

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)

**ПОЯСНОВАЛЬНА ЗАПИСКА**

кваліфікаційної роботи ступеня бакалавра  
(бакалавра, спеціаліста, магістра)

здобувача Оберемка Ігоря Дмитровича  
(ПІБ)  
академічної групи 123-21-2  
(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 інформаційної агенції 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. Молодець Б.В.			
розділів:				
розробка апаратної частини				
розробка корпоративної мережі				
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро  
2025

**ЗАТВЕРДЖЕНО:**

завідувач кафедри інформаційних технологій  
та комп'ютерної інженерії  
(повна назва)

\_\_\_\_\_ Гнатушенко В.В.  
(підпис) (прізвище, ініціали)  
« \_\_\_\_\_ » \_\_\_\_\_ 2025 року

**ЗАВДАННЯ**

**на кваліфікаційну роботу ступеня бакалавр**

здобувача Оберемок І.Д. \_\_\_\_\_ **академічної групи** 123-21-2  
(прізвище та ініціали) (шифр)

спеціальності \_\_\_\_\_ 123 Комп'ютерна інженерія

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

на тему \_\_\_\_\_ «Комп'ютерна система інформаційної агенції з детальним  
опрацюванням побудови, налаштування та безпеки корпоративної мережі»  
затверджену наказом ректора НТУ «Дніпровська політехніка» від  
05.05.2025 № 336-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постанова завдання	10.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	25.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	09.06.2025

**Завдання видано** \_\_\_\_\_  
(підпис керівника)

доц. Молодець Б.В.  
(прізвище, ініціали)

**Дата видачі** \_\_\_\_\_

**Дата подання до екзаменаційної комісії** \_\_\_\_\_

**Прийнято до виконання** \_\_\_\_\_  
(підпис студента)

Оберемок І.Д.  
(прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка: с.64, рис.20, табл.6, джерел 20.

КОМП'ЮТЕРНА МЕРЕЖА, ІНФОРМАЦІЙНА АГЕНЦІЯ,  
КОМП'ЮТЕРНА СИСТЕМА, CISCO, ТОПОЛОГІЯ МЕРЕЖІ; CISCO PACKET  
TRACER; РОЗПОДІЛ АДРЕСНОГО ПРОСТОРУ.

**Об'єкт розробки** – комп'ютерна система інформаційної агенції.

**Мета роботи** – створення комп'ютерної системи інформаційної агенції з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Розробка комп'ютерної системи інформаційної агенції передбачає впровадження сучасних мережевих технологій, які забезпечують продуктивність, безпеку та гнучкість корпоративної мережі. Проведено аналіз існуючих рішень, що дозволило врахувати актуальні практики та специфіку структури підрозділів для оптимального проектування топології мережі.

Розробка архітектури мережі включає сегментування підсистем у вигляді окремих підмереж із впровадженням VLAN та організацією захищених каналів зв'язку за допомогою VPN, що підвищує безпеку та ізоляцію трафіку. Підбір апаратного забезпечення відповідає вимогам продуктивності, надійності та масштабованості, а оптимізація передачі даних мінімізує затримки і балансуватиме навантаження.

Виконана адресація мережевих пристроїв із застосуванням VLSM забезпечує ефективне використання IP-простору та гнучкість масштабування мережі. Передбачено можливість розширення мережі без суттєвих змін у структурі, що важливо для розвитку агенції.

Розроблена система відповідає сучасним вимогам функціональності, безпеки та ефективності, створюючи надійну основу для стабільної роботи та подальшого розвитку інформаційної агенції, що підтверджує досягнення мети кваліфікаційної роботи.

## ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ.....	6
ВСТУП.....	7
1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ .....	8
1.1 Характеристика галузі та умови застосування комп'ютерної системи інформаційної агенції.....	8
1.2 Стисла характеристика та структура об'єкта реалізації.....	10
1.2.1 Характеристика об'єкта реалізації .....	10
1.2.2 Організаційна структура підприємства.....	10
1.2.3 Функціонал співробітників .....	12
1.2.4 Розташування структурних підрозділів інформаційної агенції .....	14
1.3 Принципи та технічні методи забезпечення інформації для об'єкта реалізації .....	15
1.4 Огляд аналітичних методів для обробки та передачі інформації роботи інформаційної агенції.....	16
1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об'єкта проєктування, відомих рішень у галузі розробки КС інформаційної агенції.....	17
1.6 Постановка завдання і мета роботи .....	21
1.7 Визначення можливих напрямків рішення поставлених завдань .....	21
2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ....	23
2.1 Технічні вимоги до комп'ютерної системи інформаційної агенції .....	23
2.1.1 Загальні вимоги до системи .....	23
2.1.1.1 Вимоги до структури і функціонування системи з підсистемами ....	23
2.1.1.2 Вимоги до способів і засобів зв'язку між компонентами системи ...	24
2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи інформаційної агенції .....	25
2.1.1.4 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи.....	26
2.1.1.5 Додаткові технічні вимоги до КС.....	27

2.1.2	Вимоги до компонентів системи .....	28
2.1.3	Вимоги до видів забезпечення .....	30
2.1.3.1	Вимоги до інформаційного забезпечення.....	30
2.1.3.2	Вимоги до лінгвістичного забезпечення.....	31
2.1.3.3	Вимоги до технічного забезпечення.....	32
2.1.3.4	Вимоги до організаційного забезпечення.....	32
2.1.3.5	Вимоги до методичного забезпечення .....	33
2.2	Розробка апаратної частини комп'ютерної системи.....	34
2.2.1	Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи узгодженням зі структурою та топологією об'єкту розробки .....	34
2.2.2	Розробка специфікації апаратних засобів комп'ютерної системи .....	36
2.2.3	Визначення показників інтенсивності вихідного трафіку найбільшої локальної мережі підприємства .....	41
2.2.4	Розрахунок основних характеристик трафіку з метою підтвердження надійної роботи мережі.....	43
3	РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА .....	46
3.1	Розрахунок схеми адресації корпоративної мереж.....	46
3.2	Розробка топології комп'ютерної мережі .....	48
3.3	Налаштування мережі .....	48
3.3.1	Базове налаштування конфігурації пристроїв .....	48
3.3.2	Налаштування маршрутизації корпоративної мережі .....	50
3.3.3	Налаштування NAT .....	52
3.3.4	Налаштування VPN .....	53
3.3.5	Налаштування VLAN .....	55
3.4	Перевірка роботи комп'ютерної мережі .....	56
	ВИСНОВКИ.....	60
	ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	62

## ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

- ЗМІ – засоби масової інформації;
- ІА – інформаційна агенція;
- ІТ – інформаційні технології;
- КС – комп’ютерна система;
- КМ – корпоративна мережа;
- ПК – персональний комп’ютер;
- СППР – системи підтримки прийняття рішень;
- LAN – локальна мережа;
- VLAN – віртуальна локальна мережа;
- CMS – системи керування контентом;
- CRM – управління взаємовідносинами з клієнтами;
- DLP –Data Loss Prevention;
- DHCP – протокол динамічного розподілу адрес вузлам;
- HTTP – протокол передачі гіпертексту;
- OSPF – протокол динамічної маршрутизації;
- VPN – віртуальна приватна мережа;
- IaaS – інфраструктура як послуга;
- PaaS – платформа як послуга;
- SaaS – програмне забезпечення як послуга;
- SAN – мережі зберігання даних;
- JSON – текстовий формат обміну даними між комп’ютерами;
- MAC-адреса – унікальний ідентифікатор пристрою.

## ВСТУП

Діяльність інформаційних агенцій у сучасному світі є надзвичайно важливою, оскільки вони виконують ключову роль у формуванні суспільної свідомості та забезпеченні доступу до актуальної інформації. У епоху глобалізації та швидкого розвитку технологій інформаційні агенції стають основними джерелами новин, аналізу та коментарів, що дозволяє громадськості орієнтуватися в складних соціально-політичних процесах.

Метою кваліфікаційної роботи є розробка комп'ютерна система інформаційної агенції з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі. Комп'ютерна система з мережевою підтримкою дозволить ефективно комунікувати співробітникам інформаційної агенції, проводити аналітику інформаційного поля та надавати якісні послуги клієнтам, тим самим впливаючи на розвиток суспільства.

Розробка комп'ютерної системи проводилась з використанням сучасних мережевих технологій та програмного забезпечення провідних світових компаній для поєднання компонентів системи. Це дозволило створити комплексну систему, яка відповідає всім вимогам ефективної роботи інформаційної агенції.

У пояснювальній записці наведений опис всіх етапів розробки, тестування та впровадження комп'ютерної системи, що дає змогу оцінити її ефективність у сфері надання інформаційних послуг.

Дана робота є важливим внеском у розвиток діяльності медіа в Україні та сприяє інформаційній безпеці українського суспільства в умовах війни та розвитку критичного мислення серед громадян

## 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

### 1.1 Характеристика галузі та умови застосування комп'ютерної системи інформаційної агенції

Об'єктом проектування даної кваліфікаційної роботи є комп'ютерна система інформаційної агенції з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі, що відноситься до галузі інформаційних технологій.

Інформаційні агентства (ІА) – це зареєстровані як юридичні особи суб'єкти інформаційної діяльності, що діють з метою надання інформаційних послуг. Вони є ключовою ланкою у національній медіасистемі, формуючи порядок денний і виділяючи головні новини в інформаційному потоці. Агенції збирають, обробляють і поширюють новини для ЗМІ, установ, бізнесу та широкої аудиторії, часто через власні мережеві ресурси [1-3].

За тематикою інформаційні агентства поділяються на загальноновинні (висвітлюють усі сфери суспільного життя) та спеціалізовані (економічні, політичні, спортивні тощо). За періодичністю випуску інформації вони можуть працювати у форматі безперервної стрічки новин, кількох випусків на день, щотижневих чи щомісячних оглядів. За орієнтацією – на загальнонаціонального, регіонального споживача, традиційні ЗМІ, електронну пресу, органи влади, бізнес тощо.

Сьогодні інформаційні агенції відносять до медіа. Діяльність таких агенцій регулюється законами України «Про інформацію», «Про медіа», «Про електронні комунікації» та міжнародними договорами у сфері свободи слова та інформації [2, 4-8].

Основна функція інформаційних агенцій – оперативне забезпечення різних споживачів достовірною, актуальною та різноплановою інформацією для подальшого використання у засобах масової інформації (ЗМІ) та інших сферах [5, 9, 10], зокрема (рис.1.1):

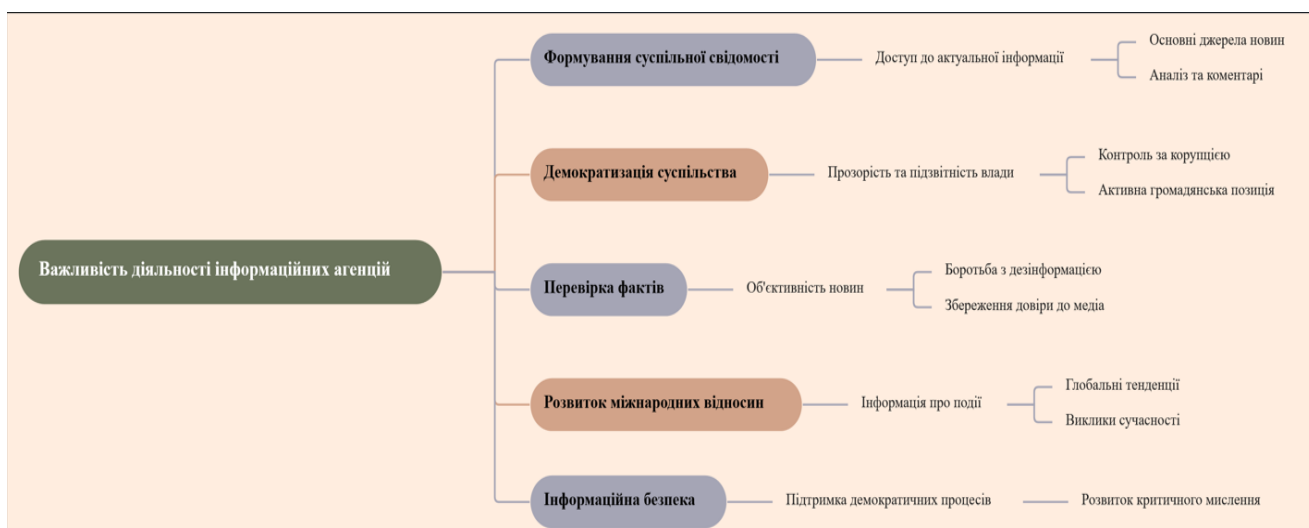


Рисунок 1.1 – Основні функції інформаційних агенцій

– Збір оперативної політичної, економічної, соціальної, культурної інформації для редакцій газет, журналів, телебачення, радіо, а також інших організацій і приватних осіб, які є передплатниками їхньої продукції.

– Обробка, створення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції.

– Забезпечення швидкого і достовірного інформування широкої аудиторії, включно з державними установами, бізнесом, ЗМІ та громадськістю.

– Надання інформаційних послуг у вигляді новинних стрічок, аналітичних матеріалів, фото- та відеоконтенту, а також організація мережі кореспондентів і редакцій для оперативного збору інформації.

– Виступати як засновник, видавець, розповсюджувач інформаційної продукції, а також забезпечувати дотримання етичних норм і законодавства у сфері інформації.

Основні послуги, які пропонують інформаційні агентства, включають:

– Підписка на новинні стрічки та оперативне інформування клієнтів про події в політиці, економіці, культурі, спорті тощо.

– Розміщення реклами на власних сайтах та інформаційних платформах.

- Надання доступу до фотобанків із великою кількістю тематичних зображень.
  - Моніторинг засобів масової інформації для відстеження згадок, тенденцій, аналізу інформаційного поля.
  - Послуги пресцентру: організація пресконференцій, брифінгів, прес-турів, підтримка зв'язків із журналістами.
  - Виробництво і розповсюдження різноманітної інформаційної продукції - текстових новин, фото-, аудіо- та відеоматеріалів.
  - Аналітичні огляди, звіти, експрес-аналіз інформації для клієнтів.
  - Підтримка корпоративних сайтів, контент-менеджмент.
  - Організація виїзних заходів, взаємодія з медіа та громадськістю.
- Така діяльність в сучасних умовах потребує сталої комунікації між співробітниками ІА та доступ до світових новин в режимі реального часу.

## **1.2 Стисла характеристика та структура об'єкта реалізації**

### **1.2.1 Характеристика об'єкта реалізації**

Інформаційна агенція веде свою діяльність більше 20 років.

Основні послуги ІА:

- оперативне інформування клієнтів шляхом підписки на таргетингові новинні стрічки;
- надання рекламних послуг на власних ресурсах;
- аналітичні послуги;
- моніторинг засобів масової інформації;
- контент-менеджмент вебресурсів клієнтів.

### **1.2.2 Організаційна структура підприємства**

На рисунку 1.2 наведена організаційна структура інформаційної агенції.

