Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня __бакалавра____
(бакалавра, спеціаліста, магістра)

студента Булах Олександр Сергійович
(ПІБ)

академічної групи 123-17-1
(шифр)

спеціальність 123 «Комп'ютерна інженерія»
(код і назва спеціальності)

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

на тему**:** «Комп'ютерна система Департаменту патрульної поліції м. Дніпро з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Проф. Цвіркун Л.І.			
розділів:				
апаратний розділ	Доц. Ткаченко В.В.			
проектування мережі та захист інформації	Ас. Панферова Я.В.			
програмне забезпечення	Ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	Проф. Цвіркун Л.І.			

Дніпро

2021

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інформаційних
технологій та
комп'ютерної інженерії

проф._____Гнатушенко В.В.
"___" _____ 2021 р.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту Булах О.С. академічної групи 123-17-1
(прізвище та ініціали) (шифр)
спеціальності 123 «Комп'ютерна інженерія»
за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему : «Комп'ютерна система Департаменту патрульної поліції м. Дніпро з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
затверджена наказом ректора НТУ "Дніпровська політехніка" від 07.06.21 р. № 317-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	Застосувати звіт з виробничої практики, інших науково-технічних джерел та розробити технічні вимоги до комп'ютерної системи Департаменту патрульної поліції м. Дніпро	05.05.2021
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи Департаменту патрульної поліції м. Дніпро	14.05.2021
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи Департаменту патрульної поліції з опрацюванням побудови, налаштування та безпеки корпоративної мереж	31.05.2021
Графічна частина	Графічні результати розробки системи подати у вигляді рисунків електричних схем та інших креслень на 10 арк. формату А4	07.06.2021

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище та ініціали)

Дата видачі 03.02.2021 р.

Дата подання до екзаменаційної комісії 12.06.2021 р.
Прийнято до виконання _____ Булах О.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 58 с., 16 рис., 7 табл., 1 додаток, 15 джерел.

Об’єкт проектування: Комп’ютерна система Департаменту патрульної поліції м. Дніпро з опрацюванням побудови, безпеки та налаштуванням корпоративної мережі.

Мета: створення комп’ютерної системи та забезпечення робочого процесу Департаменту патрульної поліції м. Дніпро з опрацюванням побудови, безпеки та налаштування мережі.

Розроблена система має можливость зміни числа пристроїв, для збільшення робочих міссць при розширені штату.

Система виконана закритою, але дозволяє модернізувати систему, та забезпечує виконання наступних дій:

- забезпечує зв’язок між відділами;
- покращення умов використання програм працівниками;
- надає доступ працівникам до Інтернету.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу ступеня бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco PacketTracer, де перевірено її функціонування.

Результати перевірки у вигляді таблиць та рисунків і наводяться у пояснювальній записці та додатках.

ПАТРУЛЬНА ПОЛІЦІЯ, КОМП’ЮТЕРНА СИСТЕМА, КОРПОРАТИВНА МЕРЕЖА, ІНТЕРНЕТ, ПРОГРАМУВАННЯ,

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації вузла

DNS (Domain Name System) – доменна система імен

VPN (Virtual Privat Network) – захист в мережі

HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпер-текстових документів

LAN (Local Area Network) – локальна обчислювальна мережа

NAT (Network Address Translation) – протокол перетворення мережевих адрес

VLAN (Virtual LAN) – віртуальна локальна мережа

БД – база даних

ІТ – інформаційні технології

КС – комп’ютерна система

ОС – операційна система

ПК – персональний комп’ютер

ПЗ – програмне забезпечення

ВСТУП

Однією з ведучих систем сучасних технологій у світі є база даних, оскільки на їх основі можна розглянути розширення інформації у сфері Internet.

З ростом інформаційних технологій також розширюється ступінь володіння інформацією та їх обробкою, збереження та захисту. Як відомо, для зберігання та опрацювання даних використовують різні засоби: бази даних, сховища даних, оперативні сховища даних. Кожна галузь різноманітна собою та керує сферою у світі інформації [1].

В ході досліджень проаналізовано основні світові тренди розвитку інформаційних технологій, відокремлено ключові відмінностей сучасних, розглянуті соціальні мережі, штучний інтелект, Інтернет-магазини.

Розглянуті роботи, які направлені на ефективне та цілеспрямоване використання результатів впровадження КМ в управлінні корпоративною мережею Департаменту патрульної поліції.

У ході цієї роботі буде розкрита можливість покращення сервісу шляхом розширення Департаменту, створюючи додаткові підрозділи.

Оскільки налагоджений робочий процес - це найголовніша складова, а шляхом покращення роботи департаменту буде спрощенна робота та взаємозв’язок поміж підрозділами.

Патрульна поліція являється складовою Національної поліції і від надійної роботи корпоративної мережі залежить робота поліцейських по забезпеченню шромадського порядка, виявлення правопорушень, безпеки дорожнього руху та оформлення необхідних документів [2].

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Огляд галузі та умов застосування системи

Департамент Патрульної поліції м. Дніпра являється складовою поліції України і розташован за адресою площа Троїцька, 2 а.

Інформаційним технологіям притаманний імідж «середовища безмежних можливостей». Одним із напрямків – корпоративні мережі. Вони дозволяють без великих витрат підвищити якість обслуговування, запропонувавши можливості дистанційного підключення і виконання послуг за місцем вимоги.

Прикладом таких систем є портал державних послуг «Дія», який через Інтернет дозволяє отримати 27 публічних послуг. Серед них: зареєструвати авто, отримати послуги, які пов’язані з з документами воді, подати позов до суду, оформити довідку про несудимість, оформити низку ліцензій, дозволів, витяги з реєстрів, допомогу при народжені дитини тощо.

Основними перевагами такої системи є:

- це відбувається швидко;
- можна заощадити на переїздах, особливо при оформленні з віддалених місц проживання;
- багато послуг;
- детальні описи послуг, які в домашній обстановці можливо вивчити;
- відсутність нав'язливого сервісу;
- немає прив'язки до місцевості, часу доби або погоди;
- ексклюзивність;
- свобода вибору способу оплати;
- нема безпосереднього контакта із службовцями.

1.2 Огляд і характеристика об’єкта впровадження

Департамент Патрульної поліції м. Дніпра з наявними мобільними патрульними поліцейскими можна охарактеризувати, як територіально розгалужене по всіх районах міста.

Керівництво Департаменту патрульної поліції та його підрозділи розміщуються в одній багато-офісної побудови, яка розташована за адресою площа Троїцька, буд. 2 а.

Для злагодженої роботи в департаменті впроваджено розбиття на піддрозділи у відповідній ієрархії з організаційною структурою управління патрульної поліції, яка включає (рисунок 1.1): «Керівництво патрульної поліції» (Leader ship), «Бухгалтерію» (Accounting), «Оперативні групи» (Task forces), «Чергові поліцейскі» (Regular patrol), Call-Center та підрозділи − Відділ 1, Відділ 2, Відділ 3 (Departm1, Departm2, Departm13).

Для прийому заяв та викликів від населення створено Call-Center, оператори якого за визначеним алгоритмом спілкуються з населенням і оформлюють заяви, які передаться до відповіних баз і на обробку.

В залежності від виду заяв вони передпються та обробляються Оперативними групами або черговими патрульними.

Задачею бухгалтерії є фінансове забезпечення діяльності Департамента та їх співробітників.

Керівництво забезпечує розподіл задач по Департаменту та підключення до виконання інших структурних підрозділів (назвемо їх умовно Відділ 1, Відділ 2 та Відділ 3,).

Саме керівництво повиненно розуміти структурну складову кожного завдання та на які складові треба її розділити щоб досягти бажаного результату в зазначений час.

Розробка ПЗ для комп'ютерної системи Департаменту здійснюється за допомогою таких технологій, як:

- Мови програмування Java, C++, Python, PHP, HTML, CSS;
- СУБД: Oracle, IBM DB2, Sketch, Adobe XD, Figma, Unix/Linux development.

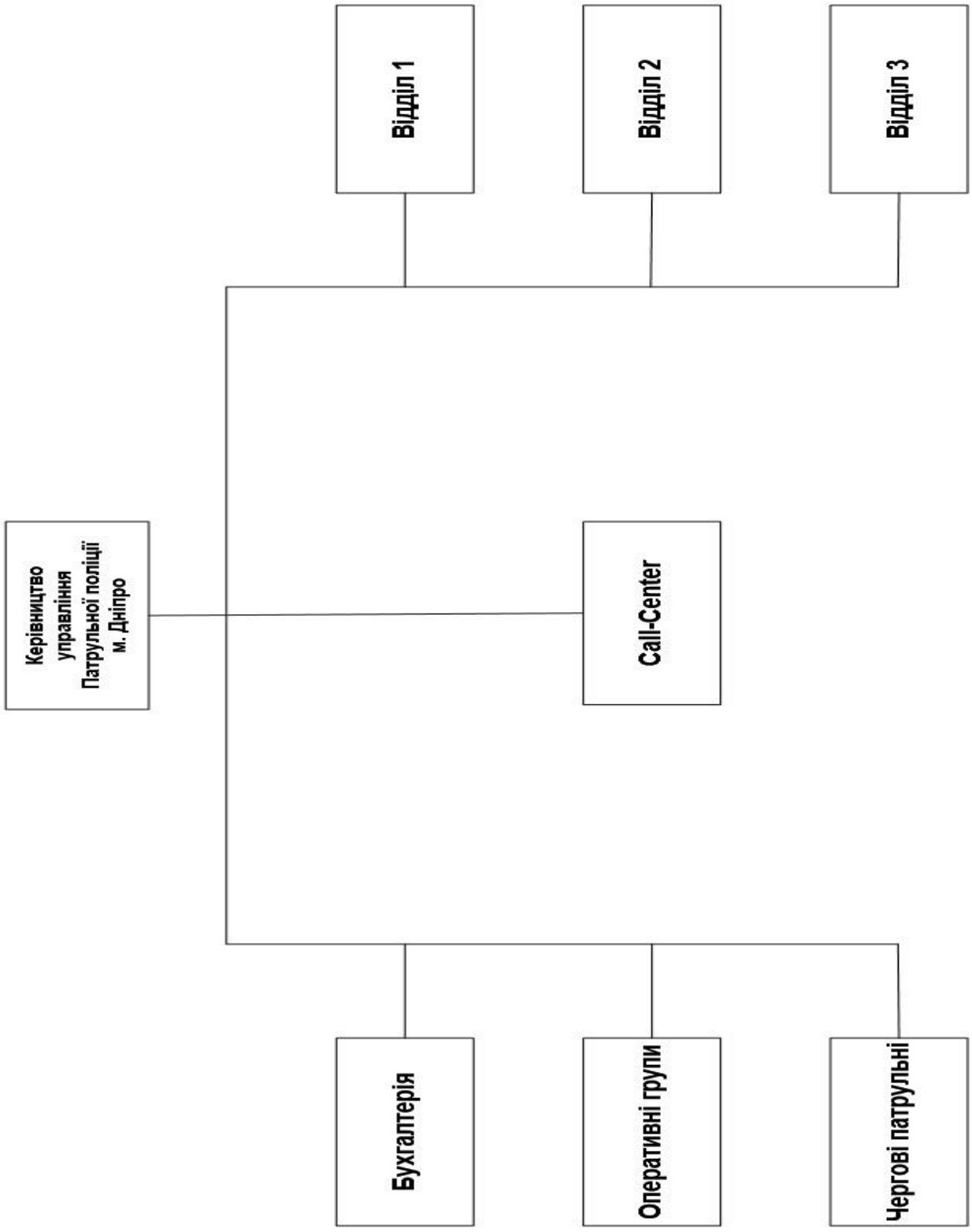

Рисунок 1.1 – Організаційна структура Департаменту управління патрульної поліції м. Дніпро

Кожна кімната Департаменту буде забезпечена охоронною системою ідентифікації ID карткою, що здає додадкове забезпечення безпеки данних, Департаменту в цілому, а також дасть змогу уникнути несанкційованого входу на територію. Крім вирішення питань контролю доступу, система здійснює облік робочого часу співробітників, що призводить до підвищення трудової дисципліни і мотивації персоналу.

