

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Пойди Кирила Вікторовича

(ПІБ)

академічної групи 123-21-1

(шифр)

спеціальності 123 Комп'ютерна інженерія

(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія

(офіційна назва)

на тему “Комп'ютерна система регіонального офісу громадської організації з
детальним опрацюванням побудови, налаштування та безпеки корпоративної
мережі”

(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Ткаченко С.М.			
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Панферова Я.В.			

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 Пойди К.В. академічної групи 123-21-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему “Комп'ютерна система регіонального офісу громадської організації 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. Ткаченко С.М.
(прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії _____ 16.06.2025

Прийнято до виконання _____

Пойда К.В.

РЕФЕРАТ

Пояснювальна записка: 62 с., 19 рис., 6 табл., 15 джерел.

ГРОМАДСЬКА ОРГАНІЗАЦІЯ, РЕГІОНАЛЬНИЙ ОФІС,
КОМП'ЮТЕРНА МЕРЕЖА, КОМП'ЮТЕРНА СИСТЕМА, ФІЗИЧНА
ІНФРАСТРУКТУРА, АРХІТЕКТУРА МЕРЕЖІ, МАРШРУТИЗАТОР,
НАЛАШТУВАННЯ МЕРЕЖІ, БЕЗПЕКА МЕРЕЖІ.

Об'єкт розробки – комп'ютерна система регіонального офісу громадської організації.

Мета роботи – розробка комп'ютерна система регіонального офісу громадської організації з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Для досягнення цієї мети було поставлено та виконано комплекс завдань: проведено аналіз існуючих технічних і організаційних рішень у сфері комп'ютерних систем громадських організацій; здійснено детальне вивчення структури та розміщення підрозділів регіонального офісу; розроблено топологію корпоративної мережі з урахуванням специфіки організації; сформовано схему комплексу технічних засобів для забезпечення функціонування мережі; підібрано оптимальне апаратне забезпечення, що відповідає вимогам проекту; проведено оптимізацію процесів передачі даних для підвищення ефективності мережі; забезпечено коректну адресацію мережевих пристроїв відповідно до розробленої топології; передбачено можливість масштабування мережі для подальшого розвитку громадської організації. Результати роботи включають створення надійної та безпечної комп'ютерної системи, що забезпечує ефективну взаємодію учасників організації та відповідає сучасним вимогам інформаційної безпеки і масштабованості. Для перевірки функціональності комп'ютерної системи була застосована програмна платформа Cisco Packet Tracer, яка використовувалась для моделювання топології корпоративної мережі.

Створена комп'ютерна мережа повністю відповідає вимогам кваліфікаційної роботи бакалавра.

ЗМІСТ

Перелік скорочень, умовних позначок, одиниць і термінів.....	6
Вступ.....	7
1 Стан питання та постановка завдання.....	8
1.1 Стисла характеристика галузі та умов застосування комп'ютерної системи регіонального офісу громадської організації.....	8
1.2 Характеристика і структура регіонального офісу громадської організації.....	11
1.3 Стислі відомості про технології збору й передачі даних та топологічна схема розміщення структурних підрозділів регіонального офісу громадської організації.....	14
1.4 Принципи та технічні способи інформаційного забезпечення роботи регіонального офісу громадської організації.....	17
1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об'єкта проектування, відомих рішень у галузі розробки КС ГО.....	19
1.6 Завдання і мета роботи.....	22
1.7 Визначення можливих напрямків рішення поставлених завдань.....	23
2 Розробка апаратної частини комп'ютерної системи.....	25
2.1 Технічні вимоги до комп'ютерної системи.....	25
2.1.1 Вимоги до системи в цілому.....	25
2.1.1.1 Вимоги до структури і функціонування системи.....	25
2.1.1.2 Вимоги до показників призначення.....	26
2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи.....	27
2.1.1.4 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи.....	28
2.1.1.5 Додаткові вимоги.....	28
2.1.2 Вимоги до функцій, виконуваних системою.....	30
2.1.3 Вимоги до видів забезпечення.....	32