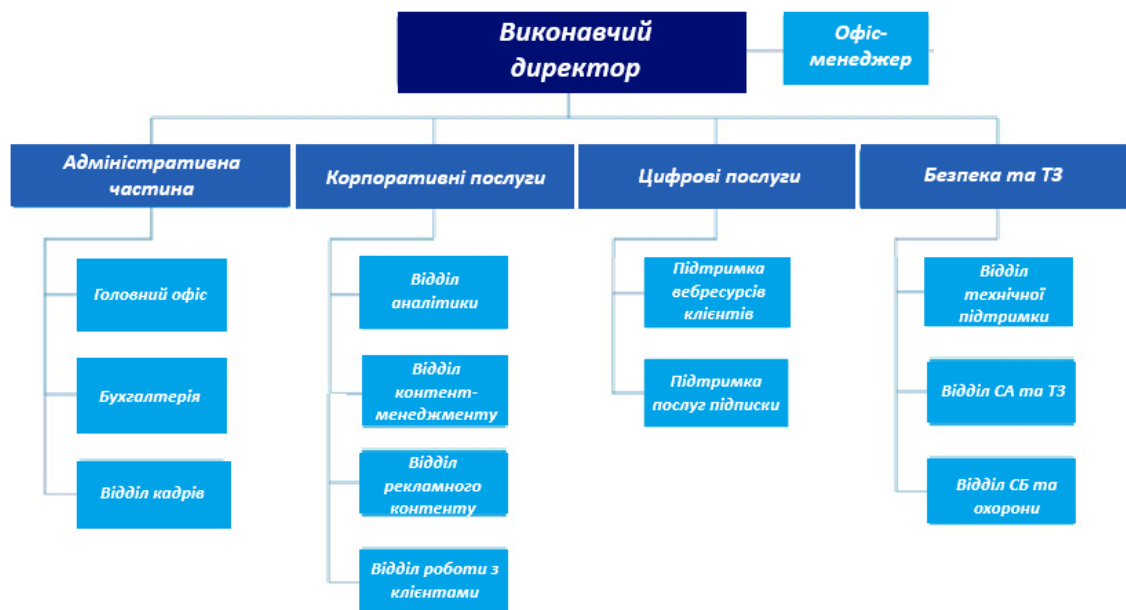


Рисунок 1.2 – Організаційна структура інформаційної агенції

Наразі ІА має 11 відділів, які належать до 4 департаментів:

Департамент 1. Адміністративна частина: головний офіс, відділ кадрів, бухгалтерія.

Департамент 2. Корпоративні послуги: відділ аналітики та моніторингу інформаційного поля, відділ контент-менеджменту, розробка рекламного контенту, відділ роботи з клієнтами.

Департамент 3. Цифрові послуги: підтримка вебресурсів клієнтів, підтримка послуг підписки.

Департамент 4. Безпека та технічне забезпечення: відділ технічної підтримки клієнтів, відділ системного адміністрування та технічного забезпечення, відділ служби безпеки та охорони.

Штат компанії (табл.1.1) включає в себе виконавчого директора, офіс-менеджера (адміністратора), бухгалтерію, працівників відділу кадрів, менеджерів по роботі з клієнтами, інформаналітиків, рекламників, розробників контенту (вебробробників), операторів з підтримки клієнтів, системних адміністраторів, працівників відділу безпеки та охорони.

Таблиця 1.1 – Штат інформаційної агенції

Відділ	Кількість штатних одиниць
Виконавчий директор	1
Головний офіс (офіс-менеджер)	1
Бухгалтерія	2
Відділ кадрів	2
Менеджери по роботі з клієнтами	4
Інформаційної аналітики	6
Рекламний	8
Розробки контенту	8
Системного та технічного забезпечення	4
Підтримки клієнтів	3
Безпеки та охорони	4

### 1.2.3 Функціонал співробітників

Виконавчий директор:

- загальне стратегічне керівництво компанією, прийняття ключових рішень;
- контроль фінансів, персоналу, юридичних, маркетингових, операційних процесів;
- представлення компанії перед партнерами, органами влади, ЗМІ;
- затвердження цін, тарифів, планів розвитку.

Офіс-менеджери:

- координація роботи офісного персоналу, організація діловодства;
- забезпечення офісу матеріалами, ведення кореспонденції, прийом дзвінків;
- організація зустрічей, корпоративних заходів, ведення первинної документації;

Бухгалтерія:

- ведення бухгалтерського та податкового обліку, підготовка фінансової звітності;

- подання звітності у фіскальні органи, підготовка документів для перевірок;

- нарахування заробітної плати співробітникам.

Відділ кадрів:

- підбір, оформлення, облік і супровід персоналу;
- ведення кадрового діловодства, трудових книжок, складання звітів;
- контроль виконання кадрових наказів, формування кадрового резерву.

Менеджери по роботі з клієнтами:

- пошук, супровід і обслуговування клієнтів, ведення клієнтської бази;
- прийом та обробка заявок, консультування клієнтів, вирішення спірних питань;

- контроль документообігу, дебіторської заборгованості, взаємодія з іншими відділами.

Інформаційної аналітики:

- моніторинг інформаційного поля, збір, обробка та аналіз інформації для потреб клієнтів, формування підписок для клієнтів;

- перевірка достовірності інформації;

- візуалізація результатів, підготовка інформації для розробників контенту, звітів, рекомендацій для керівництва.

Рекламний відділ:

- розробка рекламного контенту для клієнтів, реалізація рекламних кампаній;

- створення рекламних матеріалів, взаємодія зі ЗМІ та партнерами;

- аналіз ефективності рекламного контенту, підготовка звітності.

Відділ розробки контенту:

- створення, редагування та публікація інформаційних матеріалів (тексти, фото, відео) на власних ресурсах агенції та ресурсах клієнтів.

Відділ підтримки клієнтів:

- прийом звернень клієнтів телефоном, електронною поштою, у чаті.

- надання консультацій в режимі реального часу, оперативне вирішення проблем;
- фіксація звернень у CRM-системі, передача складних питань до відповідних відділів;
- збір та аналіз зворотного зв'язку, покращення сервісу.

Системного та технічного забезпечення:

- забезпечення безперебійної роботи ІТ-інфраструктури (сервери, мережі, робочі місця);
- встановлення, налаштування та оновлення програмного забезпечення;
- захист даних, резервне копіювання, усунення технічних несправностей.

Відділ безпеки та охорони:

- організація та контроль заходів фізичної та інформаційної безпеки;
- проведення інструктажів, моніторинг доступу до офісу та інформаційних систем;
- взаємодія з правоохоронними органами у разі інцидентів.

Такий функціонал дозволяє чітко розподілити обов'язки між співробітниками, забезпечити ефективну роботу інформаційної агенції та якісний сервіс для клієнтів.

#### **1.2.4 Розташування структурних підрозділів інформаційної агенції**

Офіс агенції займає два приміщення на першому поверсі розташованих поруч корпусів ділового центру в центрі міста Дніпро. В першому приміщенні (рис.1.3.) розташовується рецепція, відділ по роботі з клієнтами, відділ підтримки клієнтів та представники відділів розробки контенту та рекламного, які безпосередньо взаємодіють з клієнтами. Також в цьому приміщенні є кімната для нарад з клієнтами.

В другому приміщенні (рис.1.4.) більшої площі розташовуються інформаційні аналітики, відділ розробки контенту, рекламний відділ, технічний

відділ, бухгалтерія, відділ кадрів, виконавчий директор та відділ безпеки. В цьому приміщенні є кімната для нарад.



Рисунок 1.3 – План офісу для роботи з клієнтами



Рисунок 1.4 – План адміністративного офісу

### 1.3 Принципи та технічні методи забезпечення інформації для об'єкта реалізації

Інформаційна агенція впроваджує сучасні технології для збору та передачі даних, що сприяє ефективній роботі та взаємодії всіх підрозділів. Для цього

створено корпоративну мережу на базі власних серверів із налаштованим доступом до Інтернету. Обмін даними здійснюється через кабельні з'єднання, Wi-Fi і мобільний Інтернет, що гарантує постійний зв'язок і доступ до актуальної інформації.

Відділ інформаційної аналітики проводить постійний моніторинг та аналіз інформаційного поля, враховуючи інтереси клієнтів. Після обробки дані передаються до відділу розробки контенту, рекламного та технічного відділу з метою оновлення підписок клієнтів та контенту клієнтів на власних ресурсах ІА.

Менеджери по роботі з клієнтами своєчасно отримують інформацію про зміну інтересів постійних клієнтів та надають пропозиції новим клієнтам, і передають цю інформацію на опрацювання відділам інформаційної аналітики, розробки контенту, рекламному та технічному.

Відділ підтримки в режимі реального часу вирішує проблеми клієнтів, в тому числі і з доступом, у взаємодії з іншими відділами.

Технічний відділ з відділом безпеки забезпечує надійний обмін інформацією в межах офісу агенції та при зовнішньому спілкуванні з клієнтами.

Адміністративний департамент, зокрема бухгалтерія, на основі даних отриманих від менеджерів про послуги, які надані клієнтам, виставляє рахунки та разом з виконавчим директором приймає рішення про знижки постійним та корпоративним клієнтам.

#### **1.4 Огляд аналітичних методів для обробки та передачі інформації роботи інформаційної агенції**

Комп'ютерна мережа інформаційної агенції складається з робочих станцій і серверів та повинна забезпечувати швидкий і надійний обмін даними між усіма підрозділами та дозволяти керівництву, клієнтам співробітникам і технічному персоналу отримувати доступ до необхідної інформації. Інформація має бути доступною для авторизованих користувачів, але захищеною від несанкціонованого доступу, що можна досягнути шляхом ідентифікації та

автентифікації користувачів: використання паролів, двофакторної автентифікації, електронних ключів.

При розробці комп'ютерної мережі необхідно врахувати наявність двох офісів на різних поверхах в одній будівлі та віддалену роботу співробітників. Необхідний постійний стабільний доступ до мережі Інтернет.

Ефективне інформаційне та мережеве забезпечення роботи інформаційної агенції базується на принципах функціональності, повноти, надійності, безпеки, гнучкості та доступності. Реалізація цих принципів досягається шляхом впровадження сучасної IT-інфраструктури, використання технічних засобів захисту (ідентифікація, криптографія, брандмауери, антивірусний захист, DLP, резервне копіювання) та організаційних заходів для підтримки безпеки й ефективності інформаційних процесів. Захист від витоку даних потрібен на рівні робочих станцій і серверів [11].

Функціональність системи забезпечується підтримкою всіх бізнес-процесів і взаємодії з клієнтами через різні канали, можливість планування, контролю й аналітики. Централізована база даних, що містить повний профіль клієнтів і всі релевантні дані забезпечує повноту інформації. Регулярне створення копій даних полегшить відновлення у разі втрати або пошкодження.

Спроектовані рішення повинні забезпечувати надійність та стабільність системи, захист від збоїв, мінімізацію втрат даних, конфіденційність, цілісність і доступність інформації шляхом використання програмних і технічних засобів захисту, а також надавати можливість адаптації системи до нових вимог, інтеграції з іншими комп'ютерними системами. При цьому бажано раціональне використання ресурсів при впровадженні та підтримці системи.

### **1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об'єкта проєктування, відомих рішень у галузі розробки КС інформаційної агенції**

Існуючі рішення для інформаційних агенцій з мережевою підтримкою:

**Використання хмарних сервісів (Cloud First) [12]:** сучасні інформаційні агенції активно впроваджують хмарні технології для обробки, зберігання та поширення інформації. Основні моделі – SaaS (програмне забезпечення як послуга), PaaS (платформа як послуга), IaaS (інфраструктура як послуга). Це дозволяє швидко масштабувати ресурси, забезпечує доступ з різних пристроїв та платформ, а також дає гнучкість і прозорість у використанні ресурсів.

Моделі впровадження: публічна, приватна, колективна та гібридна хмара. Найбільші провайдери – Google, Amazon, Microsoft. Хмарні рішення інтегруються з українськими та міжнародними постачальниками ПЗ, що дає змогу адаптувати систему під потреби агенції.

**Мережеві інфраструктурні рішення, а саме [13]:**

– Комп'ютерні мережі: побудова локальних (LAN) та глобальних (WAN) мереж із використанням сучасних технологій Ethernet, Wi-Fi, TCP/IP. Це забезпечує швидкий обмін даними, можливість віддаленої роботи, проведення відеоконференцій, централізоване зберігання даних.

– Захищений віддалений доступ: впровадження VPN, SSH, IPsec для безпечної роботи співробітників із будь-якої точки світу. Це особливо актуально для журналістів у відрядженнях та віддалених редакцій.

– Мережі зберігання даних (SAN): високошвидкісні рішення для роботи з великими обсягами інформації, що використовуються в центрах обробки даних інформаційних агенцій.

**Інформаційні системи нового покоління [14]:**

– Системи підтримки прийняття рішень (СППР): інтерактивні комп'ютерні системи, що допомагають у вирішенні слабо структурованих управлінських задач. Вони інтегруються з мережевими платформами для оперативної аналітики та автоматизації інформаційних потоків.

– Інтелектуальні інформаційні системи: рішення на базі штучного інтелекту, які автоматизують збір, обробку, аналіз і поширення новин, а також персоналізують інформаційні потоки для різних категорій користувачів.

**Безпека та захист даних [13]:**

Мережеві фаєрволи, шифрування, фільтрація трафіку: впровадження сучасних засобів захисту для контролю доступу, запобігання несанкціонованим втручанням і захисту конфіденційної інформації[.

***Спеціалізовані рішення [14]:***

ContentNet: система для організації інформаційно-аналітичних центрів, що базується на міжнародних стандартах електронного документообігу (UN/EDIFACT, ebXML, UDDI) та забезпечує автоматизацію бізнес-процесів і електронний обмін даними через Інтернет.

***Комп'ютерна система інформаційної агенції з мережевою підтримкою.***

Комп'ютерна система інформаційної агенції з мережевою підтримкою – це сукупність апаратних і програмних засобів, які забезпечують збір, обробку, зберігання, передачу та розповсюдження інформації з використанням комп'ютерних мереж. Такі системи є основою для сучасних інформаційних агентств, редакцій ЗМІ, новинних порталів і корпоративних прес-служб.

**Основні компоненти та функції [15, 16]:**

– Комп'ютерна мережа: забезпечує зв'язок між комп'ютерами, серверами та іншими пристроями, дозволяє швидко передавати, зберігати й обробляти інформацію, а також організувати спільний доступ до ресурсів (сервери, принтери, сховища даних).

– Мережеве обладнання: до складу входять мережеві карти, комутатори (switch), маршрутизатори (router), концентратори (hub), модеми, блоки безперебійного живлення тощо.

– Мережеві операційні системи: забезпечують підтримку мережевого обладнання, протоколів, безпеки, віддаленого адміністрування та розподіленої обробки даних.

– Програмне забезпечення для обробки та розповсюдження інформації: це системи керування контентом (CMS), бази даних, поштові сервери, платформи для обміну повідомленнями, відеоконференцій, FTP-сервери для обміну файлами тощо.

Типові архітектурні рішення [15, 16]:

- Локальні комп'ютерні мережі (LAN): використовують технології Ethernet (IEEE 802.3), топології «зірка» або «шина», забезпечують об'єднання робочих місць редакторів, журналістів, аналітиків, адміністраторів.

- Виділені сервери: для зберігання великих обсягів інформації, архівів новин, мультимедійних матеріалів, баз даних контактів, аналітики тощо.

- Віддалений доступ через VPN: надає можливість співробітникам працювати з дому або у відрядженні, зберігаючи захищений доступ до внутрішніх ресурсів агенції.

- Розподілення навантаження та резервування: застосування кластеризації серверів, резервування каналів зв'язку для забезпечення безперебійної роботи та збереження даних.

- Інформаційні агентства зазвичай впроваджують багаторівневі мережі з виділеними сегментами для різних відділів (адміністрація, IT, фінанси, редакція), використовуючи сучасні комутатори (наприклад, Cisco Catalyst 9200), маршрутизатори з підтримкою сервісної інтеграції, Wi-Fi для мобільності, а також засоби для віддаленого адміністрування та моніторингу.