Впровадження даної системи значно спрощує роботу Департаменту, позбавивши персонал від рутинного збору даних, складання звітів, відомості інформації в одну базу даних.

Департамент разташовується в 2 будівлях, з яких в одній – це Керівництво та підрозділи Департаменту, в другій − Call-Center.

1.3 Аналіз призначення та методів підготовки програмного забезпечення

У програмного забезпечення, як у живої істоти є свій життєвий цикл.

Життєвий цикл ПЗ - стадії, що проходить програмний продукт від появи ідеї до її реалізації в коді, імплементації у бізнес і подальшої підтримки. Моделі життєвого циклу багато в чому зумовлюють і методології розробки ПЗ для отримання державних послуг.

Основний процес прийняття замовлення та реалізація продукту виконується наступним чином:

- постановка завдання на розробку програмного забезпечення. На цьому етапі відбувається деталізація вимог, прив'язка їх до технології методології майбутньої розробки;
- проектування моделей взаємодії і об'єктних моделей. Цей етап служить основою кодування в процесі розробки програмного забезпечення;
- проектування баз даних. Основою для проектування баз даних є об'єктна модель, вибрана з урахуванням специфіки системи управління базою даних;

- проектування і дизайн майбутніх призначених для користувача інтерфейсів. Етап припускає розробку вибраних інтерфейсів з урахуванням того, які технології розробки по вибрані;
- тестування розробленого ПЗ. Цей етап має на увазі тестування готового пз силами незалежних підрозділів з метою контролю якості і його відповідності технічним і функціональним вимогам, що пред'являються;
- розвиток по і його технічна підтримка. Актуальність і затребуваність програмного забезпечення багато в чому визначається можливістю подальшого розвитку і удосконалення програмного продукту.

Існує деяка варіативність у проходженні етапів ЖЦ під час розробки та впровадження продукту на ринок. Для кожного продукту це відбувається по-своєму, але щоб цим якось керувати були сформульовані моделі життєвого циклу ПЗ – спрощене й узагальнене уявлення про те, як розвивається продукт.

Більш наглядно також можна продемонструвати схематично на даній таблиці, що циклічно обґрунтовує весь процес створення ПЗ від прийому замовлення до його реалізації (рисунок 1.2).

Рисунок 1.2 – Процес реалізації ПЗ в схематичному вигляді

У сучасному світі при виконанні замовлення, зазвичай впроваджується декілька моделей або прикладів виконаної роботи, замовлення має однакову платформу робочого середовища, але різний формат-дизайн оформленого ПЗ.

Комп'ютерне програмне забезпечення, або просто програмне забезпечення, являє собою набір даних чи комп'ютерних інструкцій, які наказують комп'ютеру, як працювати. Це на відміну від фізичного обладнання, з якого будується система і фактично виконує роботу. У програмній інженерії, комп'ютерна програма все відомості обробляються комп'ютерними системами, програмами та даними. Програмне забезпечення включає в себе комп'ютерні програми, бібліотеки і пов'язані з ними невиконувані дані, такі як онлайн - документації або цифрових засобів масової інформації. Комп'ютерне обладнання і програмне забезпечення вимагають один від одного, і жоден з них не може бути реально використовуватися самостійно.

Зазвичай у гарно-зарекомендованої фірми вже є приклади робочого середовища і як-раз на стадії аналізу вимог з заказчиком вирішуються найдрібніші деталі виконання замовлення, - це і є найголовнішим єтапом стадії виконання задачі. У результаті виконання процесу визначається «що робить» програмна система.

На етапі збору інформації від заказника можна виділити 3 основні етапи вимог, як зазначено на рисунок 1.3.

Рисунок 1.3 – Вимоги до заказного ПЗ

Головні питання, а саме: «Що повинна виконувати программа?», «Необхідні задачі?» та «Як її виконувати?».

В ході роботи буде використовуватись водоспадна модель проектування програмного забезпечення. Вибір тієї або іншої моделі здійснюється відповідно до обраної методології розробки програмного забезпечення.

Процес розробки складається з безлічі підпроцесів, або дисциплін, деякі з яких показані нижче. У моделі водоспаду вони йдуть одна за одною.

- Аналіз вимог − Специфікація програмного забезпечення
- Проєктування програмного забезпечення
- Програмування
- Тестування програмного забезпечення
- Системна інтеграція
- Впровадження програмного забезпечення (або Установка програмного забезпечення)
- Супровід програмного забезпечення

Водоспадна модель життєвого циклу (англ. *waterfall model*) була запропонована в 1970 р. Вінстоном Ройсом. Вона передбачає послідовне виконання всіх етапів проєкту в строго фіксованому порядку. Перехід на наступний етап означає повне завершення робіт на попередньому етапі. Вимоги, визначені на стадії формування вимог, суворо документуються у вигляді технічного завдання і фіксуються на весь час розробки проєкту. Кожна стадія завершується випуском повного комплекту документації, достатньої для того, щоб розробка могла бути продовжена іншою командою розробників.

Етапи проєкту у відповідності з каскадною моделлю:

- Формування вимог;
- Проєктування;
- Реалізація;
- Тестування;

- Впровадження;
- Експлуатація та супровід.

Переваги

- Повна і погоджена документація на кожному етапі;
- Легко визначити терміни і витрати на проєкт.

Недоліки

У водоспадної моделі перехід від однієї фази проєкту до іншого передбачає повну коректність результату (виходу) попередньої фази. Однак неточність будь-якої вимоги або некоректна його інтерпретація в результаті призводить до того, що доводиться «відкочуватися» до ранньої фази проєкту і необхідна переробка не просто вибиває проєктну команду з графіка, але часто призводить до якісного зростання витрат і, не виключено, до припинення проєкту в тій формі, в якій він спочатку замислювався. На думку сучасних фахівців, основна помилка авторів водоспадної моделі полягає у припущеннях, що проєкт проходить через весь процес один раз, спроєктована архітектура хороша і проста у використанні, проєкт здійснення розумний, а помилки в реалізації легко усуваються в міру тестування. Ця модель виходить з того, що всі помилки будуть зосереджені на реалізації, а тому їх усунення відбувається рівномірно під час тестування компонентів і системи[1]. Таким чином, водоспадна модель для великих проектів мало реалістична і може бути ефективно використана тільки для створення невеликих систем.

1.4 Задача та мета роботи

Обмін данних Департамента здійснюється через мережу Інтернет, вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим вихідним кодом допоможе для створення зашифрованих каналів типу точка-точка або сервер-клієнти між комп'ютерами та дозволить встановлювати з'єднання між комп'ютерами, що знаходяться за NAT і мережевим екраном, без необхідності зміни їх налаштувань.

На сьогоднішній час це є найпоширінішою системою передачі інформації поміж відділами компанії, та є гнучким рішенням для структурних роботи підприємстра.

Основним завданням та метою роботи Департаменту патрульної поліції є забезпечення громадського порядку та безпеки, реагування на повідомлення про правопорушення і надзвичайні події, забезпечення безпеки дорожнього руху.

Метою бакалаврської роботи є розробка комп’ютерна система, яка повинна виконувати інформаційну підтримку діям Департаменту з впровадження новітніх технологій.

1.5 Визначення напрямку вирішення поставленої задачі

Для вирішення поставленої задачі показані новітні технології, які допоможуть у розвитку обробки інформаціїї, їх сховище та захист самої мережі, як між працівниками, так і в самій мережі.

Тобто саме мережа є провідною складовою у постанові даної роботи, оскільки впровадження новітніх технологій допоможе у взаємозв’язку як із населенням, так і з іншими організаціями.

Всі необхідні заходи необхідно здійснювати для удосконалення роботи мережі та комп’ютерної систеит Департаментц патрульної поліції.

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

Комп'ютерна система, що розробляється, повинна складатись з підсистем «Керівництво патрульної поліції», «Бухгалтерії», «Оперативні групи», Call-Center та підрозділів Підрозділ 1, Підрозділ 2 та Підрозділ 3 і об'єднуватися за допомогою корпоративної мережі..

Корпоративна обчислювальна мережа - це комунікаційна мережа, яка забезпечує в межах деякої обмеженої території взаємозв'язок для широкого кола програмних продуктів. Вона підтримує зв'язок між ЕОМ, терміналами, обладнанням, забезпечує сумісне використання ресурсів. Для побудови мережі треба використати все доступні ресурси, які вже існують у компанії, а також ресурси які допоможуть її вдосконалити.

Корпоративна обчислювальна мережа буде включати нижче наведені компоненти:

- кабельна підсистема з пропускною здатністю до 1000 Мб/с;
- активне обладнання (комутатори, маршрутизатори, сервери);

Кабельна підсистема повинна будуватися відповідно до вимог стандарту ISO / IEC 11801 Class D, категорія 5E.

Загальна кількість автоматизованих робочих місць - 90.

Максимальна довжина кабелю від інформаційного порту RJ-45 до комутаційної панелі не повинна перевищувати 80 м.

Локальна обчислювальна мережа в цілому повинна відповідати категорії не нижче 5E, всі комплектуючі (кабель, розетки, комутаційні панелі, з'єднувальні шнури) повинні відповідати категорії не нижче 5E.

Для створення корпоративної обчислювальної мережі необхідно використовувати тільки компоненти відповідно до вимог ISO 9001 (ГОСТ 40.9001-88).

Всі кабельні системи корпоративної обчислювальної мережі мають бути виконані з урахуванням вимог щодо фізичного захисту трас від пошкодження:

- прокладку кабелю за металевими жолобами і в кабель-каналах, що забезпечить від ушкодження каналів;

- кріплення кабелю по всій трасі за допомогою спеціальних стяжок по всій довжині.

Структурована кабельна система представляє свого роду «конструктор», за допомогою якого проектувальник мережі будує потрібну йому конфігурацію зі стандартних кабелів, з'єднаних стандартними роз'ємами й комутують на стандартних кросових панелях. При необхідності конфігурацію зв'язків можна легко змінити — додати комп'ютер, сегмент, комутатор, вилучити непотрібне обладнання, а також поміняти з'єднання між комп'ютерами й концентраторами.

Кількість автоматизованих робочих місць може бути змінено підрядником за погодженням із замовником на етапі проектування локальної обчислювальної мережі.

Всі порти RJ-45 розташовані на робочих місцях, а так само на комутаційної панелі в комутаційній шафі повинні бути промарковані таким способом, що б їх можна було однозначно ідентифікувати. Маркування повинна бути виконана друкарським способом.

Технологія прокладки кабелю повинна забезпечувати збереження естетичного вигляду приміщень після виконання монтажних робіт.

Застосувати уніфіковані типи кабелів і роз'ємів в рамках робочих місць, все повинно устатковано залежно до стандартів комп’ютерної мережі, магістралі повинні бути вкрити захисною оболонкою для уникнень ушкоджень, а також для комфортної роботи самими працівниками.

2.2 Вимоги до функцій, що виконуються системою

Ще одною характеристикою надійності є відмовостійкість (fault wrance). У мережах під відмовостійкостю розуміється здатність системи сховати від користувача відмову окремих її елементів. В відмовостійкій системі відмова одного з її елементів приводить до деякого зниження якості її роботи, а не до повного останову.

Ключові елементи системи повинні існувати в декількох екземплярах, щоб при відмові одного з них функціонування системи забезпечували інші.

Також треба виділити 3 необхідні підсистеми для захисту даних:

Підсистема керування доступом має забезпечувати: ідентифікацію, аутентифікацію і контроль за доступом користувачів (процесів) до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроях, програм, каталогів, файлів, записів і т. д.; керування потоками інформації, очищення областей, що звільняються, оперативної пам'яті і зовнішніх накопичувачів.

Підсистема реєстрації й обліку виконує: реєстрацію й облік доступу до ІС, видачу вихідних документів, запуск програм і процесів, доступ до файлів, що захищаються; передачу даних по лініях і каналах зв'язку, реєстрацію зміни повноважень доступу, створення об'єктів доступу, що підлягають захисту, облік носіїв інформації, оповіщення про спроби порушення захисту.

Криптографічна підсистема передбачає: шифрування конфіденційної інформації, шифрування інформації, що належить різним суб'єктам доступу (групам суб'єктів), з використанням різних ключів, використання атестованих (сертифікованих) криптографічних засобів.

