністратора про інцидент (значення 1); у разі коли Користувач не здійснює заборонених запитів, але і не може виконати відповідну дію – система хмарних обчислень підказує користувачеві наступні запити які можна виконати в системі хмарних обчислень для отримання користувачем необхідного результату (значення 0,5).

Для того, щоб визначити можливі канали витоку інформації в системі хмарних обчислень необхідно визначити потоки інформації в системі хмарних обчислень.

Скористаємося спеціальним інструментом структурного аналізу потоку даних, який допоможе вибудувувати ієрархію даних і виявляти їх взаємозв'язки – DFD (діаграма потоків даних).

В результаті аналізу системи хмарних обчислень, виявлені наступні інформаційні потоки:

- Log-дій хмарного аудитора;
- Log-дій хмарного брокера;
- Log-дій користувачів системи хмарних обчислень;
- дані про запити і дії користувачів хмарних обчислень – відомості про стан об'єктів управління.

Графічна мова опису, моделювання систем становить основу підходу і методології IDEF0.

На рисунку представлена модель потоків інформації в системі аналізу поведінки користувача (рис.4.11).

Для розроблюваного засобу основною функцією є «аналіз аномальної поведінки користувача на основі автоматної моделі». Це буде головним блоком діаграми.

Далі необхідно визначити вхідні і вихідні потоки. Вхідними потоками є:

- Log-дій хмарного аудитора;
- Log-дій хмарного брокера;

- Log-дій користувачів системи хмарних обчислень;
- алгоритм аналізу запитів і дій хмарного актора;
- шаблони нормальних і аномальних запитів і дій.

Вихідними потоками є:

- звіти запитів і дій акторів;
- формування шаблонів запитів і дій акторів.

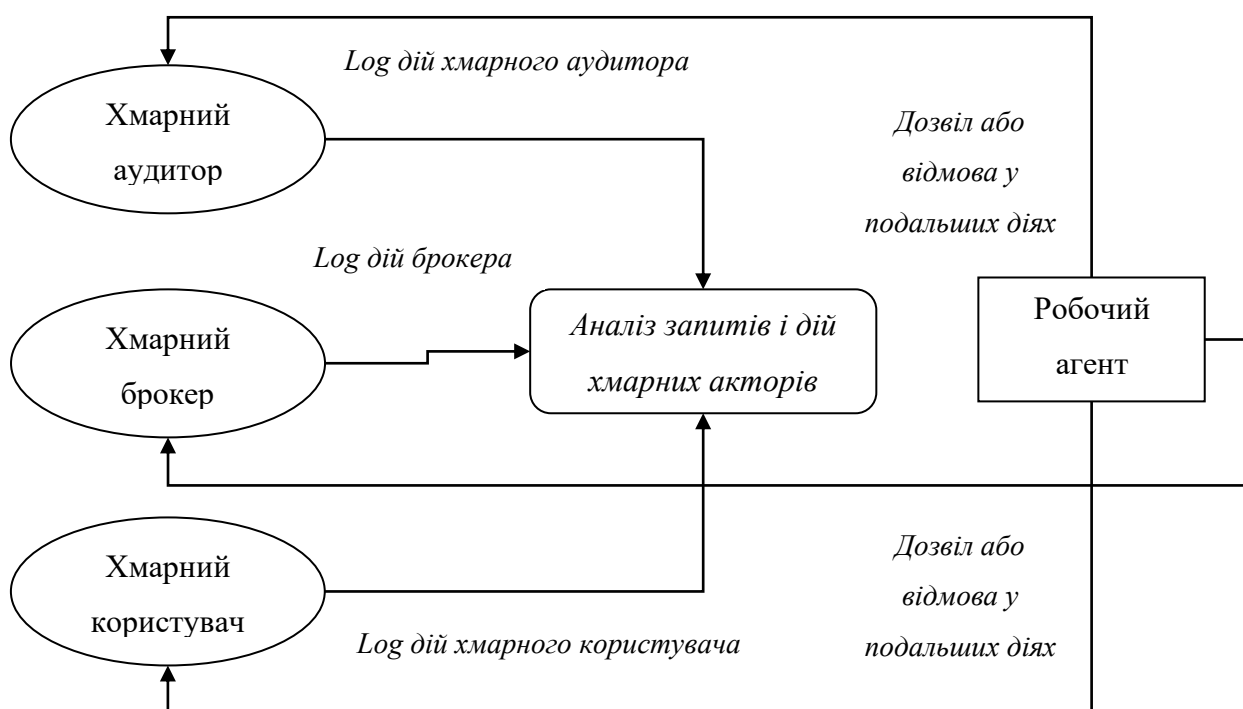


Рисунок 4.11 – Модель потоків інформації в системі аналізу поведінки користувача

Даний підхід аналізу аномальної поведінки користувачів і акторів в системі хмарних обчислень на основі автоматної моделі повинен бути елементом даної системи хмарних обчислень, що функціонують на базі віртуальної платформи і сприятиме підвищенню рівня захищеності системи хмарних обчислень.