- Системи зберігання та обробки даних: використовуються сервери з великим обсягом пам'яті та дискового простору, резервне копіювання, архівування, швидкий доступ до архівів новин і мультимедіа.

Основні переваги мережевої підтримки:

- Оперативна передача інформації на великі відстані.

- Можливість інтерактивної взаємодії та зворотного зв'язку.

- Віддалене керування та адміністрування.

- Сумісне використання ресурсів та централізоване зберігання даних.

- Гнучкість масштабування та модернізації системи.

## **1.6 Постановка завдання і мета роботи**

Мета даної кваліфікаційної роботи полягає в розробці комп'ютерної системи інформаційної агенції з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Для досягнення мети кваліфікаційної роботи необхідно виконати наступні завдання:

- Провести аналіз існуючих рішень;
- Провести аналіз структури та розташування підрозділів інформагенції;
- Розробити архітектуру та топологію корпоративної мережі;
- Розробити схему комплексу технічних засобів;
- Провести підбір відповідного апаратного забезпечення;
- Виконати оптимізацію передачі даних;
- Виконати адресацію мережевих пристроїв;
- Забезпечити можливість масштабування мережі.

## **1.7 Визначення можливих напрямків рішення поставлених завдань**

Зважаючи на потреби інформаційної агенції щодо побудови, налаштування та безпеки корпоративної мережі, можливі такі ключові етапи рішення:

### **1. Планування та архітектура мережі.**

Розробка оптимальної фізичної та логічної структури мережі з урахуванням розташування приміщень, потреб у підключеннях, зон покриття Wi-Fi, маршрутизації та сегментування.

### **2. Вибір мережевого обладнання.**

Використання надійного сучасного обладнання, зокрема компанії Cisco, що підтримує промислові стандарти та протоколи для забезпечення високої швидкості передачі даних і надійного захисту мережі.

### **3. Забезпечення безпеки мережі.**

Розробка комплексної стратегії безпеки, яка включає:

- Встановлення міжмережевих екранів (брандмауерів) для захисту на кордонах мережі.
- Використання NAT для приховування внутрішніх IP-адрес.
- Організація VPN для захищеного віддаленого доступу.
- Шифрування трафіку для запобігання перехопленню даних.
- Впровадження систем виявлення та запобігання вторгненням (IDS/IPS).
- Аутентифікація та авторизація користувачів із застосуванням сильних методів (наприклад, двофакторна аутентифікація).

#### 4. Моніторинг мережі.

Впровадження систем моніторингу, які дозволяють у реальному часі відстежувати стан мережі, навантаження, виявляти аномалії та несанкціоновану активність, що сприяє оперативному реагуванню на загрози.

#### 5. Кабельна інфраструктура.

Проектування надійної кабельної інфраструктури з використанням крученої пари категорії 5e, розподільних панелей, роз'ємів Ethernet та інших необхідних компонентів для забезпечення стабільного зв'язку між пристроями та приміщеннями.

## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ** **Технічні вимоги до комп'ютерної системи інформаційної агенції**

### **2.1.1 Загальні вимоги до системи**

Комп'ютерна мережа інформаційної агенції призначена для забезпечення ефективного, безпечного та оперативного обміну інформацією між внутрішніми користувачами та зовнішніми системами, надання послуг клієнтам через інтернет, повинна бути побудована на основі сучасних мережевих технологій з високим рівнем безпеки, мати потужне апаратне забезпечення для обробки і зберігання інформації, а також спеціалізоване програмне забезпечення для реалізації основних послуг агенції

#### **2.1.1.1 Вимоги до структури і функціонування системи з підсистемами**

Комп'ютерна мережа має бути поділена на 5 підмереж:

- підмережа реєстрації та відділу по роботі з клієнтами. Через дану підмережу мають здійснюватися взаємодія та комунікація з клієнтами. Для кожного окремого вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі. Пропускна здатність не повинна бути меншою за 1 Мбіт/с, затримка не має перевищувати 150 мс, а рівень втрати пакетів не повинен перевищувати 5%.
- підмережа інформаційних аналітиків. Через дану підмережу здійснюється аналіз інформації потрібної для функціонування інформаційної агенції. Для кожного окремого вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі. Пропускна здатність не повинна бути меншою за 1 Мбіт/с, затримка не має перевищувати 150 мс, а рівень втрати пакетів не повинен перевищувати 5%.
- підмережа розробки контенту. Через дану підмережу здійснюють свою роботу відділ розробки контенту та відділ розробки реклами. Для

кожного окремого вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі. Пропускна здатність не повинна бути меншою за 1 Мбіт/с, затримка не має перевищувати 150 мс, а рівень втрати пакетів не повинен перевищувати 5%.

- підмережа управління агенцією. Через дану підмережу компанія управляється директором, бухгалтерією та відділом кадрів. Для кожного окремого вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі. Пропускна здатність не повинна бути меншою за 1 Мбіт/с, затримка не має перевищувати 150 мс, а рівень втрати пакетів не повинен перевищувати 5%.
- підмережа технічних спеціалістів. Через дану підмережу свою діяльність здійснюють відділ безпеки та технічний відділ. Для кожного окремого вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі. Пропускна здатність не повинна бути меншою за 1 Мбіт/с, затримка не має перевищувати 150 мс, а рівень втрати пакетів не повинен перевищувати 5%.

Розроблена комп'ютерна мережа повинна бути змонтована та сконфігурована з урахуванням можливості масштабування, тобто забезпечувати підключення нових робочих станцій або серверів до вже наявних підсистем, а також дозволяти інтеграцію додаткових підсистем у майбутньому.

#### **2.1.1.2 Вимоги до способів і засобів зв'язку між компонентами системи**

У підмережах інформаційної агенції слід забезпечити максимальну швидкість передачі даних до 100 мегабайт на секунду, тоді як між підмережами ця швидкість має становити не менше 1000 мегабайт на секунду.

Технічне обслуговування робочих станцій, серверів та мережевого обладнання необхідно проводити кожні 3–6 місяців. Функціонування мережі та

серверів повинне забезпечуватися з доступністю не менше 99%, без збоїв і переривань.

Система має гарантувати безперервну роботу всього обладнання, підключеного до комп'ютерної мережі, а сама мережа повинна бути інтегрована з глобальною мережею Інтернет.

### **2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи інформаційної агенції**

Умови та регламент експлуатації системи передбачають:

- Забезпечення високої надійності та безпеки функціонування системи.
- Захист системи від несанкціонованого доступу, втручання або пошкоджень.
- Наявність автоматизованих механізмів діагностики, контролю, корекції та відновлення у разі виникнення помилок або збоїв.
- Використання резервних копій даних та програмного забезпечення для запобігання втраті інформації.
- Можливість оновлення та модернізації системи без припинення її роботи.

Вимоги до параметрів електроживлення та заземлення включають:

- Стабільне живлення від мережі 220 В з частотою 50 Гц.
- Захист від перепадів напруги, коротких замикань, перегрівання та перевантажень.
- Наявність аварійного живлення від акумуляторних батарей або генератора, що забезпечує роботу системи не менше 4 годин у разі відключення основного живлення.
- Надійне заземлення для запобігання статичній електриці та електромагнітним перешкодам.

Регламент обслуговування системи передбачає:

- Планове технічне обслуговування кожні 6 місяців, яке включає перевірку стану апаратури, очищення вентиляторів і фільтрів, заміну

зношених або пошкоджених компонентів, контроль параметрів живлення і заземлення, перевірку програмного забезпечення, оновлення драйверів і антивірусних баз, а також дефрагментацію жорсткого диска.

- Непланове обслуговування у разі виявлення помилок або збоїв, що включає детальну діагностику, усунення несправностей, заміну компонентів або програмного забезпечення, а також тестування і налаштування системи.

Для проведення ремонту та обслуговування система повинна мати комплект запасних виробів і приладів, який містить запасні модулі, плати, кабелі, конектори, індикатори, перемикачі тощо. Цей комплект має перебувати під постійним обліком та інвентаризацією, а персонал зобов'язаний вести журнал видачі та повернення запасних виробів і приладів.

#### **2.1.1.4 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи**

Персонал для обслуговування комп'ютерної системи інформаційної агенції повинен бути професійно підготовленим, мати відповідну кваліфікацію та працювати за чітко визначеними графіками, що забезпечить надійність і стабільність функціонування комп'ютерної системи.

Вимоги до кількості та кваліфікації обслуговуючого персоналу комп'ютерної системи інформаційної агенції передбачають наявність спеціалістів із відповідними технічними знаннями та досвідом для забезпечення безперебійної роботи, обслуговування і підтримки мережевого обладнання, серверів та робочих станцій.

Кількість персоналу має бути достатньою для цілодобового або змінного режиму роботи, залежно від масштабу і складності системи: 2-3 системних адміністратора або інженери мережі для покриття основних змін і оперативного реагування на несправності, додатково – фахівці з безпеки інформації, аналітики та технічної підтримки.

Кваліфікація персоналу:

- високий рівень знань у сфері мережевих технологій (Ethernet, VLAN, VPN, DHCP, NAT, AAA), операційних систем (Windows, Linux), а також у адмініструванні серверів і мережевого обладнання (наприклад, Cisco ISR, Catalyst);
- навички роботи з інструментами моніторингу, діагностики, резервного копіювання та відновлення даних;
- знання стандартів інформаційної безпеки, методів захисту від несанкціонованого доступу, а також уміння впроваджувати політики безпеки;
- досвід у плановому та неплановому технічному обслуговуванні, оновленні програмного забезпечення і апаратних компонентів.

Режими роботи персоналу.

1. Організація роботи в змінному режимі для забезпечення безперервного моніторингу та підтримки системи.
2. Планові технічні роботи слід проводити у визначені періоди (наприклад, кожні 3-6 місяців) із мінімальним впливом на роботу системи.
3. Наявність оперативної служби реагування для швидкого усунення збоїв і аварійних ситуацій у будь-який час доби.

#### **2.1.1.5 Додаткові технічні вимоги до КС**

Ці вимоги спрямовані на забезпечення стабільної роботи комп'ютерної системи, зниження ризиків виходу з ладу обладнання та підвищення загальної надійності інформаційної інфраструктури агенції.

До додаткових технічних вимог до комп'ютерної системи інформаційної агенції належать умови експлуатації, що забезпечують стабільну та надійну роботу обладнання, а також організація інфраструктури для безпечного розміщення і підключення техніки:

Температурний режим: підтримка стабільної температури в приміщенні від +18°C до +25°C для запобігання перегріванню обладнання.

Вологість повітря: рівень відносної вологості повинен бути в межах 40–60% для уникнення конденсації і електростатичних розрядів.

Електроживлення: забезпечення стабільної напруги 220 В, 50 Гц із захистом від перепадів, коротких замикань, перевантажень та наявністю аварійного живлення (UPS або генератор) з часом автономної роботи не менше 2 годин.

Заземлення: надійне заземлення обладнання для захисту від електростатичних розрядів і електромагнітних перешкод.

Розетки та електропроводка: використання сертифікованих розеток із заземленням, розподіл навантаження по лініях живлення, організація окремих ліній для критичного обладнання.

Кабель-канали та прокладання кабелів: використання спеціалізованих кабель-каналів для захисту мережевих і електричних кабелів, забезпечення зручного доступу для обслуговування, а також дотримання стандартів роздільного прокладання силових і сигнальних кабелів для зменшення перешкод.

Вентиляція та кондиціонування: організація систем вентиляції або кондиціонування для підтримки оптимальних кліматичних умов.

Фізичний захист: обладнання має розміщуватися у спеціальних шафах або кімнатах із контролем доступу для запобігання несанкціонованому втручанню.

Освітлення: адекватне освітлення робочих зон для комфортної роботи персоналу та безпечного обслуговування обладнання.

### **2.1.2 Вимоги до компонентів системи**

Підмережа реєстрації та відділу по роботі з клієнтами забезпечує роботу співробітників, які взаємодіють із клієнтами компанії. Основні функції:

- Організація комунікації з клієнтами (через електронну пошту, IP-телефонію, CRM-системи тощо).

- Доступ до зовнішніх інформаційних ресурсів для обробки запитів клієнтів.
- Швидкий та безперебійний обмін даними між рецепцією, відділом по роботі з клієнтами та іншими відділами.

Підмережа інформаційних аналітиків призначена для аналітиків, які здійснюють збір, обробку та аналіз інформації, необхідної для функціонування інформаційної агенції. Основні функції:

- Доступ до зовнішніх і внутрішніх джерел даних для аналітичної роботи.
- Передача великих обсягів інформації між вузлами аналітиків.
- Підтримка роботи спеціалізованого програмного забезпечення для аналізу даних.

Підмережа розробки контенту об'єднує відділи, які займаються створенням контенту та розробкою рекламних матеріалів. Основні функції:

- Спільна робота над мультимедійними файлами та проектами.
- Доступ до інструментів розробки контенту, хмарних сервісів та зовнішніх платформ.
- Синхронізація та резервне копіювання робочих матеріалів.

Підмережа управління агенцією використовується керівництвом, бухгалтерією та відділом кадрів для забезпечення адміністративного управління компанією. Основні функції:

- Доступ до корпоративних інформаційних систем (ERP, бухгалтерські програми, кадрові системи).
- Захищений обмін службовою інформацією.
- Підтримка процесів прийняття управлінських рішень.
- Ведення бухгалтерського обліку і звітності агенції.
- Планування та аналіз фінансових показників агенції.

Підмережа технічних спеціалістів об'єднує відділ безпеки та технічний відділ, які відповідають за підтримку та захист мережевої інфраструктури. Основні функції:

- Моніторинг і адміністрування мережі та серверів.
- Реалізація заходів із забезпечення інформаційної безпеки.
- Впровадження та тестування нових технічних рішень.
- Керування DNS та DHCP серверами.

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

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

Інформаційне забезпечення комп'ютерної системи інформаційної агенції повинно гарантувати повноту, своєчасність і актуальність збору даних із різноманітних джерел, таких як новинні стрічки, засоби масової інформації, аналітичні звіти та інші релевантні ресурси. Для ефективної роботи інформація має бути структурована та класифікована у базах даних із чіткою системою категоризації, що забезпечує швидкий пошук, фільтрацію та таргетинг контенту відповідно до потреб клієнтів. Важливо забезпечити надійний захист інформації, включно з контролем доступу, шифруванням, системами резервного копіювання та відновлення даних, що дозволяє запобігти втратам і несанкціонованому доступу.

Система має підтримувати інтеграцію з аналітичними та моніторинговими інструментами, які автоматизують обробку великих обсягів інформації, дозволяють формувати докладні звіти та виявляти ключові тенденції у медіапросторі. Крім того, інформаційне забезпечення повинно забезпечувати можливість оперативного оновлення та публікації контенту на вебресурсах клієнтів із збереженням історії змін, що важливо для підтримки актуальності та достовірності інформації.

Для надійної та безпечної передачі інформації між внутрішніми підмережами та зовнішніми ресурсами повинні використовуватися сучасні мережеві протоколи і технології, такі як DHCP, NAT, VPN, VLAN, що гарантують стабільність, безпеку і гнучкість мережевої інфраструктури. Водночас система повинна бути відмовостійкою, мати механізми автоматичного

моніторингу, діагностики та відновлення даних у разі збоїв, що забезпечує безперервність роботи і мінімізацію ризиків втрати інформації.

Особливу увагу необхідно приділити документуванню та аудиту інформаційних процесів, що включає ведення журналів доступу, змін і подій, що забезпечує прозорість, контроль і відповідність нормативним вимогам. Загалом, інформаційне забезпечення комп'ютерної системи інформаційної агенції має бути комплексним, інтегрованим і орієнтованим на підтримку оперативності, точності, безпеки та надійності інформаційних потоків, що є ключовими для ефективної діяльності агенції в умовах динамічного інформаційного середовища.