Число портів активного обладнання повинно забезпечувати функціонування 100% автоматизованих робочих місць і мати додатковий запас не менше 15%.

Обладнання повинно функціонувати 24 години на добу, 7 днів на тиждень, без урахування часу необхідного для проведення регламентних робіт відповідно до рекомендацій виробника.

У випадку не працездатності робочої станції у не робочий час, що була можливість перейти на іншу робочу станцію для продовження робочого процесу.

Відділи повинні підтримувати зв'язок один між одним, також між співробітниками має бути налагоджена система ієрархічного доступу. Повинна бути налагожена робота між підрозділами для гнучкого вирішення задач у найшвидший проміжок часу, працездатність системи цілодобово.

2.3 Вимоги до видів забезпечення

2.3.1 Вимоги до інформаційного забезпечення

Працівник має право на:

- надання йому роботи, обумовленої трудовим договором;
- надання робочого місця, відповідне державним нормативним вимогам охорони праці та умов, передбачених колективним договором;
- повну достовірну інформацію про умови праці та вимоги охорони праці на робочому місці;
- професійну підготовку, перепідготовку та підвищення своєї кваліфікації в порядку, встановленому Трудовим кодексом України.
- отримання матеріалів і документів, ознайомлення з проектами рішень керівництва підприємства, що стосуються його діяльності;
- взаємодія з іншими підрозділами роботодавця для вирішення оперативних питань своєї професійної діяльності;
- представляти на розгляд керівництва пропозиції з питань своєї діяльності.

2.3.2 Вимоги до лінгвістичного забезпечення

Розробка програм повинна вестися з використанням мов високого рівня C++ або Python.

Взаємодія клієнтів з системою організована українською або англійською мовами на вибір користувача.

Інтерфейс клієнта повинен бути зрозумілим, простим і розроблений з обліком наступний принципів:

− використовування довідників і шаблонів для введення даних;

− використовування підказок при неправильних діях користувача;

− наявність довідкової інформації по роботі в системі.

2.3.3 Вимоги до технічного забезпечення

Вимоги до технічного забезпечення представлені в таблиці 2.1 та 2.2.

Таблиця 2.1 - Технічні вимоги до маршрутизатора

Тип	Характеристика
Процесор	ARM, не менш ніж, 680MHz
Пам'ять	Не менш ніж: 256MB DDR
Жорсткий диск	Не менш ніж: 512MB на чипі пам'яті NAND, microSD слот
Ethernet порти	Не менш ніж: П'яти 10/100/1000 Mbit/s Ethernet портів з підтримкою Auto MDI/X
Працездатність у режимі брандмауера	Не менш ніж 1 Гбіт/с
Підтримка протоколів маршрутизації RIP, OSPF, BGP	Так
Підтримка EoIP тунелів	Необмежено
Підтримка PPPoE тунелів	Не менш ніж 500
Підтримка PPTP тунелів	Не менш ніж 500
Підтримка L2TP тунелів	Не менш ніж 500
Підтримка OVPN тунелів	Необмежено
Підтримка VLAN інтерфейсів	Необмежено
Правила брандмауэра P2P	Необмежено
NAT правила	Необмежено
Активних користувачів Хот-Спот	500

Таблиця 2.2 - Технічні вимоги до комутатора

Тип	Характеристика
Кількість портів Gigabit Ethernet 10/100/1000	Не менш ніж: 8-24 порти
Кількість портів SFP	Не менш ніж: 4 слоти
Пропускна здатність	Не менш ніж: 48 Гбіт/сек; 35.7 Mpps
Системна пам'ять memory	Не менш ніж: 128 Мбайт
Об'єм буфера пакетів	Не менш ніж: до 0.75 Мбайт
Вбудована флеш-пам'ять	Не менш ніж: 32 Мбайт
Розміри бази данних адрес	Не менш ніж: 8000 MAC-адрес
Кількість VLAN	Не менш ніж: 1024
Кількість транків	Не менш ніж: 64
Кількість черг	Не менш ніж: 8
Кількість маршрутизованих VLAN	Не менш ніж: 32

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ДЕПАРТАМЕНТУ

3.1 Обґрунтування вибору мережевої технології та середовища передачі даних

У ході проектування комп'ютерної мережі буде використовуватись технологія локальної мережі, вона звичайно займає обсяг одного чи декількох поряд розміщених будинків. Кількість пристроїв, що складають мережу, типово не перевищує декількох тисяч. Невеликі локальні мережі (20-35 робочих місць) можуть утворювати єдину робочу групу.

Даний проект буде реалізовано з використанням технології Fast Ethernet ураховуючи розміщення будівель та структуру розміщення мережі, середовища передачі даних віступає 100Base-TX на основі кабелю UTP категорії 5e.

3.2 Обґрунтування вибору мережевої технології та середовища передачі даних

Fast Ethernet (FE) - загальна назва для набору стандартів передачі даних в комп'ютерних мережах за технологією Ethernet зі швидкістю до 100 Мбіт / с, на відміну від вихідних 10 Мбіт / с.

Стандарт Fast Ethernet визначає три типи середовища передачі сигналів Ethernet зі швидкістю 100 Мбіт/с:

- 100Base-TX - дві кручені пари проводів. Передача здійснюється відповідно до стандарту передачі даних в крученому фізичному середовищі, розробленому ANSI (American National Standards Institute - Американський національний інститут стандартів). Кручений кабель для передачі даних може бути екранованим або неекранованим. Використовує алгоритм кодування даних 4B/5B і метод фізичного кодування MLT-3.

- 100Base-FX - дві жили волоконно-оптичного кабелю. Передача також здійснюється відповідно до стандарту передачі даних у волоконно-оптичному середовищі, який розроблений ANSI. Використовує алгоритм кодування даних 4B/5B і метод фізичного кодування NRZI.

Специфікації 100Base-TX і 100Base-FX відомі також як 100Base-X

- 100Base-T4 - це особлива специфікація, розроблена комітетом IEEE 802.3u. Відповідно до цієї специфікації, передача даних здійснюється за чотирма крученим парам телефонного кабелю, який називають кабелем UTP категорії 3. Використовує алгоритм кодування даних 8B/6T і метод фізичного кодування NRZI.

  Порівняльні характеристики можна побачити в Таблиці 3.1

Таблиця 3.1 – Порівняльні характеристики Fast Ethernet

фізичний інтерфейс	100Base-FX	100Base-TX	100Base-T4
порт пристрої	Дуплекс SC	RJ-45 (8P8C)	RJ-45 (8P8C)
Середовище передачі	Оптичне волокно	Вита пара UTP Cat. 3,4,5	Вита пара UTP Cat.5 (5e)
сигнальна схема	4B / 5B	4B / 5B	8B / 6T
бітове кодування	NRZI	MLT-3	
Число кручених пар / волокон	2 волокна	2 кручених пари	4 кручених пари
протяжність сегмента	До 412 м (ММВ), до 2 км (дуплекс, ММВ), до 100 км (ОМВ)	До 100 м	До 100 м

Додатково стандарт Fast Ethernet включає рекомендації по використанню кабелю екранованої крученої пари категорії 1, який є стандартним кабелем, традиційно використовується в мережах Token Ring. Організація підтримки і рекомендації по використанню кабелю STP в мережі Fast Ethernet надають спосіб переходу на Fast Ethernet для покупців, що мають кабельну розводку STP.

Специфікація Fast Ethernet включає також механізм автоузгодження, що дозволяє порту вузла автоматично налаштовуватися на швидкість передачі даних - 10 або 100 Мбіт/с. Цей механізм заснований на обміні пакетів з портом концентратора

або перемикача. Це і буде основною опорною функцією та роботою у проектованій мережі.

Виходячи з наведеного опису технології, можна визначитися з середовищем передачі, так як є найпотужнішою у впроваджені мережі такого маштабу та допоможе у її розширені у майбутньому, що показує гнучкість данної технології.

3.2 Схема проектованої корпоративної мережі Департаменту

Будівлі Департаменту та Call-Center розташовані один від одного на приблизній відстані до 200 метрів. Також у кожне приміщення впроваджене підключення від 2 провайдерів мережі Internet, що надає можливість 24 добової роботи підприємства у цілому. Треба враховувати перебої на лінії, стихійні лиха, технічні роботи провайдера, що дасть можливість гнучко перепідключатись поміж провайдерів до мережі. Топологічна схема розміщення Департаменту роедставлена на рис. 3.1, логічна схема – на рис. 3.2, фізична топологія – на рис. 3.3.

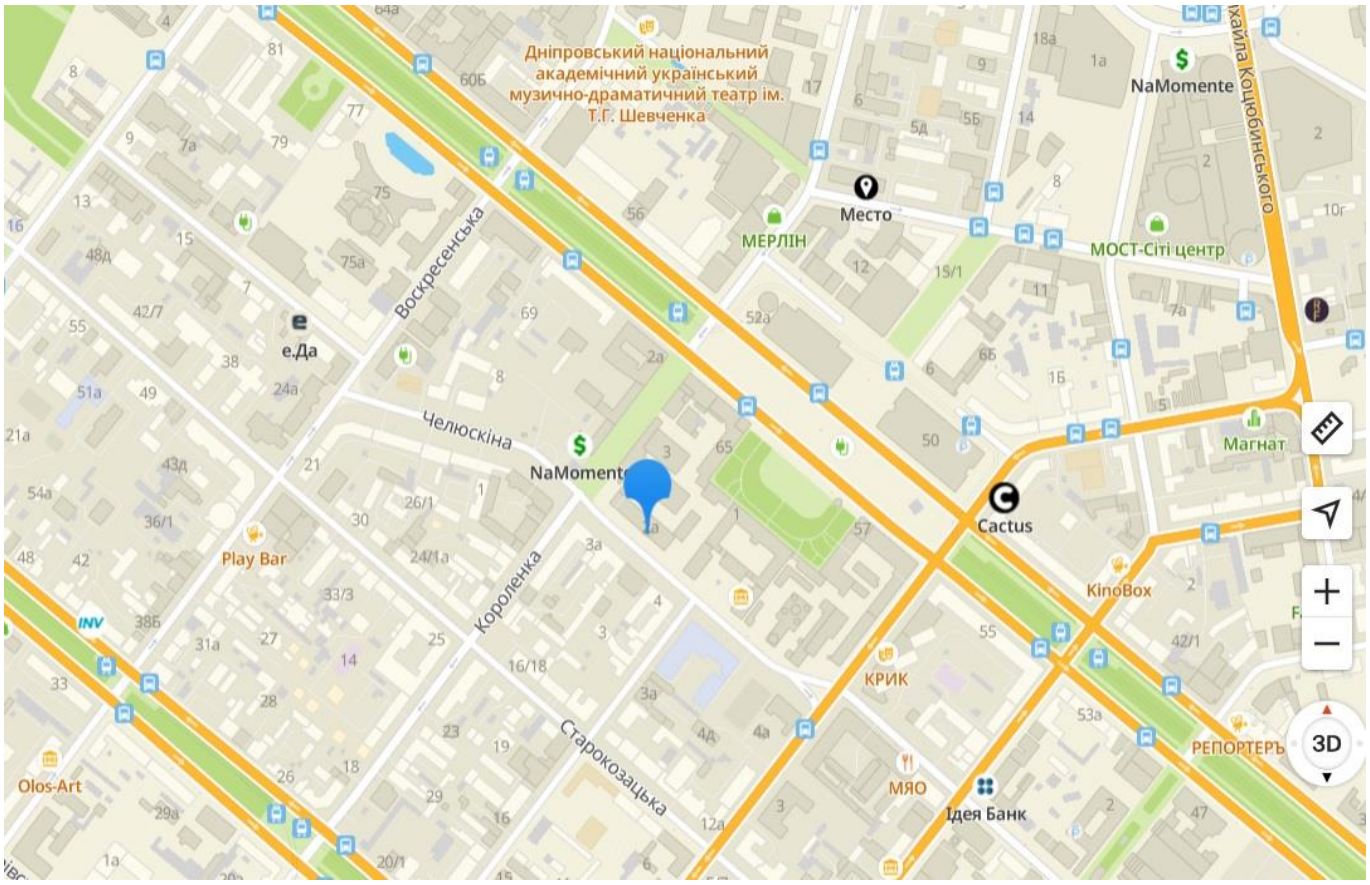

Рисунок 3.1 – Топологічна схема розміщення Департаменту патрульної поліції м. Дніпро