Основним завданням системи аналізу аномальних запитів і дій акторів в системі хмарних обчислень на основі автоматної моделі є забезпечення виявлення і блокування основних загроз безпеки інформації в системі хмарних обчислень.

Даних підхід повинен бути універсальний і призначений для захисту системи хмарних обчислень як від зовнішніх, так і від внутрішніх порушників; а так само для прийняття рішення про дозвіл або заборону запитів і дій акторів системи, для цього необхідний аналіз попередніх дій і запитів акторів. В процесі функціонування системи поповнюється база сигнатур з дозволяючими і заборонними запитами і діями, так само відбувається аналіз і фіксація запитів і дій в системі хмарних обчислень.

## Висновки

В ході виконання даної роботи було досліджено питання: «Комп'ютерна система дніпровської філії мережі магазинів електроніки ТОВ «АЛЛО» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі». Запропонована модель ефективного розподілу трафіку, відображає функціональну сторону роботи маршрутизатора. Принцип роботи маршрутизатора полягає у накопиченні інформації та її рівномірному розподілі. Сучасний маршрутизатор має кілька входів, через які надходить трафік та, відповідно, кілька виходів, через які трафік пересилається до наступних мережних пристроїв. Метод розподілу навантаження реалізовано як доповнення до існуючих протоколів маршрутизації, які крім таблиць маршрутизації підтримують топологічні таблиці і володіють додатковими відомостями, що відображають стан каналів. Найбільш важливими показниками якості алгоритму ефективного балансування мережі є:

- вартість навантаження;
- скорочення втрати IP пакетів в певний період часу;
- рівномірне завантаження всіх вузлів.

Використання показника завантаженості каналів зв'язку не виключає можливості перевантажень одного з каналів зв'язку при балансуванні трафіку нерівноцінним розподілом. Максимальна пропускна здатність досягається за рахунок розрахунку коефіцієнта балансування навантаження не на основі метрики маршруту, а на основі пропускної здатності каналів зв'язку балансуючого маршрутизатора шляхом знаходження найбільшого загального дільника. Сфера застосування запропонованого алгоритму підвищення ефективності мережі шляхом штучного балансування трафіку – мінімальні пропускні здібності, які існують в маршрутах, по яких буде проводитися балансування трафіку.



## Перелік посилань

1. Главацкий С.П. Дослідження впровадження і продуктивності IPv6 / С.П. Главацкий // Вестник Херсонского национального технического университета. – Херсон, 2016. – № 59. – С. 148–154.
2. Гулиус В.А. Модель оценки производительности сети Fast Интернет / В.А. Гулиус // Матеріали X Міжнародної науково-технічної конф. “Системний аналіз та інформаційні технології” / В.А. Гулиус, А.А. Янковский. – Київ, 2008.
3. Виноградов Н.А. Исследование характеристик полезной пропускной способности в условиях меняющейся нагрузки / Н.А. Виноградов, Н.Н. Лесная, А.С. Савченко, Е.В. Колисник // Пробл. информатизації та упр. – 2009. – Вип. 4. – С. 28–31.
4. Довженко Т.П. Исследование очереди маршрутизатора в сети TCP/IP с применением основных TCP-алгоритмов активного управления очередью и предотвращения перегрузок [Електронний ресурс] / Т. П. Довженко // Зв'язок. – 2015. – № 2. – С. 22–25. – Режим доступу: [http://nbuv.gov.ua/UJRN/Zvjazok\\_2015\\_2\\_8](http://nbuv.gov.ua/UJRN/Zvjazok_2015_2_8).
5. ITU «Measuring the Information Society Report» [Електронний ресурс] // Режим доступу: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf> (25.04.2023).
6. Oleksiy Nedashkivskyu. Estimation of quality of Internet services in Ukraine // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Slavske in Lviv region, 23 February, 2016 – 26 February, 2016, p.31.
7. MEF 33 (MetroInternetForum. Technical Specification MEF 33 Интернет Access Services Definition January 2012 [Електронний ресурс] // – Режим доступу:

[https://www.mef.net/Assets/Technical\\_Specifications/PDF/MEF\\_33.pdf](https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_33.pdf)  
(27.04.2023.).