### **2.1.3.2 Вимоги до лінгвістичного забезпечення**

Вимоги до лінгвістичного забезпечення комп'ютерної системи інформаційної агенції полягають у забезпеченні підтримки багатомовної обробки, аналізу та генерації текстової інформації, що є ключовим для ефективного функціонування агенції в умовах різноманітності джерел і аудиторій. Система повинна підтримувати автоматичне розпізнавання, обробку та класифікацію текстів різними мовами, зокрема українською та англійською, а також забезпечувати коректне відображення і кодування символів.

Лінгвістичне забезпечення має включати засоби морфологічного, синтаксичного та семантичного аналізу текстів, що дозволяють підвищувати точність пошуку, фільтрації та таргетування інформації. Важливо також інтегрувати інструменти машинного перекладу, корекції помилок і лексичного нормалізування для уніфікації контенту та полегшення його подальшої обробки.

Система повинна підтримувати формування аналітичних звітів і новинних стрічок з урахуванням лінгвістичних особливостей текстів, а також забезпечувати можливість автоматичного генерування контенту різними мовами. Для підвищення якості інформаційного продукту необхідно впроваджувати технології розпізнавання іменованих сутностей, тематичного моделювання та аналізу тональності.

Крім того, лінгвістичне забезпечення повинно враховувати специфіку галузевої термінології та стилістики, що характерні для інформаційної агенції, забезпечуючи гнучкість у налаштуванні словників і правил обробки текстів. Важливо також забезпечити інтеграцію з системами управління контентом (CMS) та аналітичними платформами для комплексної роботи з інформаційними потоками.

### **2.1.3.3 Вимоги до технічного забезпечення**

Вибраний маршрутизатор компанії Cisco повинен мати щонайменше 4 порти RJ-45 та підтримувати можливість розширення за допомогою модулів NIM-1T або NIM-4T. Для забезпечення мережі підприємства необхідно використовувати 5 комутаторів із 24 портами RJ-45 кожен та 3 комутатори із 48 портами відповідно. Робочі станції мають бути оснащені мінімум 16 ГБ оперативної пам'яті DDR4 та накопичувачем SSD об'ємом не менше 240 ГБ у форм-факторі 2,5".

### **2.1.3.4 Вимоги до організаційного забезпечення**

Організаційне забезпечення комп'ютерної системи інформаційної агенції передбачає створення чіткої структури управління, відповідального персоналу та регламентованих процедур, які забезпечують ефективну експлуатацію, підтримку та розвиток інформаційної інфраструктури. В першу чергу, необхідно визначити ролі і обов'язки співробітників, які відповідають за адміністрування мережі, обслуговування серверів, безпеку інформації та технічну підтримку користувачів. Важливо забезпечити наявність кваліфікованого персоналу, що володіє знаннями у сфері мережевих технологій, системного адміністрування, інформаційної безпеки та роботи з прикладним програмним забезпеченням.

Організаційно важливо також забезпечити належний документообіг, включно з веденням журналів доступу, обліком змін у конфігураціях, реєстрацією інцидентів та звітністю щодо технічного стану системи. Це сприяє прозорості, контролю і відповідності нормативним вимогам.

Крім того, слід організувати навчання та підвищення кваліфікації персоналу для підтримки сучасного рівня знань і навичок, необхідних для роботи з новітніми технологіями та стандартами. Важливо також планувати розвиток інформаційної системи, враховуючи зростання обсягів даних і розширення спектра послуг, що надаються агенцією.

#### **2.1.3.5 Вимоги до методичного забезпечення**

Методичне забезпечення є невід'ємною складовою комп'ютерної системи інформаційної агенції, що сприяє стандартизації процесів, підвищенню надійності, безпеки і ефективності роботи інформаційної інфраструктури.

Методичне забезпечення комп'ютерної системи інформаційної агенції включає розробку, впровадження та підтримку комплексу нормативних документів, інструкцій, стандартів і рекомендацій, які регламентують порядок експлуатації, обслуговування, адміністрування та безпеки інформаційної системи. Воно має містити детальні методики з організації роботи з апаратним і програмним забезпеченням, процедур діагностики, усунення несправностей, оновлення програмного забезпечення та резервного копіювання даних.

Методичні матеріали повинні також охоплювати стандарти інформаційної безпеки, правила контролю доступу, заходи щодо захисту від несанкціонованого втручання, а також рекомендації з організації моніторингу стану системи і реагування на інциденти. Важливо, щоб методичне забезпечення передбачало чіткі алгоритми дій персоналу у випадках аварійних ситуацій, а також порядок ведення технічної документації і звітності.

Крім того, методичні матеріали мають включати навчальні посібники і рекомендації для підвищення кваліфікації співробітників, що забезпечує ефективне використання системи та адаптацію до змін у технологіях і нормативних вимогах. Вони повинні бути доступними, оновлюватися у відповідності з розвитком інформаційної інфраструктури та забезпечувати єдині підходи до управління і підтримки комп'ютерної системи.

## 2.2 Розробка апаратної частини комп'ютерної системи

### 2.2.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи узгодженням зі структурою та топологією об'єкту розробки

Відповідно до організаційної структури та топологічної схеми розміщення структурних підрозділів інформаційної агенції (рис. 1.2–1.4) була розроблена структурна схема комплексу технічних засобів КС ІА (рис.2.1, 2.2).

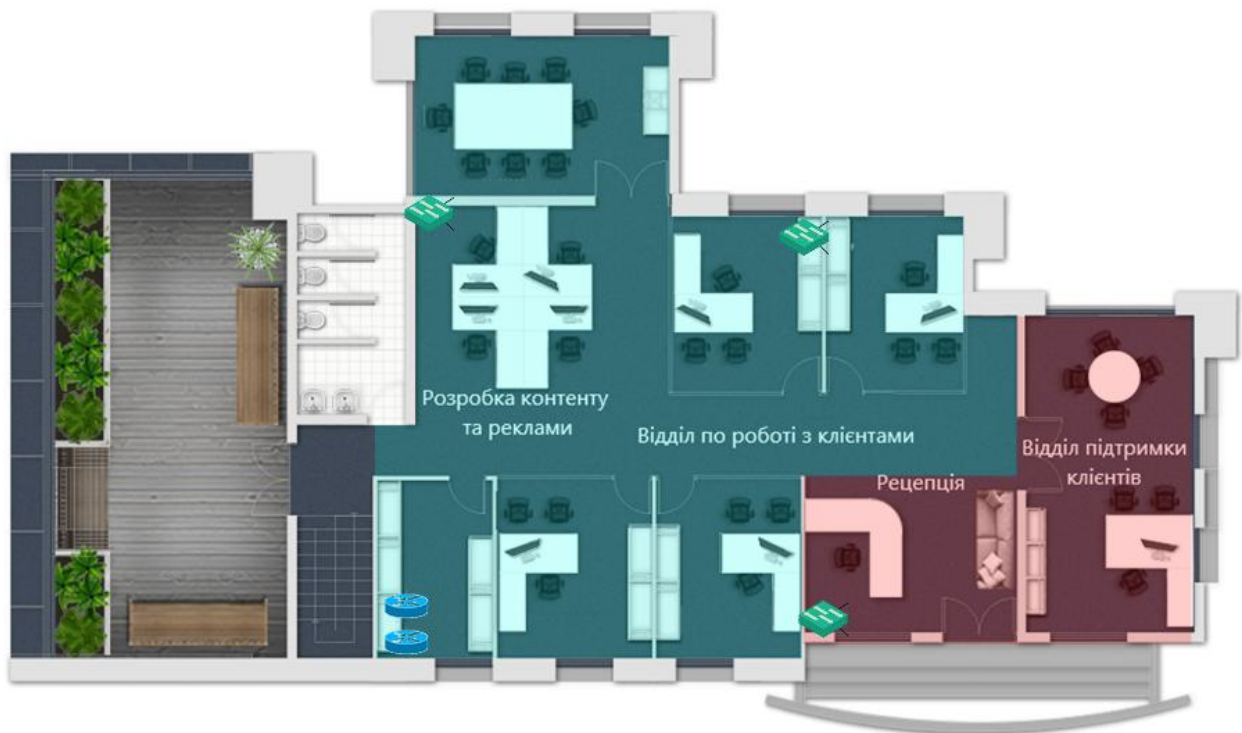


Рисунок 2.1 – Структурна схема комплексу технічних засобів КС ІА в офісі для роботи з клієнтами

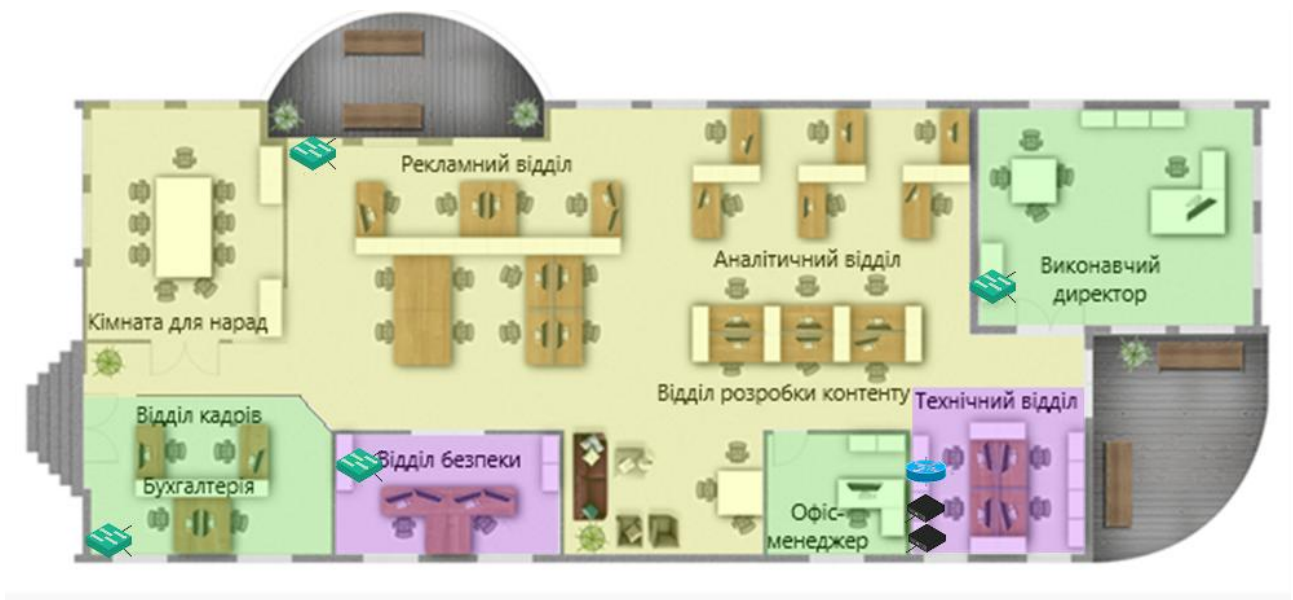


Рисунок 2.2 – Структурна схема комплексу технічних засобів КС ІА офісу роботи над контентом

Кожна підсистема реалізована як окрема підмережа. Для встановлення маршрутизаторів і серверів призначено серверну кімнату, укомплектовану спеціалізованими шафами. Серверна кімната та всі відповідні шафи обладнані дверцятами із замками, доступ до яких мають виключно системні адміністратори та директор підприємства.

Підмережу LAN 1, в якій розміщено рецепцію та відділ підтримки клієнтів, виділено в дві кімнати в першому офісі, де в одній було розміщено маршрутизатор біля рецепції.

Підмережу LAN 2, в якій розміщено відділ по роботі з клієнтами та відділ розробки контенту та реклами, виділено в шість кімнат на першому поверсі, комутатори та маршрутизатори розміщені у технічному приміщенні, доступ до якого мають виключно системні адміністратори та директор підприємства.

У другому офісному приміщенні було розміщено підмережу LAN 3, для бухгалтерського підрозділу, директора, офіс менеджера та відділу кандрів. У цьому ж офісі було розміщено комутатор та два маршрутизатора, які розміщені у спеціальній шафі, яка закривається на замок, ключ до якого є у системних адміністраторів та директора..

Підмережа LAN 4, розміщена в другому офісному приміщенні, призначена для відділів безпеки та технічного відділу. В технічному відділі розміщено DNS сервер та Radius сервер.

Підмережа LAN 5, розміщена в другому офісному приміщенні та призначена для рекламного відділу, аналітичного відділку, відділу розробки контенту та кімнати для нарад.

Усі сервери, комутатори, маршрутизатори та вузли комп'ютерної мережі з'єднанні між собою кабелями, які протягнуті вздовж стінок у спеціальному металевому кабель-каналі.

### **2.2.2 Розробка специфікації апаратних засобів комп'ютерної системи**

Для комп'ютерної системи було обрано два сервери Cisco UCS C220 M3 LFF у різних конфігураціях, які наведені в таблиці 2.1. Cisco UCS C220 M3 LFF встановлюється в стійку, призначений для роботи як з віртуалізованими, так і з невіртуалізованими додатками. Він характеризується високою продуктивністю, масштабованістю та надійністю при компактних розмірах. Сервер підтримує встановлення до двох процесорів Intel Xeon E5-2600 та до 512 ГБ оперативної пам'яті. Для зберігання даних передбачена можливість підключення до восьми 3,5-дюймових жорстких дисків або твердотільних накопичувачів SSD. Cisco UCS C220 M3 LFF оптимально підходить для різноманітних задач, зокрема для роботи у ролі серверів баз даних, веб-серверів і серверів віртуалізації. Завдяки поєднанню високої продуктивності й надійності у компактному корпусі цей сервер є ефективним рішенням для центрів обробки даних та інших середовищ з обмеженим простором [17].

Окрім високої продуктивності та надійності, сервер Cisco UCS C220 M3 LFF оснащений низкою розширених функцій, що спрощують адміністрування та технічне обслуговування. Зокрема, підтримується Cisco UCS Manager, який дозволяє централізовано керувати кількома серверами через єдиний інтерфейс. Додатково сервер оснащений Cisco Integrated Management Controller (IMC), що забезпечує можливості віддаленого управління, включаючи моніторинг

апаратного стану, керування живленням, оновлення прошивки, а також підтримку різних інтерфейсів адміністрування, таких як веб-інтерфейс, CLI та XML API, і стандартних протоколів SNMPv3 та IPMIv2.0 [17].

Для маршрутизаторів комп'ютерної системи було вибрано 7 пристроїв Cisco Catalyst 8300-1N1S-4T2X у різних конфігураціях. Cisco Catalyst 8300-1N1S-4T2X – це модульний корпоративний маршрутизатор для філій, який входить до периферійної платформи серії Cisco Catalyst 8300. Він призначений для швидкого надання мережевих послуг і має форм-фактор 1 RU з одним слотом SM, одним NIM та одним PIM. Маршрутизатор оснащений двома портами 10 Gigabit Ethernet і чотирма портами 1 Gigabit Ethernet, підтримує 10Gig WAN Cisco SD-WAN із підтримкою 5G/LTE, а також забезпечує продуктивність маршрутизації до 19,7 Гбіт/с [18].

У випадках, потреби підключення маршрутизаторів за допомогою послідовного кабелю, були встановлені додаткові модулі NIM-1T або NIM-4T. Модуль Cisco NIM-1T представляє собою однопортову послідовну інтерфейсну карту WAN, тоді як Cisco NIM-4T забезпечує наявність чотирьох послідовних портів WAN [18].