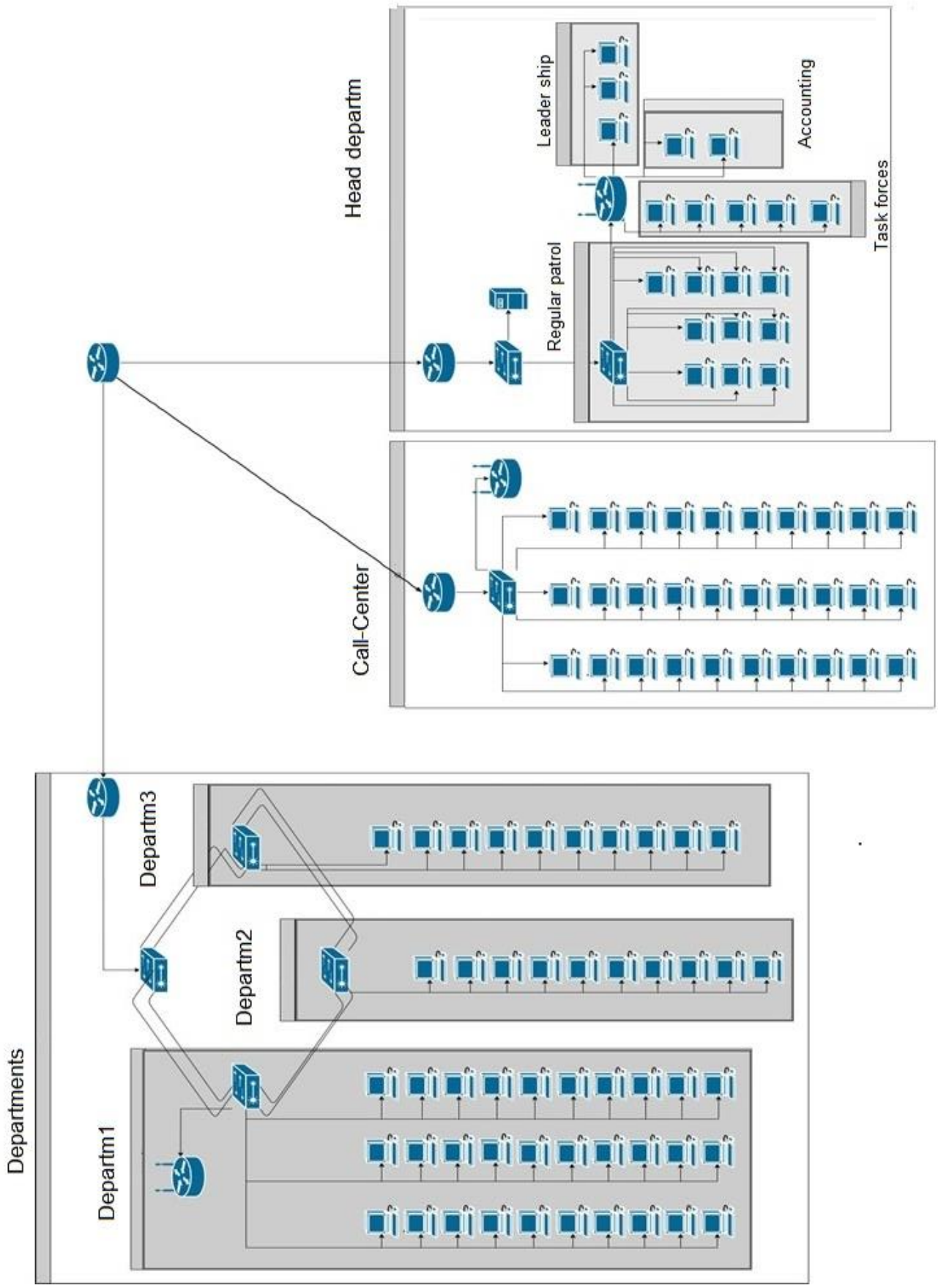

Рисунок 3.2 − Логічна схема мережі

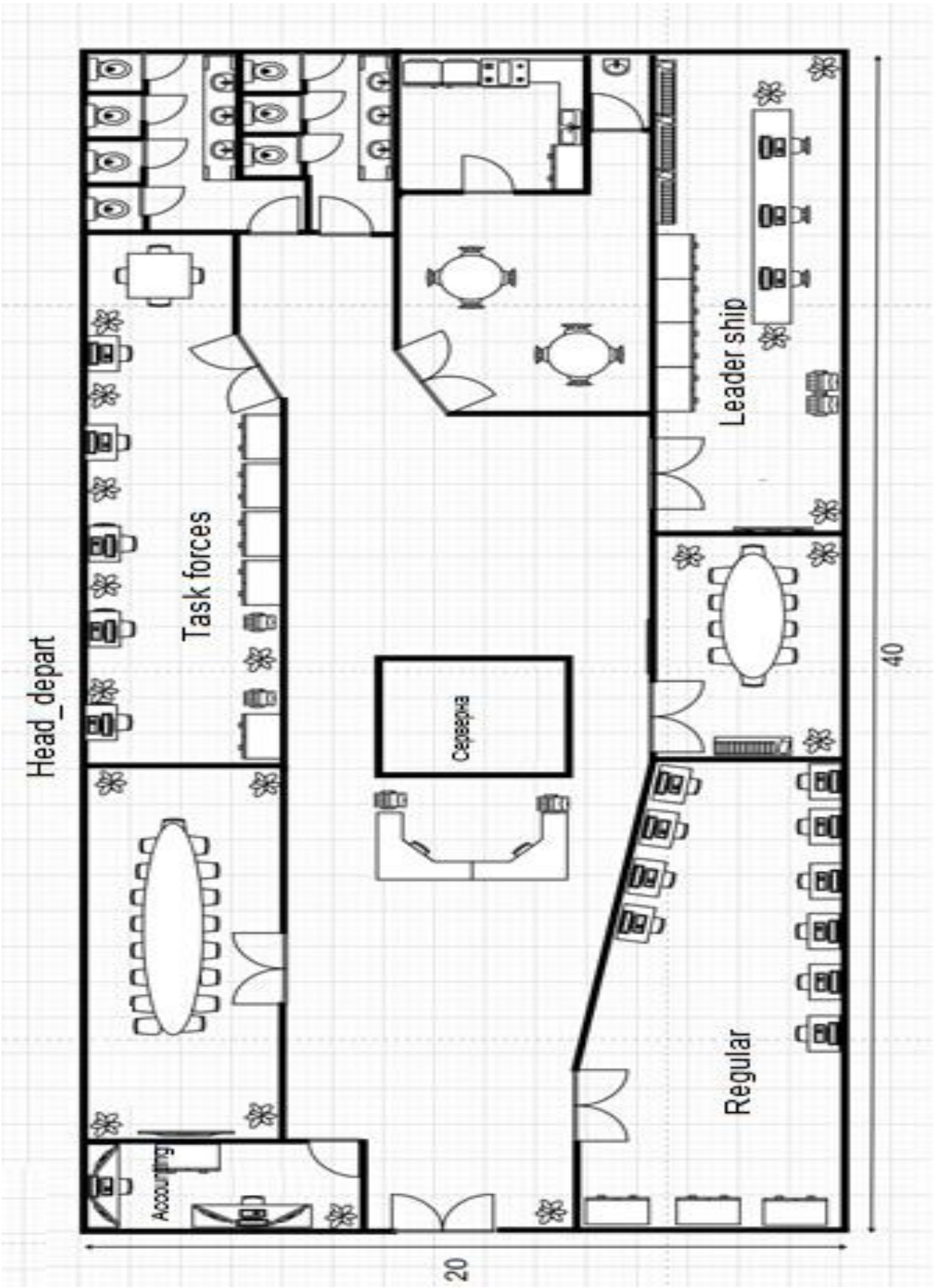

Рисунок 3.3 − Фізична топологія розміщення обладнання Департаменту

3.4 Вибір обладнання для побудови корпоративної мережі Департаменту

Зазвичай розрізняють активне та пасивне мережеве обладнання. Так як нам потрібно створити надійну комп'ютерну мережу то буде використано професійне мережеве обладнання провідних фірм у цієї галузі, що забезпечить високу пропускну спроможність та відмовостійкість мережі в цілому. Для схеми на рис. 3.3 підберемо обладнання і приведемо його характеристики (рисунок 3.4 – 3.9)

Комутатор: Cisco RV345P Dual WAN Gigabit VPN Router (RV345P-K9-G5)

Рисунок 3.4 – Комутатор Cisco RV345P Dual WAN Gigabit VPN Router (RV345P-K9-G5)

Характеритики:

Швидкість LAN портів

- 1 Гбіт / с

WAN-порт

- Ethernet
- USB 3G
- USB 4G

підтримка протоколів

- DHCP
- IPsec
- L2TP
- НІЧ
- PPPoE

- PPTP

Наявність USB порту

- 2

Інтерфейси

- 2 x 10/100/1000 Мбіт / с Gigabit Ethernet RJ-45 WAN
  8 x 10/100/1000 Мбіт / с Gigabit Ethernet RJ-45 LAN
  8 x 10/100/1000 Мбіт / с Gigabit Ethernet RJ-45 LAN з підтримкою PoE

Особливості

- підтримка PoE

Функції VPN

- IPsec сайт-к-сайту: попередньо сконфігуровані профілі для віртуального хмари Amazon і Microsoft Azure
  Протокол тунелювання рівня 2 (L2TP) (через IPsec): віддалений доступ через L2TP (через IPsec для Windows)
  Віддалений доступ IPsec: зі стандартного клієнта IPsec і Cisco IPsec VPN (наприклад, Mac OS, клієнти Apple iOS)
  Інкапсуляція загальної маршрутизації (GRE) по IPsec
  Режим Teleworker (Cisco IPsec VPN): маршрутизатор виступає клієнтом для підключення до центрального VPN-шлюзу в режимі телепрацівників
  Протокол тунелювання точка-точка (PPTP): 25 з'єднань, пропускна здатність 100 Мбіт / с

Підтримка VPN-тунелів

- є

Функції безпеки

- Безпека IP (IPsec): 50 з'єднань, пропускна здатність 650 Мбіт / с
  Безпека портів: 802.1X

Брандмауер:

- Пакетна інспекція, пропускна здатність 900 Мбіт / с для TCP, трафік протоколу користувальницьких датаграм (UDP) управління

Протоколи управління:

- Веб-браузер (HTTP / HTTPS)
- Простий протокол мережевого управління (SNMP) v1, v2c і v3

Оновлення прошивки:

- З локального ПК, з USB-накопичувача або з сайту виробника через веб-браузер
- Можливо автоматичне оновлення прошивки

Додаткові характеристики:

- VLAN: 32

Якість обслуговування (QoS):

- IPV6: подвійний стек, 6rd, 6in4
- WAN: клієнт протоколу динамічної настройки вузла DHCP, статичний IP-адресу, протокол точка-точка через Ethernet (PPPoE), прозорий міст

Подвійний стек Lite:

- Апаратне DMZ (край мережі): якщо включено, один порт LAN буде DMZ-портом

Маршрутизація:

- Протокол маршрутної інформації (RIP) v1, v2 і RIP для IPv6 (RIPng)
- Маршрутизація між VLAN
- Статична маршрутизація, IGMP-проксі

Перетворення мережевих адрес (NAT):

- Перенаправлення порту
- Трансляція порт-адреса (PAT)
- Один-до-одному NAT
- Обхід VPN NAT
- Протокол встановлення сеансу (SIP), шлюз прикладного рівня (ALG), FTP ALG

Системна пам'ять:

- Flash: 256 МБ

- ОЗУ: 1 ГБ

Маршрутизатор D-Link (DES-1210-28P)

Рисунок 3.5 - Маршрутизатор D-Link (DES-1210-28P)

Характеристики [3-5]:

Швидкість LAN портів

- 1 Гбіт / с

WAN-порт

- Ethernet
- SFP

Підтримка протоколів

- DHCP

Інтерфейси

- 24 x PoE 10/100 Мбіт / с Base-TX
  2 x 100/1000 Мбіт / с Base-T
  2 x Комбо-порт 100/1000 Мбіт / с Base-T / SFP