8. IEEE Std 802. – 2015I [Электронный ресурс] // – Режим доступа:  
<http://standards.ieee.org/getieee802/download/802.3-2015.zip> (27.04.2023).

9. ANSI/TIA-568.0-D, Generic Telecommunications Cabling for Customer Premises, 2015

10. ANSI/TIA-568.1-D, Commercial Building Telecommunications Infrastructure Standard, 2015

11. ANSI/TIA-568-C.2, Balanced Twisted-Pair Telecommunication Cabling and Components Standard, published 2009

12. ANSI/TIA-568-C.3, Optical Fiber Cabling Components Standard, published 2008, plus errata issued in October, 2008.

13. TIA-569-B (2004; Amd 1 2009) Commercial Building Standard for Telecommunications Pathways and Spaces

14. ANSI/TIA/EIA-606-A-2002, Administration Standard for Commercial Telecommunications Infrastructure.

15. Недашківський О.Л. Использование многопарных кабелей пятой категории – «шаг навстречу массовым продажам» // Тезисы докладов Первой международной научно-технической конференции «Проблемы информатизации». – Черкассы: ЧГТУ; Киев: ГУТ; Тольятти: ТГУ; Полтава: ПНТУ, 2013 –С. 12.

16. Adomnicăi C. Routing protocols behaviour under bandwidth limitation / C. Adomnicăi // Proc. of Int. Conf. on Information and Computer Networks. – 2012. – Т. 27. – С. 52-57

17. Awduche, D. RSVP-TE: extensions to RSVP for LSP tunnels / D. Awduche, L. Berger, D. Gan et al. – RFC 3209, December, 2001

18. Boyle, J. Applicability statement for traffic engineering with MPLS / J. Boyle, V. Gill, A. Hannan et al. – RFC 3346, 2002

19. C. Villamizar OSPF Optimized Multipath (OSPF-OMP), February 1999, [Электронный ресурс], режим доступа к журналу, <http://tools.ietf.org/html/draft-ietf-ospf-omp-02>.
20. D. E. Comer. Network interconnection with TCP IP – Principles. Protocols and Architecture // Volume L Editora Campus. – 1998.
21. Gabrielyan, E. Fault-Tolerant Streaming with FEC through Capillary Multi-Path Routing / E. Gabrielyan: Т. 3. – IEEE, 2006. – P. 1497–1501
22. Gabrielyan, E. Reliable multi-path routing schemes for real-time streaming / E. Gabrielyan, R. D. Hersch. – IEEE, 2006. – P. 65–65.
23. J. Moy. Ascend Communications, Inc. April 1998. OSPF Version 2, [Электронный ресурс], режим доступа к журналу, <http://www.ietf.org/rfc/rfc2328.txt>.
24. M. Crotti, F. Gringoli, and L. Salgarelli, Impact of Asymmetric Routing on Statistical Traffic Classification // IEEE GLOBECOM, Honolulu, Hawaii, USA, 2009.
25. N. Borovina, S. Kreso OSPF – based model of adaptive routing and possibility for stable network operations // 5th WSEAS Int. Conf. on Applied Informatics and Communication. – 2005.
26. R. Susitaival and S. Aalto Adaptive load balancing with OSPF // Networking Laboratory, Helsinki University of Technology. – 2004.
27. R. Yager, D. Filev Essentials of Fuzzy Modeling and Control. – John Wiley & Sons, 1994.
28. T. B. Pereira, L. L. Ling An adaptive OSPF routing strategy based on bandwidth estimation // Revista da Sociedade Brasileira de Telecomunicacoes. – 2003. – Vol. 18 № 1.
29. W. John, S. Tafvelin, and T. Olovsson, Passive Internet Measurement: Overview and Guidelines based on Experiences // Computer Communications, vol. 33, no. 5, pp. 533..550, – 2010.



30. Wallace K. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide / K. Wallace. – Cisco Press, 2014

31. Anvitha Prabhu, Shashank Singh, and Shridhar Dhodapkar “CEF Polarization [Электронный ресурс]. – Режим доступа: <http://www.cisco.com/c/en/us/support/docs/ip/expressforwarding-cef/116376-technote-cef-00.html>.

32. Cisco Express Forwarding Overview (техническая заметка на сайте компании Cisco) [Электронный ресурс]. – Режим доступа: <http://www.cisco.com/c/en/us/support/docs/ip/enhancedinterior-gateway-routing-protocol-eigrp/13677-19.html>

33. How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP – Режим доступа: <http://www.cisco.com/c/en/us/support/docs/ip/enhancedinterior-gateway-routing-protocol-eigrp/13677-19.html>