Було обрано 5 комутаторів Cisco Catalyst 8200L C8200L-1N-4T, де Cisco Catalyst 8200L C8200L-1N-4T – це захищений комутатор, який забезпечує високошвидкісне підключення Ethernet в компактному форм-факторі. Він має 4 порти гігабітних інтерфейсів Ethernet. Його пропускна здатність комутації при максимальному навантаженні в повнодуплексному режимі досягає 38 Гбіт/с, що повною мірою покриває потреби підприємства [17].

Для організації більших підмереж було обрано два комутатори Meraki MS355-48X-HW. Цей стековий комутатор доступу забезпечує високопродуктивне підключення в корпоративних мережах. Він оснащений 48 портами RJ45 зі швидкістю до 1 Гбіт/с кожен та двома портами QSFP+. Загальна пропускна здатність комутатора становить 544 Гбіт/с, а пропускна здатність стекування – 400 Гбіт/с. Крім того, пристрій підтримує маршрутизацію третього рівня та технологію UPoE (Universal Power over Ethernet).

Було обрано комплектуючі до персональних комп'ютерів співробітників. Так було обрано наступні комплектуючі до персональних комп'ютерів: Intel Xeon E5-2697v3 [], NVIDIA GeForce RTX 3060 12GB [19], плашка оперативної пам'яті Kingston DDR4 32GB/3200 ECC UDIMM [19], M.2 NVME 500GB [19]. Таким чином процесор з 14 ядрами та 20-ма потоками на 3.6 GHz, 32 Гб оперативною пам'яттю, та відеокартою мають забезпечити комфортну роботу над текстовими редакторами, великими корпусами тексту та базові технічні потреби для необхідного програмного забезпечення.

В якості принтера для логістичної підмережі було обрано Canon i-SENSYS MF455DW, бо цей кольоровий лазерний принтер, який забезпечує високу швидкість друку та велику місткість паперу. Він має загальну вхідну ємність 500 аркушів, підтримує двосторонній друк. Він підходить для мережі інформаційної агенції, де є робота пов'язана з друком великої кількості інформації. Він має швидкість друку 38 стор/хв, що дозволяє швидко друкувати великі документи. Він має невеликий розмір відносно своїх параметрів. А наявність екрану спрощує налаштування принтеру [20].

Для локальної мережі було обрано кабель Ethernet виробництва ATcom, що належить до категорії 6 та призначений для передачі даних у LAN-системах та інших мережевих інфраструктурах. Конструкція кабелю передбачає чотири пари скручених мідних провідників діаметром 0,51 мм, а для зниження впливу електромагнітних завад використовується екранування типу FTP (Foil Twisted Pair). Кабель має ізоляцію з ПВХ, що забезпечує його безпечну експлуатацію всередині приміщень. Він підтримує передачу даних на високих швидкостях із максимальною смугою пропускання до 250 МГц і сумісний із кабелями категорій 5 та 5e. Такий кабель оптимально підходить для застосування в мережах Gigabit Ethernet і Fast Ethernet. Заплановано закупити 610 метрів кабелю, з яких 215 метрів буде залишено в резерві для можливих ремонтів, розширення мережі або інших непередбачених потреб.

Для з'єднання окремих маршрутизаторів було обрано послідовний кабель типу Smart Serial Back-to-Back DCE DTE, який забезпечує підключення двох

маршрутизаторів Cisco із Smart Serial інтерфейсами. Цей кабель оснащений 12-контактним роз'ємом Smart Serial, розробленим компанією Cisco. На мережевих кінцях кабелю розташовані фізичні роз'єми, що є стандартними для відповідних інтерфейсів.

Таблиця 2.1 – Таблиця специфікації обраних апаратних засобів комп'ютерної мережі

Позиція	Найменування	Технічна характеристика	Кількість	Порти	Примітки
1	Cisco UCS C220 M3 LFF	2 процесори E5-2650 v2 1.7-2.1 GHz, 4 модулів оперативної пам'яті на 4 GB 1333Mhz, 1 SSD на 100GB, жорсткий диск на 2 TB	1	2 RJ-45	TFTP сервер
2	Cisco UCS C220 M3 LFF	2 процесори E5-2650 v2 1.7-2.1 GHz, 4 модулів оперативної пам'яті на 4 GB 1333Mhz, 1 SSD на 100GB, жорсткий диск на 2 TB	1	2 RJ-45	DNS Server
3	Cisco Catalyst 8300-1N1S-4T2X  ISR 4331	2 джерела живлення, 8 GB оперативної пам'яті, 16 GB постійної пам'яті M2 SSD	2	4 RJ-45, 3 NIM	Додано 3 модуля NIM-1T та 1 модуль NIM-4T
4	Cisco Catalyst 8200L C8200L-1N-4T	4 GB оперативної пам'яті, 8 GB флеш-пам'яті	10	2 48 RJ-45 , 2 SFP	Для підмереж
5	Meraki MS355-48X-HW	-	2	48 RJ-45, 2 QSFP+	Для підмереж

Позиція	Найменування	Технічна характеристика	Кількість	Порти	Примітки
6	PC	Intel Xeon E5-2697v3, NVIDIA GeForce RTX 3060 12GB, 32 GB оперативної пам'яті DDR4, 512 GB (SSD)	28	1 RJ-45 USB	Робочі станції
7	Canon i-SENSYS MF455DW	Роздільна здатність: 1200x1200 dpi, формат: A4, технологія друку: лазерна, кількість картреджів: 1	1	RJ-45, USB	Принтер
8	ATcom FTP cat.6 CCA 4 pairs 0.51 mm, internal, PVC	250Мг, 4 пари по 0.51 мм	610м	RJ-45	Для поєднання мережевих пристроїв
9	Smart Serial Back-to-Back Smart Serial DCE DTE Cable	0.75 м	3	DB-25	Для поєднання маршрутизаторів

Було розроблено загальну структуру мережевого обладнання підприємства, відповідно до якої для підвищення надійності мережі та рівномірного розподілу навантаження прийнято рішення про створення додаткових маршрутів між маршрутизаторами, внаслідок чого було встановлено додаткові міжмереві маршрутизатори.

Загальна структура обладнання мережі підприємства представлена на рисунку 2.3.

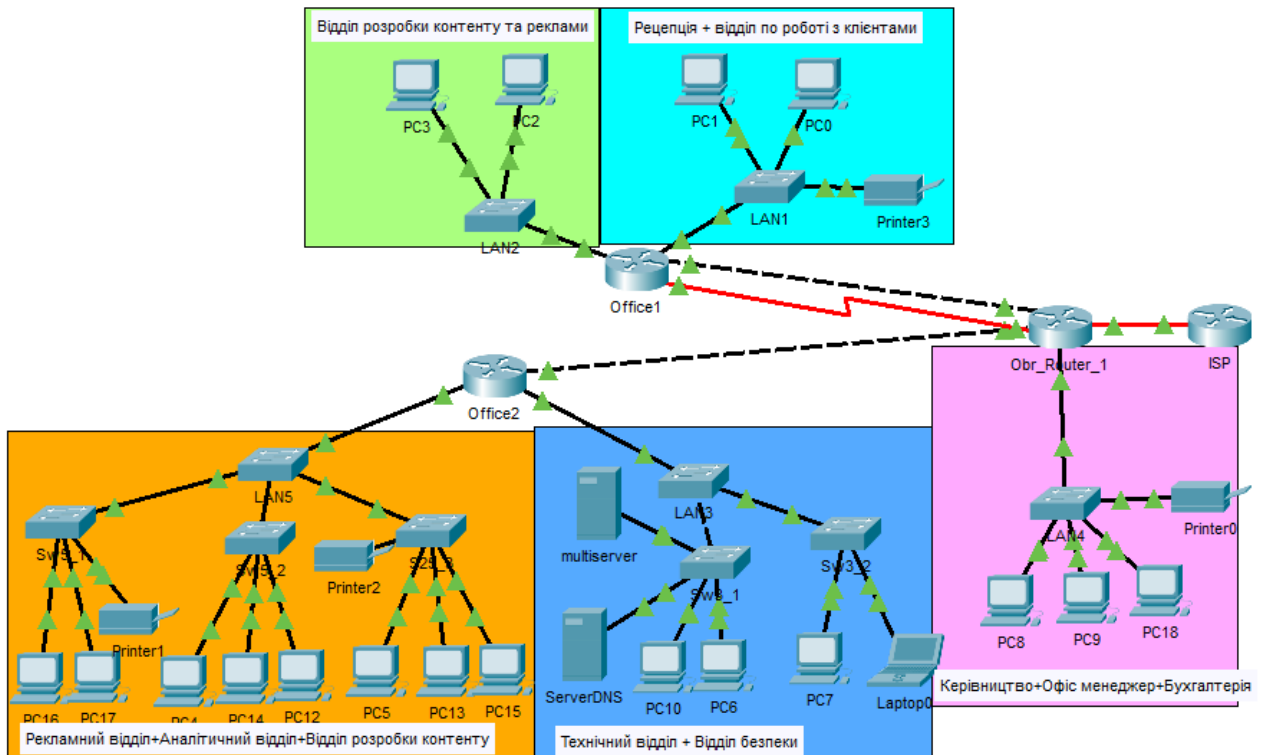


Рисунок 2.3 – Топологія мережі інформаційної агенції

### 2.2.3 Визначення показників інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Відповідно до технічних вимог, і структури підприємства інформаційної агенції найбільшою локальною мережею має бути підмережа LAN 5, де на етапі розгортання має бути розміщено 28 ПК для рекламного, аналітичного відділів та відділу розробки контенту.

Для проведення розрахунків відомі наступні дані:

- середня довжина вихідного повідомлення в локальній мережі LAN 5 (l) дорівнює 625 байтам, або 5000 бітам;
- затримка передачі пакету в локальній мережі LAN 5  $\leq 6$  мс;
- середня інтенсивність вихідного трафіку в локальній мережі LAN 5 ( $\mu$ ) = 108 кадрів/с;
- кількість вузлів в локальній мережі LAN 5 (N) = 28;

- кількість портів в комутаторів рівня доступу в локальній мережі LAN 5 ( $n$ ) = 48;
- пропускна здатність ліній передачі даних в локальній мережі LAN 5 ( $C$ ) = 1000000 біт/секунду.

Спершу була розрахована пропускна здатність локальної мережі на рівні доступу за формулою 2.1.

$$P_{p,p} = \mu * l * n, \quad (2.1)$$

- де  $\mu$  – середня інтенсивність вихідного трафіку в локальній мережі LAN 5;  
 $l$  – середня довжина вихідного повідомлення в локальній мережі LAN 5;  
 $n$  – Кількість портів в комутаторі рівня доступу в локальній мережі LAN 5

$$\text{Тобто } P_{p,p} = 108 * 5000 * 48 = 25920000(\text{біт/с}) = (26.92 \text{ Мбіт/с})$$

Наступним кроком було розраховано значення інтенсивності виходу за формулою 2.2.

$$\mu_{\text{вих}} = C / l, \quad (2.2)$$

- де  $C$  – пропускна здатність лінії передачі даних в локальній мережі LAN 5;  
 $l$  – середня довжина вихідного повідомлення в локальній мережі LAN 5.

$$\text{Тобто } \mu_{\text{вих}} = 10000000 \text{ біт/с} / 5000 \text{ біт} = 2000 \text{ (пакетів/с)}$$

Далі було розраховано максимальну кількість кінцевих вузлів, яких локальна мережа LAN 5 зможе обслуговувати, враховуючи встановлені раніше комутатори до неї. Для цього розрахунку було використано формулу 2.3.

$$N = \mu_{\text{вих}} / \mu, \quad (2.3)$$

де  $\mu_{\text{вих}}$  – значення інтенсивності виходу пакетів на секунду в локальній мережі LAN 5;

$\mu$  – середня інтенсивність вихідного трафіку в локальній мережі LAN 5.

Тобто  $N = 2000 / 108 \approx 18,52$  одиниць.

Було розраховано інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 5 за формулою 2.4.

$$\lambda = N * \mu, \quad (2.4)$$

де  $N$  – кількість вузлів в мережі в локальній мережі LAN 5;

$\mu$  – середня інтенсивність вихідного трафіку в локальній мережі LAN 5.

Тобто  $\lambda = 28 * 18,52 = 518,56$  пакетів/секунду.

#### **2.2.4 Розрахунок основних характеристик трафіку з метою підтвердження надійної роботи мережі**

Для розрахування коефіцієнту затримки на рівні розподілу в локальній мережі LAN 5 було застосовано формулу 2.5.

$$\rho = \lambda / \mu_{\text{вих}}, \quad (2.5)$$

де  $\lambda$  – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 5;

$\mu_{\text{вих}}$  – значення інтенсивності виходу пакетів на секунду в локальній мережі LAN 5.

Тобто  $\rho = 518,56 / 2000 \approx 0,259$

Було розраховано коефіцієнт зайнятості комутаторів в локальній мережі LAN 5, для цього було застосовано формулу 2.6.

$$r = \rho / (1 - \rho), \quad (2.6)$$

де  $\rho$  – коефіцієнту затримки на рівні розподілу в локальній мережі LAN 5.

$$\text{Тобто } r = 0,259 / (1 - 0,259) \approx 0,349.$$

Було розраховано значення середньої затримки кадру в локальній мережі LAN 5, для цього було застосовано формулу 2.7.

$$T = 1 / (\mu_{\text{вих}} - \lambda), \quad (2.7)$$

де  $\mu_{\text{вих}}$  – значення інтенсивності виходу пакетів на секунду в локальній мережі LAN5;

$\lambda$  – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 5.

$$T = 1 / (2000 - 518,56) \approx 67,5 * 10^{-6} \text{ секунд}$$

Використовуючи попередні розрахунки, було розраховано середню довжину черги в локальній мережі LAN 5. Для цього було використано формулу 2.8.

$$L_{\text{черги}} = \rho^2 / (1 - \rho), \quad (2.8)$$

де  $\rho$  – коефіцієнту затримки на рівні розподілу в локальній мережі LAN 5.

$$\text{Тобто } L_{\text{черги}} = (0,259)^2 / (1 - 0,259) \approx 0,0906.$$

Було розраховано середній час перебування пакета в черзі в локальній мережі LAN 5 за допомогою формули 2.9.

$$T_{\text{очік}} = L_{\text{черги}} / \lambda, \quad (2.9)$$

де  $L_{\text{черги}}$  – середня довжина черги в локальній мережі LAN 3;

$\lambda$  – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 5.

$$\text{Тобто } T_{\text{очік}} = 0,0906 / 518,56 = 17,5 \cdot 10^{-5} \text{ (секунди)}$$

Було розраховано пропускну здатність каналу в локальній мережі LAN 3, для цього було застосовано формулу 2.10.

$$b = \lambda * l, \quad (2.10)$$

де  $\lambda$  – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 3;

$l$  – середня довжина вихідного повідомлення в локальній мережі LAN 3.

$$\text{Тобто } b = 518,56 * 5000 = 2\,592\,800 \text{ біт/с} \approx 2,59 \text{ Мбіт/с.}$$

В результаті проведення розрахунків було з'ясовано що усі значення розрахованих показників задовільняють технічні вимоги.

### 3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

#### ПІДПРИЄМСТВО Розрахунок схеми адресації корпоративної мережі

Згідно з завданням, у мережах LAN1-LAN5 для зв'язку між маршрутизаторами було використано блок адрес 10.21.30.0/20, що зображено на таблиці 3.1.