Особливості

- підтримка PoE

Підтримка VPN-тунелів

- немає

Продуктивність:

- Комутаційна матриця: 13 Гбіт / с
- Швидкість перенаправлення 64-байтних пакетів: 10 Mpps
- Таблиця MAC-адрес: 8K

- SDRAM для CPU: 128 МБ DDR3
- Буфер пакетів: 512 КБ
- Flash-пам'ять: 16 МБ
- Jumbo-фрейм: 9K

PoE:

- Стандарт : 802.3af, 802.3at
- Потужність: до 30 Вт (порти 1-4) / до 15.4 Вт (порти 5-24)

Функції 2 рівня:

- Spanning Tree Protocols: 802.1D STP, 802.1w RSTP
- Link Aggregation : 802.3ad, максимум 8 груп, 8 портів на групу
- Віддзеркалення портів: 1 група, One-to-One, Many-to-One

Багатоадресна розсилка 2 рівня:

- IGMP Snooping: 256 груп
- IGMP v1, v2
- IGMP v3 awareness
- IGMP snooping Fast Leave на основі VLAN вузла
- MLD v1, v2

VLAN:

- 802.1Q Tagged VLAN: 256
- VLAN на основі порту
- Asymmetric VLAN
- Auto Voice VLAN

Списки управління доступом (ACL):

- ACL , правила доступу: 1280
- ACL на основі: порту комутатора, пріоритету 802.1p, VLAN ID, MAC-адреси, Ether type, TOS, IPv4 адреси, IPv6 адреси, DSCP, типу протоколу, номера порту TCP / UDP
- 802.1X: управління доступом на основі порту Guest VLAN

Маршрутизатор: D-Link DGS-1210-52

Рисунок 3.6 - Маршрутизатор D-Link DGS-1210-52

Характеристики:

Швидкість LAN портів

- 1 Гбіт / с

WAN-порт

- Ethernet
- SFP

Інтерфейси

- 48 x 10/100 Мбіт / с Base-TX
  2 x 100/1000 Мбіт / с Base-T
  2 x Комбо-порт 100/1000 Мбіт / с Base-T / SFP

Функції безпеки

- Port Security: до 64 MAC-адрес на порт
- Захист від широкомовного / многоадресного / одноадресна шторму
  IP-MAC-Port Binding (IMPB): перевірка пакетів ARP / IP пакетів
- DHCP Snooping
- D-Link Safeguard Engine

Продуктивність:

- Комутаційна матриця: 18 Гбіт / с

- Швидкість перенаправлення 64-байтних пакетів: 13 Mpps
- Таблиця MAC-адрес: 16K
- SDRAM для CPU: 128 МБ DDR2
- Буфер пакетів: 1 МБ
- Flash-пам'ять: 16 МБ

CoS на основі:

- черги пріоритетів 802.1p
- ToS
- DSCP
- TCP / UDP-порта

Списки управління доступом (ACL):

- ACL, правила доступу: 200
- ACL на основі: порту комутатора, пріоритету 802.1p, MAC-адреси, Ether type, TOS, IPv4 адреси, IPv6-адреси , номера порту TCP / UDP, класу трафіку IPv6

Маршрутизатор: D-Link DGS-1008P PoE

Рисунок 3.7 - Маршрутизатор: D-Link DGS-1008P PoE

Характеристики [6]:

Тип:

- некерований

Кількість портів:

- 8

Порти:

- Гігабітний Ethernet

Вимоги:

- PoEPoE 802.3af (PSE) до 15.4 Вт на порт,
- PoE 802.3at (PSE) до 30 Вт на порт

Середовище передачі даних:

- 100BASE-TX: неекранована кручена пара категорій 5,
- 10BASE-T: неекранована кручена пара категорії 3, 4, 5,
- 100BASE-TX / 1000Base-T: неекранована кручена пара категорій 5

Метод передачі:

- Store-and-Forward (зберігання і передача)

Автоматичне виявлення MDI / MDIX:

- є

Відповідність мережевим стандартам:

- IEEE 802.3x (полнодуплексная зв'язок),
- IEEE 802.3 10BASE-T (10 Мбіт / с),
- IEEE 802.3u 100BASE-TX (100 Мбіт / с),
- IEEE 802.3ab 1000BASE-T (1000 Мбіт / с)

Бездротовий маршрутизатор D-Link DIR-615 / T4 (N300, 4xFE LAN, 1xFE WAN, 2 антени)

Рисунок 3.8 - Бездротовий маршрутизатор D-Link DIR-615 / T4 (N300, 4xFE LAN, 1xFE WAN, 2 антени)

Характеристики [7]::

Частота роботи Wi-Fi:

- 2.4 ГГц

Швидкість LAN портів:

- 100 Мбіт / с

Кількість антен:

- 2

WAN-порт:

- Ethernet

Підтримка протоколів:

- DHCP
- IPsec
- L2TP
- НІЧ
- PPPoE
- PPTP

Конструкція антен:

- незнімні

Особливості

- підтримка IPTV
- Підтримка VPN-тунелів

Функції брандмауера:

- Перетворення мережевих адрес (NAT)
- Контроль стану з'єднань (SPI)
- IP-фільтр
- IPv6-фільтр
- MAC-фільтр
- URL-фільтр

- DMZ-зона

Швидкість бездротового з'єднання:

- IEEE 802.11b: 15 дБм при 1, 2, 5.5, 11 Мбіт / с
- IEEE 802.11b: 15 дБм при 6, 9, 12, 18, 24, 36, 48, 54 Мбіт / с
- IEEE 802.11b: HT20 / HT40 MCS0 / 1/2/3/4/5 /

Сервер Dell PowerEdge T30 (T30v01)

Рисунок 3.9 - Сервер Dell PowerEdge T30 (T30v01)

Характеристики [8]:

Тип процесорів:

- Intel Xeon - чотирьохядерний Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц)

Об'єм оперативної пам'яті

- 16 ГБ

Чіпсет

- Intel C236

Тип оперативної пам'яті

- Архітектура: 4 слота DIMM
- Максимальний обсяг ОЗУ: до 64 ГБ, DDR4, 2133 ГГц

Кількість ядер процесора

- 4

Контролери SAS / SATA

- Intel Rapid Storage Controller 12.0(Рівні RAID - 0/1/10/5)

Жорсткий диск:

- 1 ТБ, SATA
- Можливість встановити: до чотирьох жорстких дисків SATA (4 жорстких диска SATA форм-фактора 3.5 ")

Оптичний привід: DVD +/- RW

Кількість зайнятих / доступних слотів ОЗУ : 2/4

Передня панель:

- 2 x USB 3.0
- 2 x USB 2.0
- 3.5 мм вхід для навушників
- 3.5 мм вхід для мікрофона

Задня панель:

- 4 x USB 2.0
- 2 x USB 3.0
- 2 x DisplayPort
- 1 x HDMI
- 1 x LAN (RJ-45)
- 1 x COM (послідовний порт)

Слоти розширення:

- 2 x PCI Express Gen3 x16
- 1 x PCI Express Gen3 x4
- 1 x PCI

Кількість LAN (RJ-45):1

Швидкість LAN: Гігабітний Ethernet

Периферійні пристрої [9-12]:

Принтер: CANON i-SENSYS MF641Cw

Характеристики:

Технологія друку: лазерна

Тип друку: кольорова

Максимальний формат носія: A4 (297 x 210 мм)

Максимальне місячне навантаження: 30000 сторінок

Роздільна здатність друку: 600 x 600 dpi

Максимальна якість друку: 1200 x 1200 dpi

Швидкість ч/б друку A4: 18 стор/хв

Час виходу першої ч/б сторінки: 10.4 сек

Час виходу першої кольорової сторінки: 10.5 сек

Максимальна роздільна здатність копіювання: 600 x 600 dpi

Факс: відсутній

Можливості друк з мобільних пристроїв

Носії для друку: кольоровий папір; етикетки; конверти

Мінімальная щільність носія 60 г/м²

Максимальна щільність носія 200 г/м²

Об'єм оперативної пам'яті 1 Гб

Дисплей сенсорний : кольоровий

Параметри дисплея діагональ 12.7 см

Комунікації Ethernet 10/100/1000baseTX ; USB 2.0 тип B

Робочі станції:

Системний блок:

Модель: Everest Home&Office 1036

Характеристики:

Процесор:

- Чотирьохядерний AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)

Модель GPU:

- AMD Radeon Vega 8

Об'єм оперативної пам'яті:

- 8 ГБ

Порти:

На передній панелі:

- 2x USB 2.0/ 1x USB 3.0/ 1x вихід для навушників/ 1x вхід для мікрофона.

На задній панелі:

- 2x PS / 2 для клавіатури і миші
- 1x D-Sub (VGA)/ 1x HDMI/ 1x LAN (RJ-45)/ 4x USB 3.0/ 2x USB 2.0/ 3x аудіо роз'єми

Слоти розширення:

- 1x PCI-E 3.0 x16/ 1 x PCI-E 3.0 x1

Об`єм HDD:

- 1 ТБ

Тип відеокарти:

- інтегрована

Монітор

Модель: QUBE H24F75

Характеристики:

Діагональ дисплея: 23.8 "

Максимальна роздільна здатність дисплея: 1920 x 1080

Тип матриці: IPS

Частота оновлення: 75 Гц

Час реакції матриці: 8 мс

Інтерфейси: HDMI, VGA

Яскравість дисплея: 250 кд / м²

Контрастність дисплея: 1000: 1

Особливості: "Безрамковий" (Cinema screen)

Варіанти регулювання положення дисплея: нахил: -5 ° ~ 15 °

Додаткові роз'єми: вихід на навушники

Додаткові опції: Вбудовані колонки: 2 x 2 Вт Режим "Без мерехтіння" та режим "Знижений синій колір"

Клавіатура

Модель: 2E KS 101 USB Black

Характеристики:

Кількість кнопок: 104

Інтерфейс: USB

Тип клавіш: Оптичні

Призначення: Для настільного ПК

Форма: повнорозмірна

Тип підключення: провідні

Довжина кабелю, м: 1.8

Розміри: 439 x 133.8 x 35.5 мм

Країна-виробник товару: Китай

Гарантія: 12 місяців

Миша

Модель: HP X1500 USB Black (H4K66AA)

Характеристики:

Підключення: провідні

Розмір миші: Середня

Призначення: звичайні

Інтерфейс: USB

Тип датчика: оптичний

кількість кнопок: 3

Сумісність з ОС: Microsoft Windows

Комплект на одного працівника : системній блок + монітор + клавіатура + миша + гарнітура.

Гарнітура

Модель: Sennheiser PC 5 CHAT

Характеристики:

Тип навушників: накладні

Тип підключення: провідні

Мікрофон: є

Чутливість: дБ95

Довжина кабелю, м: 2

Частотний діапазон, Гц: 42 - 17000

На всіх робочих станціях буде використовуватись операційна система Windows, яке є на сьогоднішній день розповсюдженою серед користувачів та є найпотужнішою операційною системою на сьогоднішній день.

Буде реалізована та впроваджена Корпоративна версія Windows, а також встановлена ПО DELL Windows Server 2019 Standard ROK (634-BSFX) на серверне обладнання у мережі [13-14].

3.5 Специфікація апаратних засобів

Розробимо таблицю специфікації засобів обладнання (таблиця 3.2).

Таблиця 3.2 - Специфікація засобів обладнання

Позиція	Найменування і технічна хар-ка	Тип, марка, позначення	Одиниці виміру	Кількість
1	Комутатор	Cisco RV345P Dual WAN Gigabit VPN Router (RV345P-K9-G5)	шт	4
2	Маршрутизатор	D-Link (DES-1210-28P)	шт	2
3	Маршрутизатор	D-Link DGS-1210-52	шт	3
4	Маршрутизатор	D-Link DGS-1008P PoE	шт	1
5	Бездротовий маршрутизатор	D-Link DIR-615	шт	2
6	Сервер	Dell PowerEdge T30 (T30v01)	шт	2
7	Системний блок	Everest Home&Office 1036	шт	90
8	Монітор	QUBE H24F75	шт	90
9	Клавіатура	2E KS 101 USB Black	шт	90
10	Миша	HP X1500 USB Black (H4K66AA)	шт	90
11	Принтер	CANON i-SENSYS MF641Cw	шт	5
12	Гарнітура	Sennheiser PC 5 CHAT	шт	90
12	ОС робочих станцій	Windows 10 Professional	шт	90
13	ОС сервера	DELL Windows Server 2019 Standard ROK (634-BSFX)	шт	2

3.5 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі

Для оцінки завантаженості обладнання та ліній зв’язку, виконуються наступні розрахунки.