	5
2.1.3.1 Вимоги до інформаційного забезпечення.....	32
2.1.3.2 Вимоги до лінгвістичного забезпечення.....	33
2.1.3.3 Вимоги до технічного забезпечення.....	34
2.1.3.4 Вимоги до організаційного забезпечення.....	34
2.1.3.5 Вимоги до методичного забезпечення.....	35
2.2 Розробка апаратної частини комп'ютерної системи	35
2.2.1 Визначення та обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи на основі врахування структури та топологічних особливостей об'єкту розробки.....	35
2.2.2 Розробка специфікації апаратних засобів комп'ютерної системи.....	37
2.2.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства.....	40
2.2.4 Розрахунок основних характеристик трафіку з метою підтвердження надійної роботи мережі.....	42
3 Розробка корпоративної мережі регіонального офісу громадської організації.....	45
3.1 Розрахунок схеми адресації корпоративної мереж.....	45
3.2 Розробка топологічної схеми корпоративної мережі.....	46
3.3 Налаштування мережі.....	47
3.3.1 Базове налаштування.....	47
3.3.2 Налаштування маршрутизації корпоративної мережі.....	49
3.3.3 Налаштування NAT.....	52
3.3.4 Налаштування VPN.....	53
3.3.5 Налаштування VLAN.....	54
3.4 Перевірка роботи комп'ютерної системи.....	56
Висновки.....	60
Перелік джерел посилання.....	61

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

- AIC – автоматизовані інформаційні системи;
- ГО – громадська організація;
- ІКТ – інформаційно-комунікаційні технології;
- ІТ – інформаційні технології;
- КС – комп’ютерна система;
- КМ – корпоративна мережа;
- ПК – персональний комп’ютер;
- РО – регіональний офіс;
- СУБД – системи управління базами даних;
- LAN – локальна мережа;
- MAC-адреса – унікальний ідентифікатор пристрою
- VLAN – віртуальна локальна мережа;
- CRM – управління взаємовідносинами з клієнтами;
- DHCP – протокол динамічного розподілу адрес вузлам;
- HTTP – протокол передачі гіпертексту;
- OSPF – протокол динамічної маршрутизації;
- VPN – віртуальна приватна мережа.

ВСТУП

Громадські організації (ГО) відіграють надзвичайно важливу роль у суспільному житті України, виконуючи функції посередника між державою і громадянами, а також активного учасника соціальних, культурних і правозахисних процесів. Вони сприяють посиленню соціальної згуртованості, підтримці вразливих груп населення, розвитку місцевих ініціатив і реалізації соціально-гуманітарних проєктів.

ГО є ключовими провайдерами змін, допомагаючи у впровадженні державних стратегій, зокрема в таких сферах, як демографічна політика, соціальний захист, відновлення країни після війни та забезпечення прав людини. Вони забезпечують уряд аналітичними даними, беруть участь у формуванні і контролі за реалізацією політик, а також створюють умови для активної участі громадян у процесах самоврядування та демократії участі.

Метою кваліфікаційної роботи є розробка комп'ютерна система регіонального офісу громадської організації з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі. Комп'ютерна система з мережевою підтримкою дозволить через забезпечення ефективного обміну інформацією між співробітниками та структурними підрозділами через локальну мережу підвищити оперативність прийняття рішень і координації діяльності, впровадити віддалений доступ для співробітників і волонтерів, що дасть змогу працювати з будь-якого місця, підвищуючи мобільність і гнучкість роботи.

В кваліфікаційній роботі викладений опис розробленої на базі сучасних мережевих технологій комп'ютерної системи регіонального офісу ГО. Громадські організації є важливим інструментом розвитку демократії, соціальної справедливості та відновлення України, вони зміцнюють зв'язок між державою і суспільством, підвищують якість життя громадян і сприяють побудові відкритого, відповідального суспільства, тому ця робота є актуальною.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп'ютерної системи регіонального офісу громадської організації

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

Громадська організація – це добровільне, організаційно оформлене об'єднання громадян, створене для реалізації спільних інтересів (культурних, економічних, соціальних, екологічних тощо) [1, 2].

Основна мета діяльності таких організацій – здійснення та захист прав і свобод членів, а також задоволення суспільних інтересів певної громади. Громадські організації можуть мати різні напрями: соціальний, економічний, культурний, екологічний, правозахисний тощо. Вони діють на принципах добровільності, самоврядування, рівноправності та гласності, не мають на меті отримання прибутку і не здійснюють господарську діяльність для збагачення [1, 2].

Галузь діяльності громадської організації (ГО) охоплює координацію волонтерської діяльності, організацію заходів, збір та обробку інформації про донорів, ведення бухгалтерської документації, а також взаємодію з громадянами, партнерами й органами влади. Основні завдання регіонального офісу ГО полягають у забезпеченні ефективної комунікації, прозорості діяльності, підвищенні залученості спільноти та оптимізації внутрішніх процесів [1, 2].

Функції громадських організацій включають:

- захист прав та інтересів членів,
- організацію освітніх, культурних, соціальних заходів,
- комунікацію та інтеграцію громадян,
- посередництво між громадянами та державними органами,
- соціальну підтримку різних верств населення.