Таблиця 3.1 – Схема адресації мережі

<b>Блок адрес</b>	<b>LAN 1</b> Рецепція та відділ підтримки клієнтів	<b>LAN 2</b> Відділ по роботі з клієнтами та розробки контенту та реклами	<b>LAN 3</b> Відділ безпеки та технічний відділ	<b>LAN 4</b> Керівництво	<b>LAN 5</b> Реклам ний, анатіли чний відділи
10.21.30.0/20	2	10	6	6	28

Для розрахунку використовується метод VLSM (Variable Length Subnet Masks). Метод VLSM розділяє мережу на підмережі, які також можуть розділитися. Для мережі LAN1, в яку входить 2 вузла, необхідна маска підмережі /27, доступні адреси 10.21.30.193 - 10.21.30.222, широкомовлення за адресою 10.21.30.223. Для мережі LAN2, в яку входить 10 вузлів, необхідна маска підмережі /26, доступні адреси 10.21.30.129 - 10.21.30.190, широкомовлення за адресою 10.21.30.191. Для мережі LAN3, в яку входить 6 вузлів, необхідна маска підмережі /27, доступні адреси 10.21.30.225 - 10.21.30.254, широкомовлення за адресою 10.21.30.255. Для мережі LAN4, в яку входить 6 вузлів, необхідна маска підмережі /27, доступні адреси 10.21.31.1 - 10.21.31.30, широкомовлення за адресою 10.21.31.31. Для мережі LAN5, в яку входить 28 вузлів, необхідна маска підмережі /25, доступні адреси 10.21.30.1 - 10.21.30.126, широкомовлення за адресою 10.21.30.128. Ці дані зображені на таблиці 3.2

Таблиця 3.2 – Схема адресації підмереж

Довжина	Ім'я	К-сть	IP мережі	Маска	Перша адреса	Остання адреса
Найбільша	LAN5	28/126	10.21.30.0	/25	10.21.30.1	10.21.30.127
	LAN2	10/62	10.21.30.128	/26	10.21.30.129	10.21.30.191
Найменша	LAN3	6/30	10.21.30.224	/27	10.21.30.225	10.21.30.255
	LAN4	6/30	10.21.31.0	/27	10.21.31.1	10.21.31.31
	LAN1	2/30	10.21.30.192	/27	10.21.30.193	10.21.30.223

Згідно з завданням, для зв'язку між маршрутизаторами нами було використано блок адрес 10.1.10.0 /24. На таблиці 3.3 зображена повна схема адресації мережі.

Таблиця 3.3 – Схема адресації мережі

Назва мережі	К-сть вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN5	28/126	10.21.30.0	/25	10.21.30.1	10.21.30.127
LAN4	6/30	10.21.31.0	/27	10.21.31.1	10.21.31.31
LAN3	6/30	10.21.30.224	/27	10.21.30.225	10.21.30.255
LAN2	10/62	10.21.30.128	/26	10.21.30.129	10.21.30.191
LAN1	2/30	10.21.30.192	/27	10.21.30.193	10.21.30.223
WAN 1	2/2	10.1.10.0	/30	10.1.10.1	10.1.10.2
WAN 2	2/2	10.1.10.4	/30	10.1.10.5	10.1.10.6

Серверам було привласнено IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+10. Адресація серверів зображена на таблиці 3.4.

Таблиця 3.4 – Адресація інтерфейсів серверів

Назва серверу	Назва інтерфейсу	IP-адреса	Маска	Шлюз
Raduis Server	Fa0	10.21.30.235	27	10.21.30.226
Server DNS	Fa0	10.21.30.236	27	10.21.30.226

## 3.2 Розробка топології комп'ютерної мережі

У програмі Cisco Packet Tracer була розроблена топологічна схема, що складається із 5 підмереж.

## 3.3 Налаштування мережі

### 3.3.1 Базове налаштування конфігурації пристроїв

Для початку необхідно виконати базове налаштування пристроїв. Для цього, згідно із рекомендаціями, необхідно:

– назначити назви пристроям за наступним правилом:

Прізвище студента\_тип пристрою\_номер пристрою, наприклад, Obr\_Router\_1;

– для всіх пристроїв встановити пароль cisco до консолі та vty;

– на всіх пристроях назначити пароль class до привілейованого режиму;

– усі паролі, що зберігаються у відкритому вигляді, пропонується під час налаштування моделі комп'ютерної системи зашифрувати;

– створити банер MOTD;

– для всіх ліній vty налаштувати протокол ssh;

– призначити на всіх пристроях користувача за правилом:

група\_прізвище,

наприклад 123202\_Malov, з паролем admincisco;

– в якості імені домена використати ім'я пристрою для шифрування даних;

– створювати ключ RSA завдовжки 1024 біт;

– на DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000.

Для прикладу наведено налаштування на роутері Obr\_Router\_1.

Призначимо назву за правилом Obr\_Пристрій\_Номер.

```
Obr_Router_1 (config)#hostname Obr_Router_1
```

Призначимо пароль cisco до консолі і vty.

```
Obr_Router_1 (config)#line console 0
```

```
Obr_Router_1 (config-line)#password cisco
```

```
Obr_Router_1 (config-line)#login
```

```
Obr_Router_1 (config-line)#exit
```

```
Obr_Router_1 (config)#line vty 0 15
```

```
Obr_Router_1 (config-line)#password cisco
```

```
Obr_Router_1 (config-line)#login
```

```
Obr_Router_1 (config-line)#
```

Призначимо пароль class до привілейованого режиму

```
Obr_Router_1(config)#enable secret class
```

Паролі, що зберігаються у відкритому вигляді зашифруємо.

```
Obr_Router_1(config)#service password-encryption
```

Розробимо банер MOTD.

```
Obr_Router_1(config)#banner motd "Welcome to Obr_Router_1"
```

Призначимо на усіх лініях vty використання протоколу ssh.

```
Obr_Router_1(config)#line vty 0 15
```

```
Obr_Router_1(config-line)#transport input ssh
```

Призначимо на всіх пристроях користувача за правилом: 12321\_Obr з паролем admincisco.

```
Obr_Router_1(config)#username 123202_Obr privilege 15 secret admincisco
```

В якості імені домена використаємо ім'я пристрою.

```
Obr_Router_1 (config)#ip domain name Obr_Router_1
```

Для шифрування даних створимо ключ RSA завдовжки 1024 біт.

```
Obr_Router_1 (config)#crypto key generate rsa
```

The name for the keys will be: Obr\_Router\_1. Obr\_Router\_1

Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys.

```
How many bits in the modulus [512]: 1024
```

На DCE-інтерфейсах маршрутизаторів призначимо встановлення значення тактової частоти – 128000.

```
Obr_Router_1 (config-if)#clock rate 128000
```

Після налаштування збережемо конфігурацію пристрою.

```
Obr_Router_1#copy running-config startup-config
```

### 3.3.2 Налаштування маршрутизації корпоративної мережі

Існує 2 види маршрутизації, статична та динамічна. Статична маршрутизація передбачає ручне налаштування маршрутів адміністратором мережі, що забезпечує простоту налаштування та повний контроль, але погано масштабується і не адаптується до змін у мережі. Натомість, динамічна маршрутизація використовує протоколи, такі як RIP, OSPF і BGP, для автоматичного визначення найкращих маршрутів. Це забезпечує адаптивність і масштабованість, дозволяючи мережі автоматично реагувати на зміни. Динамічна маршрутизація підходить для великих і складних мереж, але вимагає більше знань для налаштування та споживає більше ресурсів для обміну маршрутизуючою інформацією. У данному проєкті, задля масштабованості була обрана саме динамічна маршрутизація і протокол OSPF.

Серед переваг протоколу OSPF є:

- Висока швидкість збіжності;
- Підтримка мережних масок змінної довжини VLSM;
- Відсутність обмежень досяжності;
- Оптимальне використання пропускної здатності мережі;
- Оптимальний вибір шляху маршрутизації.

Перед налаштуванням маршрутизації кожному мережевому пристрою потрібно надати IP-адресу та маску мережі відповідно до таблиць маршрутизації. Для цього обирається необхідний інтерфейс за допомогою команди:

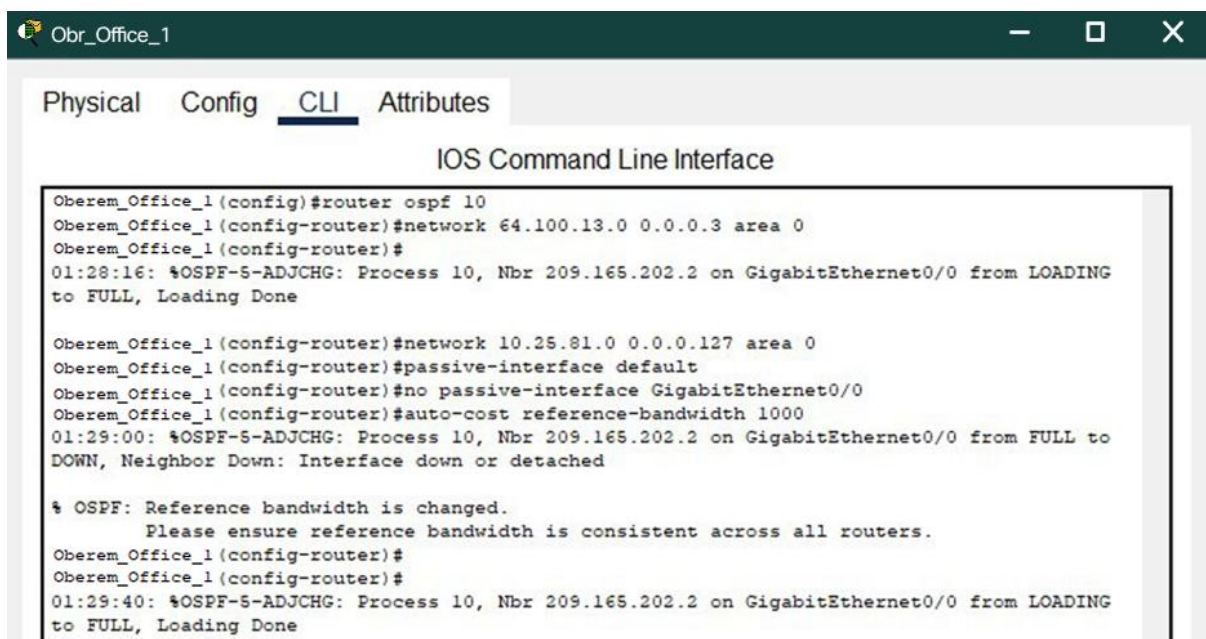
```
Obr_Router_1(config)#interface назва_інтерфейсу
```

І потім вводиться IP адреса і маска підмережі, за допомогою команди:

```
Obr_Router_1(config-if)#ip address IP-адреса маска_підмережі.
```

Після цього можна приступати до налаштування інтерфейсу OSPF.

Приклад налаштування OSPF на роутері Obr\_Router\_1 зображено на рисунку 3.1.



```
Obr_Office_1
Physical Config CLI Attributes
IOS Command Line Interface
Oberem_Office_1 (config)#router ospf 10
Oberem_Office_1 (config-router)#network 64.100.13.0 0.0.0.3 area 0
Oberem_Office_1 (config-router)#
01:28:16: %OSPF-5-ADJCHG: Process 10, Nbr 209.165.202.2 on GigabitEthernet0/0 from LOADING
to FULL, Loading Done

Oberem_Office_1 (config-router)#network 10.25.81.0 0.0.0.127 area 0
Oberem_Office_1 (config-router)#passive-interface default
Oberem_Office_1 (config-router)#no passive-interface GigabitEthernet0/0
Oberem_Office_1 (config-router)#auto-cost reference-bandwidth 1000
01:29:00: %OSPF-5-ADJCHG: Process 10, Nbr 209.165.202.2 on GigabitEthernet0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
Oberem_Office_1 (config-router)#
Oberem_Office_1 (config-router)#
01:29:40: %OSPF-5-ADJCHG: Process 10, Nbr 209.165.202.2 on GigabitEthernet0/0 from LOADING
to FULL, Loading Done
```

Рисунок 3.1 – Налаштування OSPF

Окрім цього, було виконано налаштування DHCP. Також необхідно виконати налаштування всіх маршрутизаторів на підтримку служби AAA таким чином:

- задати пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500;

- для перевірки підключень до VTY ліній на маршрутизаторі використовувати локальну базу даних користувачів;

- для доступу до консолі використовувати аутентифікацію на основі протоколу RADIUS і якщо немає – локальну базу даних;

- radius-сервер налаштувати наступним чином: ключове слово – radius123;
- в якості облікового запису користувачів використовувати ім'я пристрою з паролем admin123.

В якості Radius сервера був використаний сервер HTTP, що дозволяє зменшити витрати на технічне обладнання та спростити роботу системного адміністратора. Виконане налаштування Radius сервера зображено на рисунку 3.2.

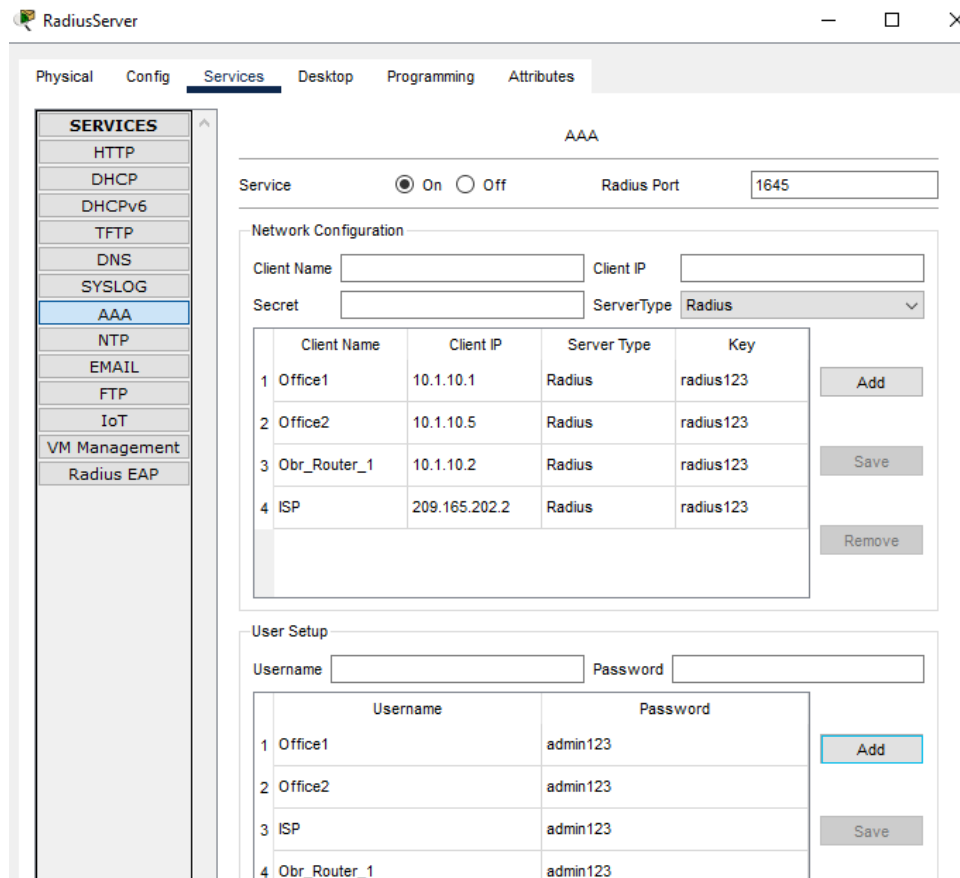


Рисунок 3.2 – Виконані налаштування Radius сервера

### 3.3.3 Налаштування NAT

Наступним етапом конфігурації мережі є налаштування стандарту NAT (Network Address Translation — трансляція мережевих адрес). Основна ідея та призначення NAT полягає у забезпеченні можливості кільком пристроям використовувати одну публічну IP-адресу для виходу в Інтернет. Для цього необхідно виконати заміну приватних IP-адрес на загальнодоступну IP-адресу.