Розрахунок основних характеристик для вихідного трафіку в найбільшому сегменті мережі закладу за умови, що послугами одночасно користуються 100% користувачів. Характеристики такі як: коефіцієнт зайнятості обслуговуючого маршрутизатора, завантаження каналу передачі даних маршрутизатора, середню затримку кадру, середню довжину черги, середній час перебування пакета в черзі, пропускну здатність каналу.

Для розрахунку приймається модель ділянки мережі як модель СМО M/M/1. Результати розрахунків порівнюються із заданими параметрами комп’ютерної системи.

Дано:

- кількість вузлів в найбільшій мережі: 50
- середня інтенсивність трафіку: μ=202 кадри/с
- середня довжина повідомлення: l=500 байт;
- вимоги до затримки передачі пакету – ≤5 мс.

Згідно кількості вузлів (50) для їх підключення на рівні розподілу обираємо комутатор Cisco RV345P Dual WAN Gigabit VPN Router (RV345P-K9-G5) (1 шт), на рівні доступу також маршрутизатор D-Link (DES-1210-28P в кількості 2 штук, також маршрутизатор D-Link DGS-1210-52 (1 шт), маршрутизатор D-Link DGS-1008P PoE та безпровідний маршрутизатор D-Link DIR-615 / T4 в кількості 1шт.

Рішення:

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 100Мбіт/с.

Для того, щоб комутатор рівня розподілу не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення.

Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=202 (кадри/с), а середня довжина повідомлення – 500 байт.

Розрахуємо пропускну здатність мережі на рівні доступу допускаючи, що послугами одночасно користуються 100% користувачів.

$P_{р.д}$= μ*l*n*8=202*500*24*8= 19,309 (Мбіт/с), де

n- кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу розраховується наступним чином. Так як до одного комутатора рівня розподілу підходять 4 комутатори рівня доступу, а загальна кількість користувачів дорівнює 50, то пропускна здатність мережі на рівні розподілу буде дорівнює:

$P_{р.р}$= μ*l*N*8=202*500*50*8= 40,400 (Мбіт/с), де

N - кількість вузлів в найбільшій мережі.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 100Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$\mu_{вих}$=100 000 000/(500*8)=25 000 пакетів/с

Оскільки кожне джерело виробляє в середньому 202 пакети/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

N=25000/202=123 джерела.

Що задовольняє нашу мережу на 50 ПК.

Кожен з 50 ПК посилає потік заявок з інтенсивністю 202 кадри/с. Інтенсивність вихідного трафіку від всіх користувачів:

$\lambda = N * \mu = 50*202=10\ 100$ (пакети/с)

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{10100}{25000} = 0{,}40$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \frac{\rho}{1-\rho} = \frac{0{,}40}{1-0{,}40} = 0{,}666$$

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

$$\mathrm{T} = \frac{1}{(\mu-\lambda)} = \frac{1}{25000-10100} = 67{,}1 \text{ мкс}$$

Середня довжина черги:

$$\mathcal{L}_{\text{чер}} = \frac{\rho^2}{1-\rho} = \frac{0{,}40^2}{1-0{,}40} = 0{,}26$$

Ця цифра може бути корисною при налаштуванні черг на обладнанні - в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, значення досить умовне; воно свідчить про те, що система працює з великим запасом по продуктивності.

Середній час перебування пакета в черзі

$$\mathrm{T}_{\text{оч}} = \frac{\mathcal{L}_{\text{чер}}}{\lambda} = \frac{0{,}26}{10100} = 25{,}74 \text{ мкс}$$

Це значення менше необхідного значення ≤5 мс, що задовольняє вимогам.

Пропускна здатність каналу:

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

$$b = \lambda * l = 10100 * 500 * 8 = 40\,000\,000 \text{ біт/с} = 40 \text{ Мбіт/с}$$

Що задовольняє пропускній здатності вихідного каналу в 100Мбіт/с.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

4.1 Розрахунок схеми адресації корпоративної мережі

Відповідно до вибраного обладнання та розробленої логічної схеми комп'ютерної мережі (рисунок 3.2) розробимо схему мережі (рисунок 4.1) та розрахуємо її адресацію.

В таблиці 4.1 показана розрахована схема адресації мережі.

Таблиця 4.1 - Схема адресації мережі

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Діапазон можливих адрес вузлів у підмережі
Head_depart	254	172.16.156.0	255.255.255.0	172.16.156.1-254
Call_Center	254	172.16.157.0	255.255.255.0	172.16.157.1-254
Departments	510	172.16.158.0	255.255.254.0	172.16.158.1-159.254

Надалі в Таблиці 4.2 розраховано схему адресації підмереж VLAN .

Таблиця 4.2 - Схема адресації VLAN

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	VLAN	Діапазон можливих адрес вузлів у підмережі
Head_depart					
Leader_ship	14	172.16.156.0	255.255.255.240	10	172.16.156.1-14
Managment_depart	14	172.16.156.16	255.255.255.240	20	172.16.156.17-30
Task_forces	14	172.16.156.32	255.255.255.240	30	172.16.156.33-46
Accounting	14	172.16.156.48	255.255.255.240	40	172.16.156.49-62
Regular_patr	14	172.16.156.64	255.255.255.240	80	172.16.156.65-78
Server	2	172.16.156.80	255.255.255.252	50	172.16.156.81-82
Departments					
Departments	64	172.16.158.0	255.255.255.192	10	172.16.156.1-62
Departm1	14	172.16.158.64	255.255.255.240	20	172.16.156.65-78
Departm2	14	172.16.158.80	255.255.255.240	30	172.16.156.81-94
Server	14	172.16.158.96	255.255.255.240	40	172.16.156.97-110
Departm3	14	172.16.158.112	255.255.255.240	80	172.16.156.113-126

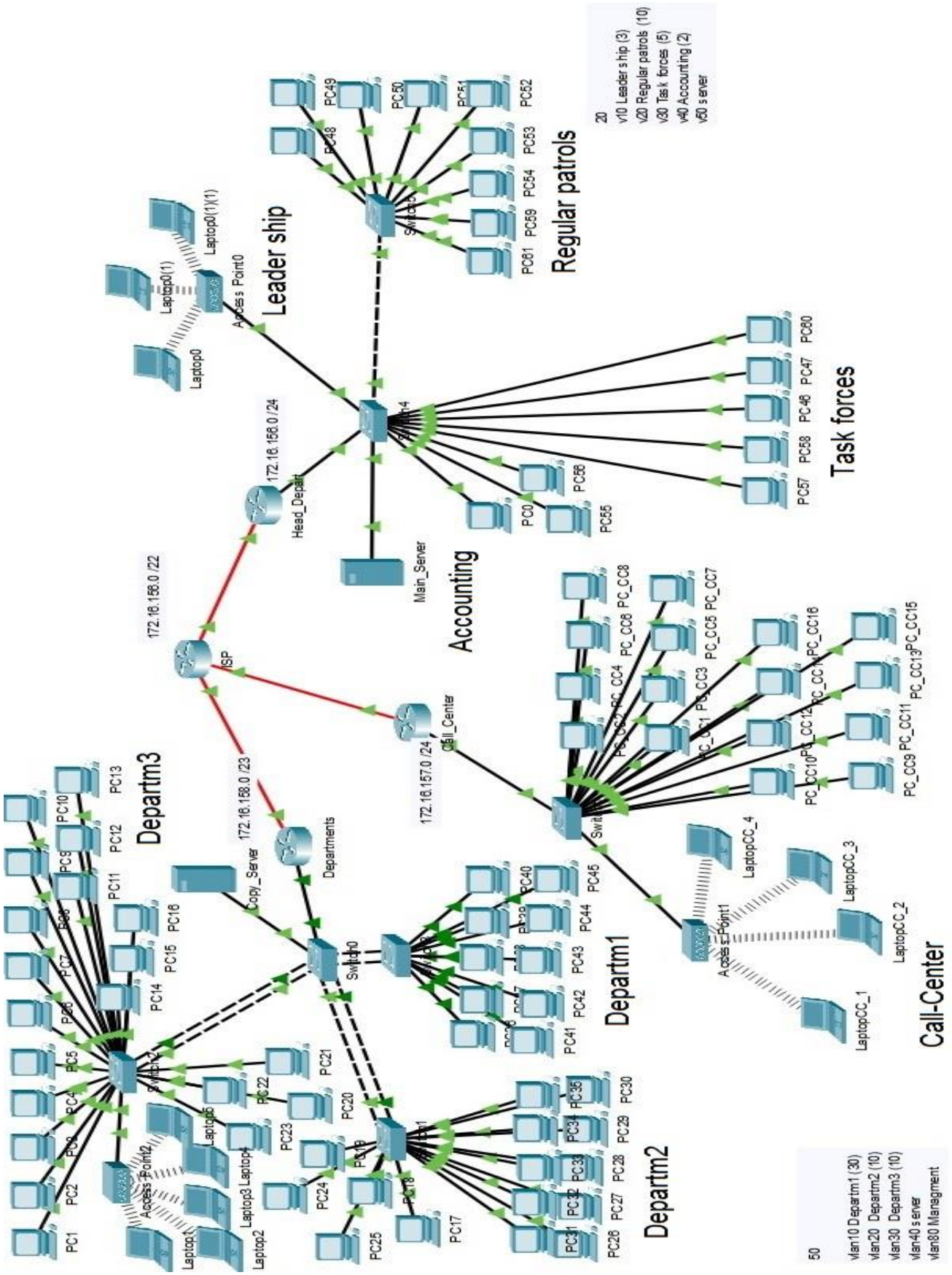

Рисунок 4.1 – Проектована схема мережі

4.2 Розрахунок схеми адресації пристроїв

Схема адресації пристроїв наведено в Таблиці 4.3.

Таблиця 4.3 – Схема адресації пристроїв в мережі.

Пристрій	Інтерфейс	IP-адреса	Маска	VLAN	Інтерфейс підключеного пристрою
Head_depart	G0/0/0	10.0.20.2	255.255.255.224	-	G0/0/0
Head_depart	G0/0.10	172.16.156.1	255.255.255.240	10	G0/1
Head_depart	G0/0.20	172.16.156.17	255.255.255.240	20	G0/1
Head_depart	G0/0.30	172.16.156.33	255.255.255.240	30	G0/1
Head_depart	G0/0.40	172.16.156.49	255.255.255.240	40	G0/1
Head_depart	G0/0.50	172.16.156.65	255.255.255.240	50	G0/1
Head_depart	G0/0.80	172.16.156.81	255.255.255.252	80	F0/22
Call_Center	G0/0/0	10.0.20.10	255.255.255.252	-	G0/2/0
Call_Center	G0/0	172.16.157.1	255.255.255.0	-	G0/1
Departments	G0/0/0	10.0.20.6	255.255.255.252	-	G0/1/0
Departments	G0/0.10	172.16.158.0	255.255.255.192	10	G0/1
Departments	G0/0.20	172.16.158.64	255.255.255.240	20	G0/1
Departments	G0/0.30	172.16.158.80	255.255.255.240	30	G0/1
Departments	G0/0.40	172.16.158.96	255.255.255.240	40	G0/1
Departments	G0/0.80	172.16.158.112	255.255.255.240	80	G0/1
Main_Server	F0	172.16.156.66	255.255.255.252	40	G0/2
Copy_Server	F0	172.16.158.99	255.255.255.240	40	F0/18

4.3 Перевірка роботи комп’ютерної системи

Перевіримо функціонування IP адресації на комутаторі

На рисунку 4.2 показано функціонування IP адресації на комутаторі.

Programmers

Physical Config CLI Attributes

IOS Command Line Interface

```
Programmers#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.16.158.10    0001.635E.62C6          --                      Automatic
172.16.158.7     000C.CF2C.D7DE          --                      Automatic
172.16.158.5     0090.0CAC.04CB          --                      Automatic
172.16.158.6     0010.1100.304D          --                      Automatic
172.16.158.8     0001.433C.227D          --                      Automatic
172.16.158.11    00D0.97A6.E579          --                      Automatic
172.16.158.9     0002.4A63.E869          --                      Automatic
172.16.158.4     0001.C763.7053          --                      Automatic
172.16.158.13    0003.E4C5.2EB3          --                      Automatic
172.16.158.14    0001.43B1.66D0          --                      Automatic
172.16.158.15    000A.412C.C926          --                      Automatic
172.16.158.12    00E0.F715.144A          --                      Automatic
172.16.158.16    0001.43A5.23AD          --                      Automatic
172.16.158.18    0002.161B.A547          --                      Automatic
172.16.158.19    000A.411E.B332          --                      Automatic
172.16.158.17    00D0.FF3D.B9A0          --                      Automatic
172.16.158.22    0000.0C86.A864          --                      Automatic
172.16.158.21    00D0.FFBC.6D70          --                      Automatic
172.16.158.27    0002.1741.B93B          --                      Automatic
172.16.158.26    0001.9769.7D7D          --                      Automatic
172.16.158.28    0004.9A2A.C027          --                      Automatic
172.16.158.29    000B.BE55.2B37          --                      Automatic
172.16.158.30    0060.3EA8.57E9          --                      Automatic
172.16.158.32    0001.9721.001A          --                      Automatic
172.16.158.31    0001.C92D.B623          --                      Automatic
172.16.158.33    00D0.D386.DB94          --                      Automatic
172.16.158.35    0060.7037.80E5          --                      Automatic
172.16.158.34    0001.4385.4049          --                      Automatic
172.16.158.36    0001.4289.4D43          --                      Automatic
172.16.158.37    0030.F231.8B62          --                      Automatic
172.16.158.69    0000.0CBB.4792          --                      Automatic
172.16.158.68    0060.477E.C4D8          --                      Automatic
172.16.158.70    0006.2AC6.8906          --                      Automatic
172.16.158.72    0002.176B.736E          --                      Automatic
172.16.158.71    0002.160E.04D6          --                      Automatic
172.16.158.74    00E0.B07A.9DC2          --                      Automatic
172.16.158.75    0005.5ED0.460B          --                      Automatic
172.16.158.73    0000.0C4E.ECAD          --                      Automatic
172.16.158.76    0007.ECEC.6422          --                      Automatic
172.16.158.77    0040.0B3C.9BEB          --                      Automatic
172.16.158.85    0090.2B30.7883          --                      Automatic
172.16.158.84    00E0.F945.0756          --                      Automatic
172.16.158.86    00E0.F9E3.B26E          --                      Automatic
172.16.158.87    0010.11DD.B19B          --                      Automatic
172.16.158.89    0001.42EA.A4B1          --                      Automatic
172.16.158.90    0001.9766.B84D          --                      Automatic
172.16.158.88    00E0.B067.6670          --                      Automatic
172.16.158.92    00E0.F7DE.95A1          --                      Automatic
```

Ctrl+F6 to exit CLI focus

Copy

Top

Рисунок 4.2 - Перевірка налаштування DHCP на комутаторі

На рисунку 4.3 показано функціонування передачі пакетів поміж різними мережами Відділу 2 та Відділу 3 [15].

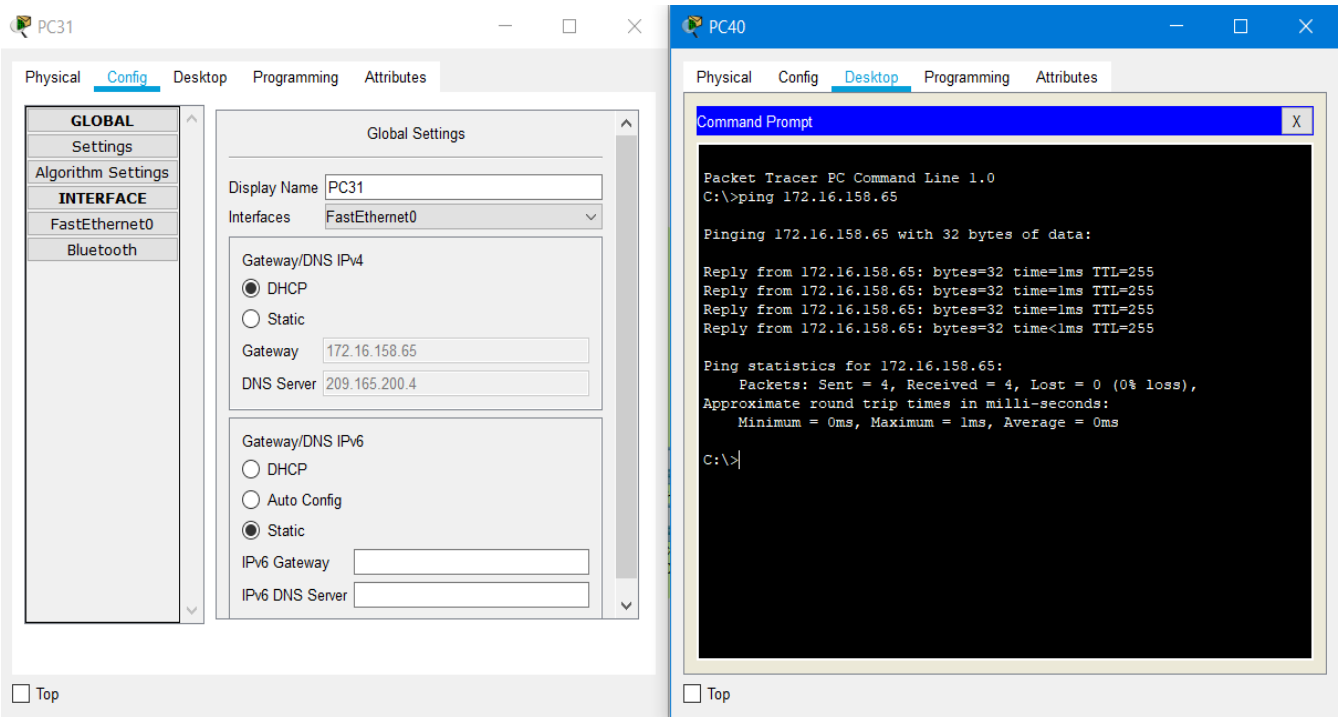

Рисунок 4.3 - Перевірка роботи PING

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Найбільш розповсюдженими атаками канального рівня є генерація широкомовних кадрів з метою перевантаження каналів передачі даних і комутаційного обладнання (до таких же наслідків приводять і так звані «широкомовні шторми» у великих комутованих мережах), підміна MAC-адрес вузлів, атаки на ARP і Spanning-Tree протоколи. Технології захисту канального рівня передбачають, перш за все, роботу з MAC-адресами вузлів, хоча ряд захисних функцій комутаторів аналізує і використовує й IP–адреси вузлів, що розширює область їх дії і на мережний рівень.

Можна виділити такі підходи до захисту на канальному рівні:

- застосування додаткових захисних функцій комутаторів, таких, як DHCP Snooping
- сегментація мережі на окремі зони (домени широкомовлення) з використанням технології віртуальних локальних мереж (Virtual Local Area Network – VLAN);
- автентифікація та авторизація на канальному рівні.
- Технологія ВПН

Функції безпеки на комутаторах:

Portsecurity — функція комутатора, що дозволяє адміністративно вказати MAC-адреси вузлів, підключених до конкретного порту (прив'язка MAC-адреси до порту) або обмежити кількість MAC-адрес на порту, яким дозволено передавати дані через порт.

Використовується для запобігання:

- несанкціонованій зміні MAC-адреси мережного пристрою,
- несанкціонованому підключенню вузла до мережі,
- атакам, спрямованим на переповнення таблиці комутації.

Функція відстеження DHCP (DHCP Snooping) — функція комутатора, яка призначена для захисту від атак з використанням протоколу DHCP (наприклад, підміна або додавання несанкціонованого DHCP-сервера в мережі або атака DHCP starvation, яка змушує DHCP-сервер видати усі існуючі на сервері адреси зловмисникові).

Функція DHCP Snooping передбачає наступні дії:

- визначення DHCP-повідомлень від ненадійних (несанкціонованих) джерел (DHCP-серверів) і відфільтровування таких повідомлень,
- розмежування DHCP-повідомлень від надійних та ненадійних джерел з подальшим відкиданням повідомлень або перенаправленням їх на відповідні порти,
- побудова та підтримка бази даних прив’язок, яка містить інформацію про ненадійні вузли з орендованими IP-адресами (вузли, які отримали IP-адреси від несанкціонованих DHCPсерверів),
- використання бази даних прив’язок для визначення та фільтрації кадрів від ненадійних вузлів.

При налаштуванні даної функції комутатор відстежує процес отримання IP-адрес вузлами з DHCPсерверів, аналізує DHCP-повідомлення, на підставі чого створює запис IP-MAC з прив’язкою до порту підключення вузла з даною MAC-адресою. В подальшому трафік від вузлів, які отримали IP-адреси з ненадійних DHCP-серверів або вузлів зі статичними IP-адресами (вузли не відповідають правилу прив’язки), не буде пропускатися через комутатор.

Функція захисту від підміни IP-адрес (IP SourceGuard або Dynamic IP Lockdown) — функція комутатора, яка виконує фільтрацію трафіку на інтерфейсах 2-го (канального) рівня на підставі аналізу бази даних прив'язок DHCP Snooping або статичних прив’язок IP-MAC.

Функція використовується для боротьби з такою атакою, як IP-spoofing. На першій стадії комутатор блокує передачу всього трафіку через захищений порт, окрім

DHCP-повідомлень. Після отримання вузлом IP-адреси та створення запису в базі даних прив'язок DHCP Snooping або створення адміністратором статичної прив’язки IPMAC весь трафік з цього вузла буде пересилатися через порт. Пересилання трафіку з інших вузлів заборонено. Таким чином, IP SourceGuard є порторієнтованою функцією, яка автоматично створює неявний список управління доступом до порту.

Virtual local area network – VLAN

Сегментація мережі на окремі зони (домени широкомовлення) з використанням технології віртуальних локальних мереж дозволяє реалізувати такий функціонал:

- контроль за широкомовним трафіком та його обмеження в рамках окремих сегментів;
- можливість створення функціональних робочих груп;
- підвищення інформаційної безпеки.

VLAN — віртуальна локальна мережа, яка являє собою групу вузлів мережі, трафік якої, в тому числі і широкомовний, на канальному рівні повністю ізольований від інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива, незалежно від типу адреси — унікальної, групової або широкомовної. У той же час всередині віртуальної мережі кадри передаються за технологією комутації. Програмне забезпечення комутаторів дозволяє переносити вузли з однієї віртуальної мережі в іншу без фізичного переключення ліній зв’язку на інші порти або комутатори. З точки зору забезпечення інформаційної безпеки найбільш цікавими функціями технології VLAN є контроль за широкомовним трафіком та підвищення інформаційної безпеки.

Підвищена інформаційна безпека VLAN також пропонує додаткові переваги для інформаційної безпеки. Користувачі однієї робочої групи не можуть отримати доступ до даних іншої групи, тому що кожна VLAN — це закрита група вузлів (обмеження реалізовано на 2-му – канальному рівні моделі OSI).

Для забезпечення передачі даних між вузлами різних VLAN необхідно задіяти 3-й – мережний рівень (налаштувати маршрутизацію між IP-мережами, кожній з яких

відповідає окрема VLAN). При цьому за допомогою додаткових фільтрів, налаштованих на маршрутизаторі або комутаторі (зазвичай 3-го рівня), можна реалізувати політику взаємодії користувачів з різних віртуальних мереж. Зокрема, на деяких комутаторах можливе направлення пакетів в різні VLAN в залежності від адрес одержувача/відправника, портів і загальної завантаженості каналу (так звані Policy-Based VLANs). Таким чином, VLAN може бути частиною загальної стратегії мережної безпеки.