Згідно із завдання, необхідно:

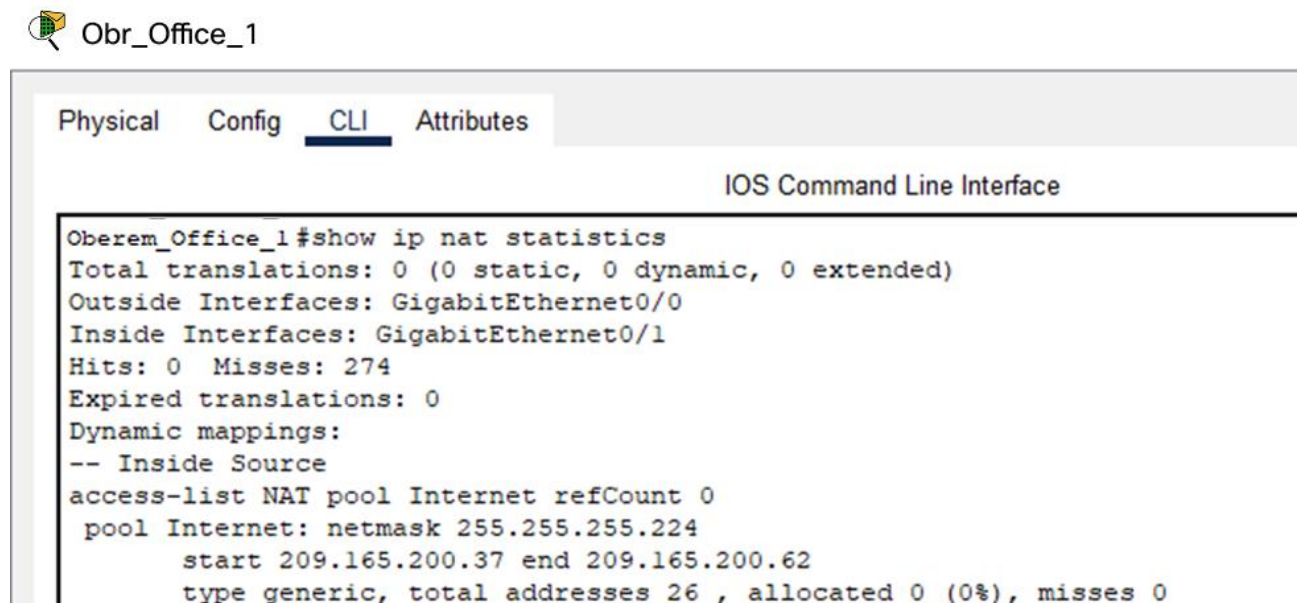
– для виходу робочих станцій в Інтернет необхідно налаштувати пограничний маршрутизатор з динамічним NAT за такими даними: ім'я пула Internet, пул адресів з 209.165.200.5 по 209.165.200.30, номер списку доступу 10;

– налаштувати сервер HTTP, щоб на вузлах при вводі в рядку браузера `http://123.dnipro.ua` (`http://209.165.200.4`) відкривався веб-сайт.

Послідовність дій, яка була виконана:

1. Створено пул Internet.
2. Налаштовано списки доступу.
3. Налаштовано NAT
4. Вказано, які інтерфейси вихідні, а які вхідні.
5. Налаштовано статичний нат для серверу HTTP та DNS.
6. Налаштовано сервер DNS щоб при вводі `http://123.dnipro.ua` (`http://209.165.200.4`) відкривався веб-сайт.

Результатом цих дій було налаштовано NAT, що зображено на рисунку 3.3.



The screenshot shows a terminal window titled 'Obr\_Office\_1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'show ip nat statistics'. The output shows that there are 0 translations (static, dynamic, or extended), 0 hits, and 274 misses. It also shows the configuration for a NAT pool named 'Internet' with a netmask of 255.255.255.224, starting at 209.165.200.37 and ending at 209.165.200.62. The pool is of type 'generic' and has 26 total addresses, with 0 allocated and 0 misses.

```
Oberem_Office_1#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: GigabitEthernet0/1
Hits: 0 Misses: 274
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list NAT pool Internet refCount 0
 pool Internet: netmask 255.255.255.224
   start 209.165.200.37 end 209.165.200.62
   type generic, total addresses 26 , allocated 0 (0%), misses 0
```

Рисунок 3.3 – Результат перевірки роботи NAT

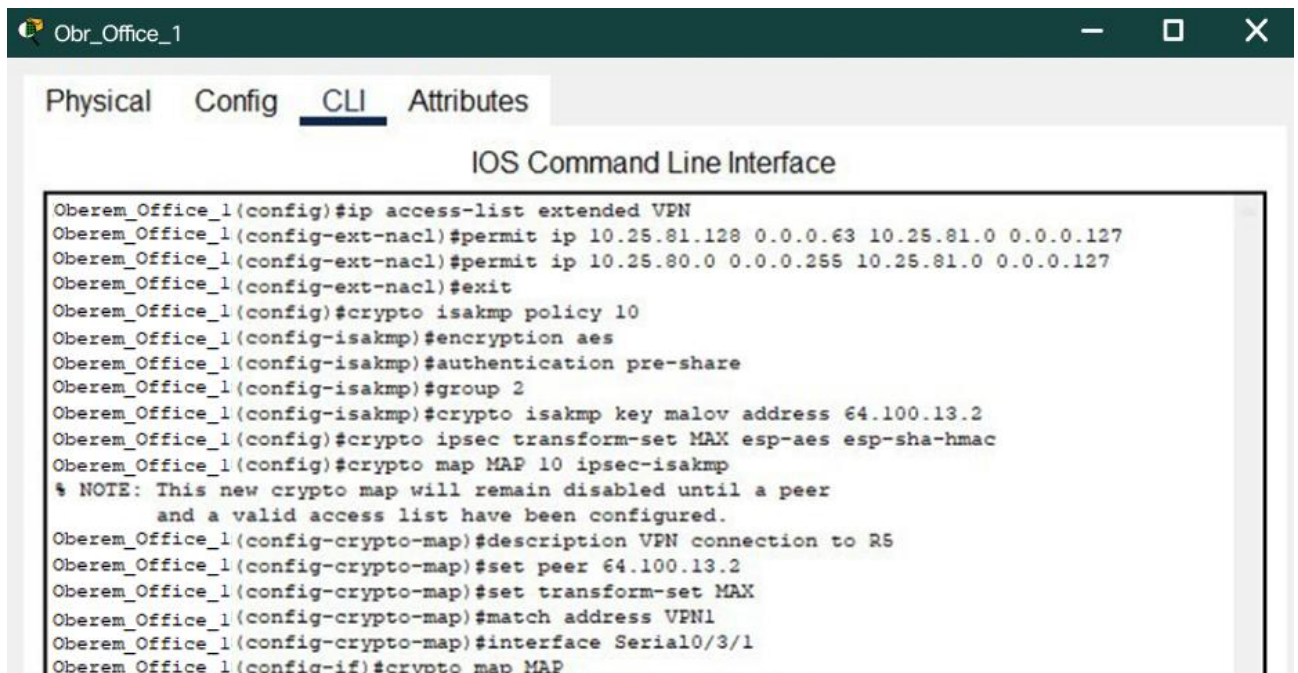
### 3.3.4 Налаштування VPN

VPN (Virtual Private Network) — це віртуальна приватна мережа, що забезпечує шифрування трафіку між користувачем і VPN-сервером та підмінює

IP-адресу пристрою. При встановленні VPN-з'єднання між комп'ютером і сервером формується захищений тунель для передачі даних. У цій мережевій топології, відповідно до поставленого завдання, було реалізовано site-to-site VPN із застосуванням протоколу IPsec для захисту трафіку між сегментами LAN3 та LAN.

Початковим етапом налаштування є створення списку доступу, який визначає дозволені для передачі підмережі організації. Далі необхідно налаштувати криптографічну політику, яка встановлює параметри автентифікації та метод шифрування. Важливо, щоб типи шифрування та криптографічні групи збігалися на обох маршрутизаторах, між якими організовується VPN. Наступним кроком є створення VPN-мапи та вказівка раніше створеного списку доступу. Після цього криптографічна мапа разом із параметрами Peer-роутера застосовується до інтерфейсу, що підключений до Інтернету.

Приклад налаштування на роутері першого офісу зображено на рисунку 3.4.



```
Obr_Office_1
Physical Config CLI Attributes
IOS Command Line Interface
Oberem_Office_1(config)#ip access-list extended VPN
Oberem_Office_1(config-ext-nacl)#permit ip 10.25.81.128 0.0.0.63 10.25.81.0 0.0.0.127
Oberem_Office_1(config-ext-nacl)#permit ip 10.25.80.0 0.0.0.255 10.25.81.0 0.0.0.127
Oberem_Office_1(config-ext-nacl)#exit
Oberem_Office_1(config)#crypto isakmp policy 10
Oberem_Office_1(config-isakmp)#encryption aes
Oberem_Office_1(config-isakmp)#authentication pre-share
Oberem_Office_1(config-isakmp)#group 2
Oberem_Office_1(config-isakmp)#crypto isakmp key malov address 64.100.13.2
Oberem_Office_1(config)#crypto ipsec transform-set MAX esp-aes esp-sha-hmac
Oberem_Office_1(config)#crypto map MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Oberem_Office_1(config-crypto-map)#description VPN connection to R5
Oberem_Office_1(config-crypto-map)#set peer 64.100.13.2
Oberem_Office_1(config-crypto-map)#set transform-set MAX
Oberem_Office_1(config-crypto-map)#match address VPN1
Oberem_Office_1(config-crypto-map)#interface Serial0/3/1
Oberem_Office_1(config-if)#crypto map MAP
```

Рисунок 3.4 – Налаштування VPN

### 3.3.5 Налаштування VLAN

VLAN (Virtual Local Area Network) — це технологія, яка дає змогу організувати віртуальні локальні мережі в межах однієї фізичної інфраструктури. За допомогою VLAN мережеві пристрої об'єднуються у логічні групи незалежно від їхнього фізичного розташування. Основними перевагами впровадження VLAN є підвищення ефективності роботи мережі, посилення її безпеки та спрощення адміністрування.

До ключових характеристик VLAN належать:

- Логічна сегментація мережі: За допомогою VLAN одна фізична мережа може бути поділена на кілька окремих логічних сегментів. Це дозволяє зменшити кількість широкомовних повідомлень у кожному сегменті й підвищити загальну продуктивність мережі.
- Підвищення рівня безпеки: Використання VLAN дає змогу ізолювати різні групи користувачів. Наприклад, співробітники фінансового відділу можуть працювати в окремій мережі, що знижує ймовірність несанкціонованого доступу до конфіденційних даних.
- Гнучкість і масштабованість: VLAN спрощують адміністрування мережі, оскільки дозволяють змінювати конфігурацію без фізичного перемикання пристроїв. Це особливо актуально в динамічних середовищах, де часто виникає потреба в оперативних змінах.
- Оптимізація керування трафіком: VLAN забезпечують можливість контролювати і пріоритезувати мережевий трафік, що гарантує належну якість обслуговування для критично важливих застосунків

Для налаштування мереж VLAN і маршрутизації між ними необхідно:

- створити 28, 38, 48, 99, 100 Vlan;
- вимкнути усі невикористовувані фізичні порти комутаторів;
- налаштувати Vlan;
- налаштувати транкові порти і порти доступу;
- налаштувати SVI-інтерфейси на комутаторах;
- налаштувати маршрутизацію між мережами VLAN;

- налаштувати маршрутизатор, що здійснює маршрутизацію між VLAN, в якості сервера DHCP для мереж VLAN;
- створити пули DHCP під назвою pollvlan№, де № – номер VLAN;
- виключити з пулу адреса мережевого обладнання;
- для кожного пулу вказати адресу DNS-сервера і шлюз за умовчанням.

Після виконання цих дій, було виконано перевірку динамічного розподілу адрес, що зображено на рисунках 3.5 та 3.6.

The screenshot shows the 'IP Configuration' window. Under 'IP Configuration', the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. Below this, the 'IPv4 Address' field contains the value '10.21.30.195' and the 'Subnet Mask' field contains the value '255.255.255.224'.

Рисунок 3.5 – Перевірка отримання вузлом адреси через DHCP

The screenshot shows the 'Gateway/DNS IPv4' window. Under 'Gateway/DNS IPv4', the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. Below this, the 'Default Gateway' field contains the value '10.21.30.226' and the 'DNS Server' field contains the value '10.21.30.236'.

Рисунок 3.6 – Перевірка отримання вузлом Gateway/DNS через DHCP

### 3.4 Перевірка роботи комп'ютерної мережі

Проведемо відправку пакетів між маршрутизаторами, щоб перевірити роботу OSPF та між ПК у різних підмережах, щоб перевірити статичний NAT та налаштовану маршрутизацію. Результат зображено на рисунку 3.7.

PDU List Window

Fire	Time(sec)	Last Status	Source	Destination	Type	Color	Num	Periodic	Edit	Delete
	0.000	Successful	Office1	Office2	ICMP		0	N	(edit)	
	0.000	Successful	Office1	Obr_Router_1	ICMP		1	N	(edit)	
	0.000	Successful	Office2	ISP	ICMP		2	N	(edit)	
	0.000	Successful	PC1	PC3	ICMP		3	N	(edit)	
	0.000	Successful	PC1	PC16	ICMP		4	N	(edit)	
	0.000	Successful	PC1	PC18	ICMP		5	N	(edit)	

Рисунок 3.7 – Результат перевірки OSPF, NAT та маршрутизації

Для перевірки DHCP необхідно перевірити IP конфігурації на ПК у різних підмережах, це зображено на рисунках 3.8-3.10.

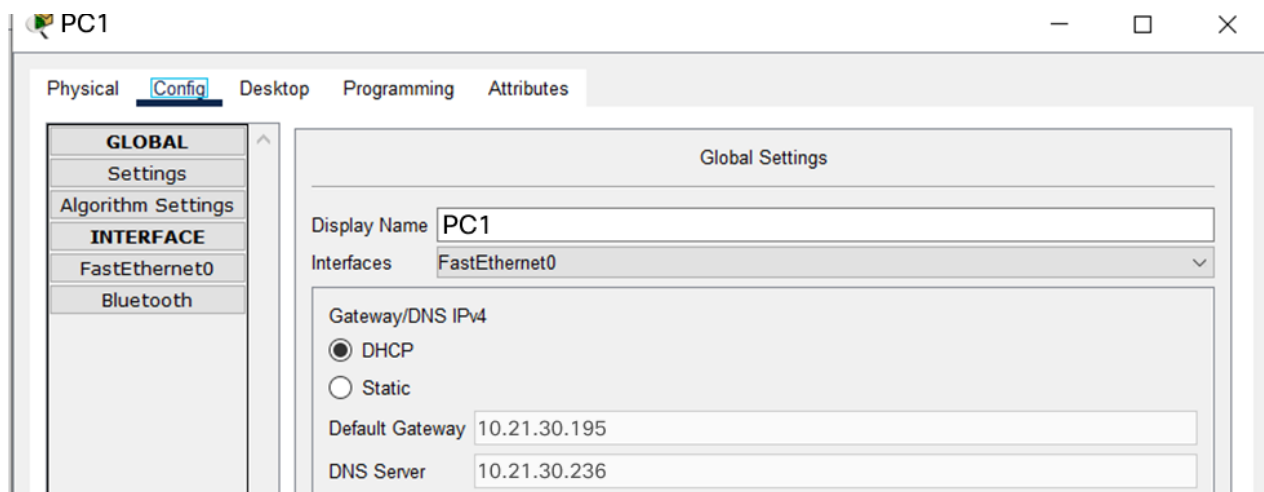


Рисунок 3.8 – Перевірка DHCP на LAN1

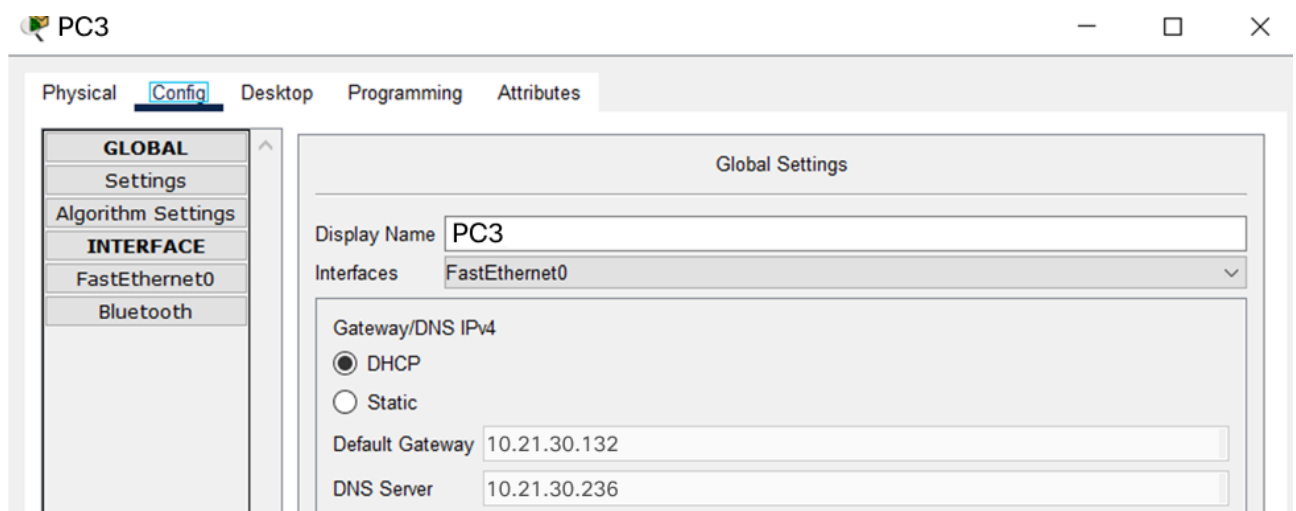


Рисунок 3.9 – Перевірка DHCP на LAN2

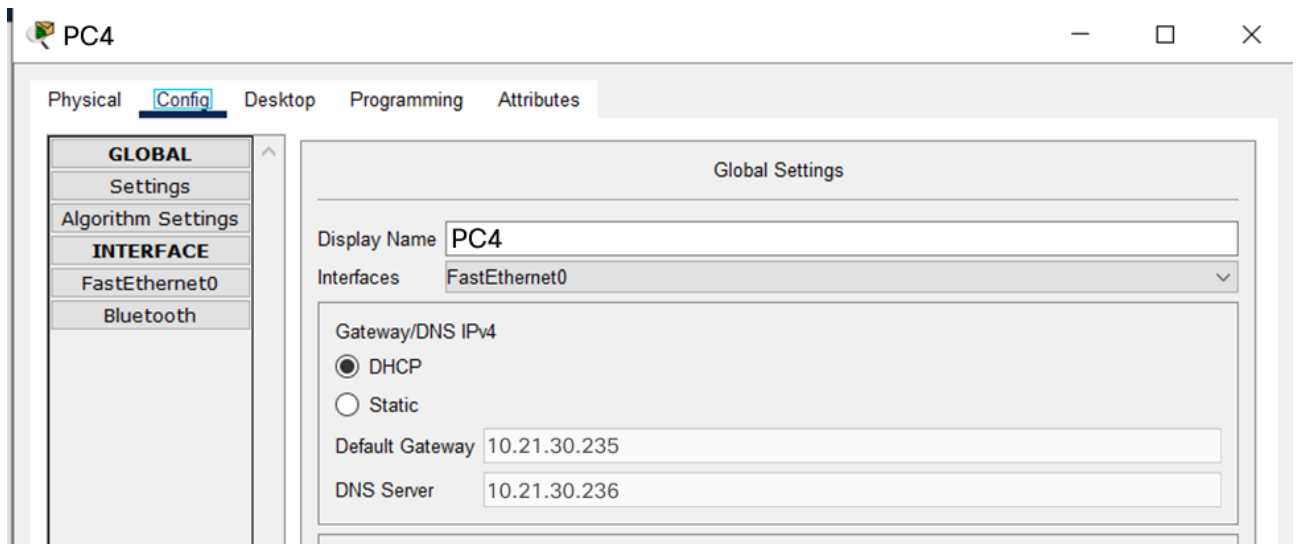


Рисунок 3.10 – Перевірка DHCP на LAN3

Для перевірки статичного NAT для серверів DNS та HTTP необхідно перейти за адресою 123.dnipro.ua, результат зображений на рисунку 3.11.

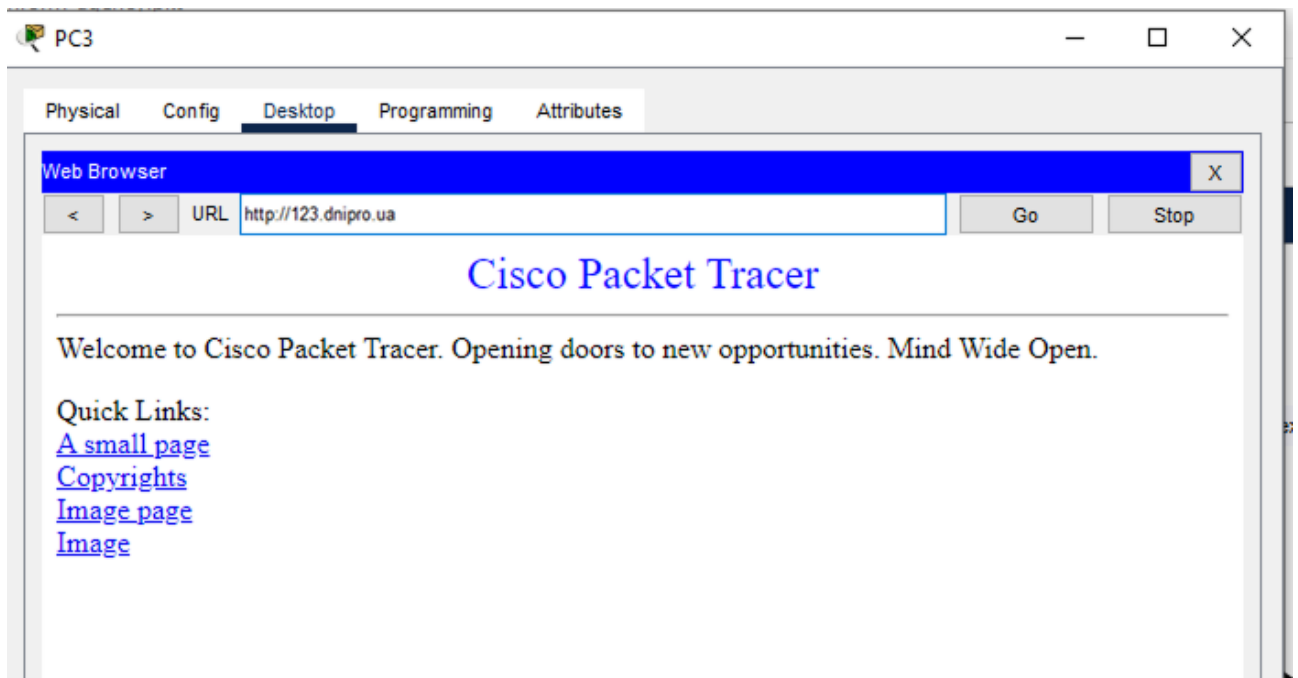


Рисунок 3.11 – Перевірка статичного NAT

Для перевірки роботи VPN була використана команда:  
 show crypto isakmp sa,  
 що відображає параметри обміну ключами Інтернету (IKE), результат цієї команди зображено на рисунку 3.12.

```

Obr_Office_1
Physical Config CLI Attributes
IOS Command Line Interface
Oberem_Office_1(config)#do show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state      conn-id slot status
209.165.202.1 10.1.10.5   QM_IDLE    1058     0 ACTIVE

IPv6 Crypto ISAKMP SA

```

Рисунок 3.12 – Перевірка роботи VPN

Також було перевірено роботу VLAN, за допомогою команди `show vlan brief`, що зображено на рисунку 3.13.

```

Sw_5_1
Physical Config CLI Attributes
IOS Command Line Interface
DEF Policy Mapping is disabled
Switch_5_1 #
Switch_5_1 #show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Gig0/1
10   Accounting               active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24
20   Resources_Department    active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14
30   Guest                   active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9
99   Management              active
100  Native                  active
1002 fddi-default           active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default        active
Poida_Switch #

```

Рисунок 3.13 – Перевірка VLAN

## ВИСНОВКИ

Сучасні інформаційні агенції використовують комплексні мережеві рішення, що поєднують хмарні сервіси, захищені комп'ютерні мережі, системи підтримки прийняття рішень, інтелектуальні технології та спеціалізовані платформи для автоматизації інформаційних процесів. Вибір конкретного рішення залежить від масштабу агенції, вимог до безпеки, обсягів інформації та необхідної гнучкості.

У результаті виконання кваліфікаційної роботи було досягнуто поставлену мету — розроблено комп'ютерну систему інформаційної агенції з урахуванням сучасних вимог до побудови, налаштування та забезпечення безпеки корпоративної мережі.

У процесі роботи:

1. Проведено детальний аналіз існуючих рішень щодо організації корпоративних мереж, що дозволило врахувати найкращі практики та сучасні технології для підвищення ефективності та захищеності інформаційної інфраструктури.
2. Вивчено структуру та розташування підрозділів інформаційної агенції, що забезпечило оптимальне проектування логічної та фізичної топології мережі з урахуванням специфіки взаємодії між підрозділами.
3. Розроблено архітектуру та топологію корпоративної мережі, що включає сегментування підсистем у вигляді окремих підмереж, впровадження VLAN, а також організацію захищених каналів зв'язку за допомогою VPN.
4. Складено схему комплексу технічних засобів і виконано підбір апаратного забезпечення відповідно до вимог продуктивності, надійності та масштабованості.

5. Реалізовано оптимізацію передачі даних, що забезпечує мінімізацію затримок, балансування навантаження та підвищення пропускнуєї спроможності мережі.
6. Виконано коректну адресацію мережевих пристроїв із застосуванням VLSM, що дозволило раціонально використовувати адресний простір та забезпечити гнучкість у подальшому масштабуванні мережі.
7. Передбачено можливість масштабування мережі для подальшого розвитку інформаційної агенції без необхідності суттєвих змін у структурі мережі.

Таким чином, розроблена корпоративна мережа відповідає сучасним вимогам щодо функціональності, безпеки, ефективності та гнучкості, забезпечуючи надійну основу для стабільної роботи інформаційної агенції та подальшого її розвитку – мета кваліфікаційної роботи досягнена.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Агентство інформаційне – Велика Українська Енциклопедія. [Електронний ресурс] – Режим доступу до ресурсу: [https://vue.gov.ua/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE\\_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5](https://vue.gov.ua/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5)
2. Захарчук І. Основні аспекти реєстрації та діяльності інформаційних агентств. [Електронний ресурс] – Режим доступу до ресурсу: <https://torgmarka.ua/ua/drukovani-zmi/osnovni-aspekti-reestratsiyi-ta-diyalnosti-informatsiynih-agentstv.html>
3. Реєстрація інформаційного агентства. [Електронний ресурс] – Режим доступу до ресурсу: <https://ogp.ua/uk/registration-enterprise-ukr/reiestratsiia-informatsiinoho-ahentstva>
4. Гарматій, О. В. Інформаційне забезпечення міжнародної діяльності: роль і значення інформаційних агентств. Міжнародні відносини: теоретико-практичні аспекти, 2018, 1, 244–254. <https://doi.org/10.31866/2616-745x.1.2018.142008>
5. Захарова І. В., Філіпова Л. Я., Задорожний І. С., Тарасенко Д. А. Основи інформаційно-аналітичної діяльності : навч. посіб. / І. В. Захарова, Л. Я. Філіпова, І. С. Задорожний, Д. А. Тарасенко ; 2-е вид., випр. і допов. Черкаси: Східноєвропейський університет імені Рауфа Аблязова, 2024. 347 с.
6. ЗАКОН УКРАЇНИ. Про інформацію. (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650). <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
7. Закон України. Про медіа. (Відомості Верховної Ради України (ВВР), 2023, №№ 47-50, ст.120). <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

8. Закон України. Про електронні комунікації. поточна редакція – Редакція від 01.04.2025, підстава - 4116-IX. <https://zakon.rada.gov.ua/laws/show/1089-20#n2282>
9. Закон України. Про інформаційні агентства. <https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80#Text>
10. Інформаційне агентство. Вікіпедія. [Електронний ресурс] – Режим доступу до ресурсу: [https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5\\_%D0%B0%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5_%D0%B0%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE).
11. Ковальова О. В. Інформаційне забезпечення професійної діяльності : навчальний посібник / О. В. Ковальова. – Київ: ВД «Дакор», 2021. – 288 с.
12. Використання комерційних хмарних технологій для обробки даних державних реєстрів України. IFES Україна | Квітень 2023. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ifesukraine.org/wp-content/uploads/2024/01/ifes-ukraine-the-use-of-commercial-cloud-technologies-for-processing-data-from-state-registers-of-ukraine-1.pdf>
13. Мережеві рішення. [Електронний ресурс] – Режим доступу до ресурсу: <https://softtim.com.ua/rishennya/merezhevi-rishennya>
14. Сучасні інформаційні технології та системи в управлінні [Електронний ресурс] : зб. матеріалів I Всеукр. наук.-практ. конф. молодих вчених, аспірантів і студентів ; 6–7 квітня 2017 р. – Київ : КНЕУ, 2017. – 213 с.
15. Peterson and Davie. Computer Networks: A Systems Approach. Release Version 6.1. 2019, 489P.
16. Комп'ютерні мережі. Курс лекцій. [Електронний ресурс] – Режим доступу до ресурсу: <https://e-tk.lntu.edu.ua/>
17. Cisco UCS C220 M3 Technical information. Технічні відомості. [Електронний ресурс] – Режим доступу до ресурсу:

<https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m3-lff-specsheet.pdf>

18. Cisco Catalyst 8300 Series Edge Platforms Data Sheet. [Електронний ресурс]

– Режим доступу до ресурсу:

<https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8300-series-edge-platforms/datasheet-c78-744088.html>

19. Комп'ютерні комплектуючі. Інтернет-магазин Brain. [Електронний

ресурс] – Режим доступу до ресурсу:

[https://brain.com.ua/ukr/Komplektuyuchi\\_do\\_PK-c204/](https://brain.com.ua/ukr/Komplektuyuchi_do_PK-c204/)

20. Офісні принтери та сканери. Canon. Продукція, рішення та послуги Canon

для бізнесу. [Електронний ресурс] – Режим доступу до ресурсу:

<https://www.canon.ua/business/products/office-printers/>