VPN – Virtual Private Network

За способом реалізації:

- У вигляді спеціального програмно—апаратного забезпечення . Реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно—апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.
- У вигляді програмного рішення. Використовують персональний комп’ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.
- Інтегроване рішення. Функціональність VPN забезпечує комплекс, вирішальний також завдання фільтрації зв’язку, організації мережевого екрану і забезпечення якості обслуговування.

За призначенням:

- Intranet VPN . Використовують для об’єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв’язку.
- Remote Access VPN . Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним будівлею або філією) та одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп’ютера або, перебуваючи у

відрядженні, підключається до корпоративних ресурсів за допомогою ноутбука.

- Extranet VPN. Використовують для мереж, до яких підключаються «зовнішні» кор истувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників ВНЗ, тому потрібно забезпечення спеціальних «рубежів» захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

Переваги VPN очевидні. Надавши користувачам можливість з'єднуватися через Інтернет, масштабованість досягається в основному збільшенням пропускної здатності каналу зв'язку, коли мережа стає перевантаженої. VPN допомагає заощадити на телефонних витратах, оскільки вам не потрібно мати справу з пулом модемів. Крім того, VPN дозволяють отримати доступ до мережевих ресурсів, які в звичайній ситуації адміністратори змушені виносити на зовнішнє з'єднання.

До недоліків VPN можна віднести порівняно низьку надійність. У порівнянні з виділеними лініями та мережами на основі Frame relay віртуальні приватні мережі менш надійні, проте в 5 −10, а іноді і в 20 разів дешевше.

У проектованій мережі буде використано обмеження за IP адресою, також встановлений аутентифікаційний доступ в VLAN підключені до маршрутизатора та впроваджено VPN мережу на програмному рівні для обмеження доступу до корпоративних ресурсів співробітників та інших несанкційованих підключень.

На рисунку 5.1, показана робота VLAN на маршрутизаторах.

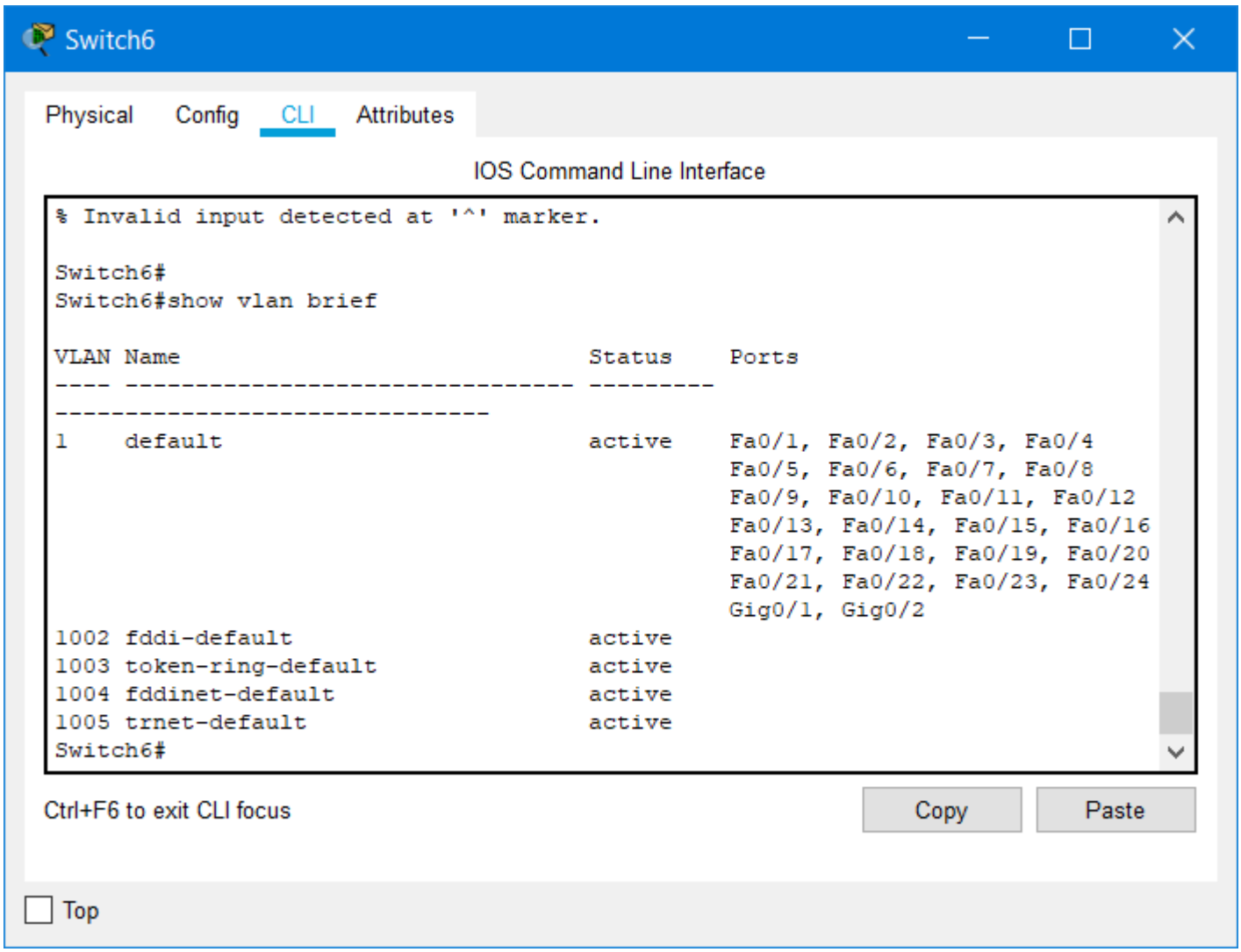

Рисунок 5.1 – Перевірка роботи VLAN на маршрутизаторах

ВИСНОВКИ

В даній випускній кваліфікаційній роботі була спроектована корпоративна мережа Департаменту патрульної поліції м. Дніпро шляхом установки та об’єднання робочих місць в спільну мережу з розподілом на підмережі.

Визначена мета та задачі проектування, проведено огляд сфери діяльності, умов праці на сьогоднішній день, простежено ринок обігу та найголовніші потребуючі нововедення.

Розглянуто різні технології комп’ютерних мереж та методи їх реалізації та після ретельного аналізу серед них було обрано FastEthernet, яка працює в середовищі передачі 100Base-TX, яке забезпечує швидкість передачі даних до 100 Мбіт/с виокристовуючи середу передачі інформації витої пари категорії 5е.

Ця мережа найкраще підходить для реалізації, так як вона найпростіша в реалізації та має не складну топологію і може бути під’єднана до мережі Інтернет за допомогою оптично-волоконної лінії, яка надається провайдером, без додаткових перетворювачів.

При проектуванні корпоративної мережі було обрано кабель UTP cat. 5e.

При виборі обладнання враховувались наступні факти: швидкість передачі даних, експлуатаційні характеристики, надійність та ціна. Було проведено розрахунок адресації методом VLSM, було розбито адресу для підмереж відповідно до відділів. А для реалізації заходів інформаційної безпеки, відділи були розділені за допомогою віртуальних локальних мереж, що допомогло скоротити витрати на допоміжні маршрутизатори, але виконати поставлені задачі.

Було прийнято реалізувати статичну маршрутизацію, так як система поділена на досить не велику кількість підмереж.

Після розрахунків адрес була спроектована модель в програмі PacketTracer і перевірена працездатність розробленої схеми системи. Було пораховано капітальні витрати на закупівлю та установку обладнання та щорічні експлуатаційні витрати.

Задача даної кваліфікаційної роботи – розробити проект Комп’ютерної системи Департаменту патрульної поліції м. Дніпро – вирішена.

ПЕРЕЛІК ПОСИЛАНЬ

1. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.
2. http://patrol.police.gov.ua/dpp-structure
3. Маршрутизатор https://rozetka.com.ua/d_link_des_1210_28p/p178075/
4. Маршрутизатор https://rozetka.com.ua/d_link_des_1210_52/p178076/
5. Маршрутизатор https://rozetka.com.ua/d_link_des_1210_52/p178076/
6. Коммутатор https://brain.com.ua/Fayrvol_Cisco_RV345P-K9-G5-p293786.html?
7. Бездротовій маршрутизатор https://rozetka.com.ua/30703615/p30703615/
8. Сервер https://rozetka.com.ua/servers/c125754/producer=dell/
9. Системний блок https://hard.rozetka.com.ua/computers/c80095/
10. Монітор https://hard.rozetka.com.ua/qube_h24f75/p220196389/
11. Клавіатура https://hard.rozetka.com.ua/2e_ks101ub/p19881722/
12. Принтер https://www.foxtrot.com.ua/uk/shop/mfu_canon_i-sensys-mf641cw.html?
13. Серверна операційна система Microsoft Windows Server 2019 Standard Edition x64 – https://soft.rozetka.com.ua/microsoft_eom_p73_07797/p69583250/
14. Клієнтська операційна система Windows 10 Professional - Професійна (FQC-09521) Ukrainian Upgrade Open Level Academic – https://soft.rozetka.com.ua/microsoft_fqc09521/p4056176/
15. Перелік команд для налаштування мережі CISCO https://www.cisco.com/c/ru_ru/td/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book/cf_cli-basics.html.

Додаток А

Текст програми налаштування центрального маршрутизатора

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.21004-01 12 01

Листів 7

2021

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування центрального маршрутизатора комп’ютерної системи.

Програма призначена для забезпечення налаштування центрального маршрутизатора, а саме базового налаштування, інтерфейсів, віддаленого доступу та підключення до Інтернет-провайдера, а також організації VLAN, DHCP та NAT.

ЗМІСТ

```
//1. Програмування базового налаштування
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Head_depart
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
//2. Налаштування DHCP
ip dhcp excluded-address 172.16.156.1 172.16.156.2
ip dhcp excluded-address 172.16.156.17 172.16.156.18
ip dhcp excluded-address 172.16.156.33 172.16.156.34
ip dhcp excluded-address 172.16.156.49 172.16.156.50
ip dhcp excluded-address 172.16.156.65 172.16.156.66
!
ip dhcp pool VLAN10
 network 172.16.156.0 255.255.255.240
 default-router 172.16.156.1
 dns-server 209.165.200.4
ip dhcp pool VLAN20
 network 172.16.156.16 255.255.255.240
 default-router 172.16.156.17
 dns-server 209.165.200.4
ip dhcp pool VLAN30
 network 172.16.156.32 255.255.255.240
 default-router 172.16.156.33
 dns-server 209.165.200.4
ip dhcp pool VLAN40
 network 172.16.156.48 255.255.255.240
 default-router 172.16.156.49
 dns-server 209.165.200.4
ip dhcp pool VLAN50
 network 172.16.156.64 255.255.255.240
 default-router 172.16.156.65
 dns-server 209.165.200.4
!
no ip cef
no ipv6 cef
!
```

```
username 123-17-1_Bulah password 7 082048430017061E010803
!
license udi pid CISCO2911/K9 sn FTX152494YZ-
!
ip domain-name Head_depart
!
spanning-tree mode pvst
!
//3. Налаштування інтерфейсів
interface GigabitEthernet0/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
//4. Налаштування підінтерфейсів VLAN
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.156.1 255.255.255.240
 ip nat inside
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.156.17 255.255.255.240
 ip nat inside
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.156.33 255.255.255.240
 ip nat inside
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.156.49 255.255.255.240
 ip nat inside
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.156.65 255.255.255.240
 ip nat inside
!
interface GigabitEthernet0/0.80
```

```
encapsulation dot1Q 80
 ip address 172.16.156.81 255.255.255.248
 ip nat inside
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/0
 ip address 10.0.20.2 255.255.255.252
 ip nat outside
!
interface Vlan1
 no ip address
 shutdown
!
//5. Налаштування NAT
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list POOLPAT pool Internet overload
ip nat inside source static 172.16.156.66 209.165.200.4
ip classless
//6. Налаштування підключення до інтернет провайдера
ip route 0.0.0.0 0.0.0.0 10.0.20.1
!
ip flow-export version 9
!
ip access-list standard POOLPAT
 permit 172.16.156.0 0.0.0.255
!
banner motd ————————————You connect to central router
Head_depart————————————
!
```

```
//7. Налаштування консольних та vty ліній
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
end
```