Для сучасних ГО характерна динамічна робота з великими обсягами даних, необхідність швидкого прийняття рішень, автоматизації повторюваних офісних задач, а також підтримки відносин із донорами та волонтерами.

Для ефективної діяльності громадської організації важливим є впровадження комп'ютерної системи, яка дозволяє автоматизувати основні процеси [3]:

- Документообіг та звітність: Автоматизація обліку членів, фінансів, підготовки звітів, ведення протоколів зборів.
- Комунікації: Організація електронного листування, розсилок, управління контактами членів та партнерів.
- Планування заходів: Координація подій, реєстрація учасників, управління календарем організації.
- Інформаційна безпека: Захист персональних даних членів організації, резервне копіювання інформації, дотримання вимог законодавства щодо зберігання та обробки даних
- Інтеграція з іншими сервісами: Можливість підключення CRM-систем для управління відносинами з донорами, волонтерами, партнерами [4].
- Гнучкість і масштабованість: Використання систем з відкритим кодом або low-code/no-code рішень дозволяє адаптувати функціонал під специфіку організації, уникати зайвих витрат на ліцензії та швидко впроваджувати нові модулі.
- Технічна підтримка та навчання персоналу: Ефективне функціонування системи можливе лише за умови наявності кваліфікованого персоналу та регулярної підтримки програмного й апаратного забезпечення.

Комп'ютерна система для ГО повинна бути простою у використанні, підтримувати інтеграцію з іншими сервісами (електронна пошта, бухгалтерські програми, засоби комунікації), а також забезпечувати прозорість і підзвітність діяльності перед донорами, партнерами та громадськістю.

Врахування законодавчих вимог при застосуванні комп'ютерних систем у громадських організаціях є критично важливим із кількох причин [5]:

Захист інформації та персональних даних. Комп'ютерні системи зберігають великі обсяги важливої інформації, зокрема персональні дані членів організації, фінансову звітність, комерційні таємниці тощо. Недотримання законодавчих вимог щодо захисту цієї інформації може призвести до її втрати, несанкціонованого доступу, підробки або зловживань, що становить загрозу як для організації, так і для суспільства в цілому

Відповідальність за порушення. Законодавство України, зокрема Кримінальний кодекс, передбачає відповідальність за злочини у сфері використання комп'ютерних систем, включаючи несанкціонований доступ, втручання у роботу систем, розповсюдження неліцензійного програмного забезпечення тощо. Порушення цих норм може стати підставою для кримінальної відповідальності організації та її посадових осіб.

Дотримання авторських прав. Використання лише ліцензійного програмного забезпечення є обов'язковим, що підтверджено урядовими постановами. Це дозволяє уникнути юридичних ризиків, пов'язаних із використанням піратських програм, а також забезпечує підтримку та оновлення програмних продуктів

Інвентаризація та контроль. Законодавство вимагає ведення обліку встановлених програм, проведення планових і позапланових перевірок, а також інструктажу персоналу щодо правильного використання комп'ютерних систем. Це сприяє прозорості, підвищує рівень інформаційної безпеки та дозволяє своєчасно реагувати на можливі інциденти.

Міжнародна співпраця та стандарти. Дотримання законодавчих вимог забезпечує можливість співпраці з міжнародними партнерами, які часто висувають додаткові вимоги до захисту інформації та правового статусу програмного забезпечення.

1.2 Характеристика і структура регіонального офісу громадської організації

Громадська організація була заснована у 2014 році як волонтерська акція з відновлення будинків, знищених війною на сході України. У 2019 році ГО розпочала свою діяльність у регіонах, об'єднуючи активну молодь в українських містах. Регіональні офіси – це регіональний відділ, розташований у певному регіоні, який займається місцевими програмами, проєктами та ініціативами, які спрямовані на досягнення цілей та місії організації в цьому конкретному регіоні. Регіональні офіси з червня 2024 року підсилюють ініціативні групи в невеликих громадах та сприяють подальшому підвищенню громадянської активності молоді на півночі та півдні [6].

На рисунку 1.1 наведена структура регіонального офісу ГО.

Регіональний офіс складається з бухгалтерії, відділу грантів і партнерства, HR відділу, медіа відділу, фінансового відділу, відділу регіонального розвитку, технічного та проєктного відділі. Очолює регіональний офіс голова.

Штат РО (табл.1.1) включає в себе голову РО, головного бухгалтера, бухгалтерів, керівників відділів, менеджерів, дизайнерів, майстрів та координаторів проєктів.

Таблиця 1.1 – Штат регіонального офісу ГО

Відділ	Кількість штатних одиниць
Голова РО	1
Бухгалтерія	3
Керівники відділів	6
Менеджери	15
Дизайнер	1
Майстри	10
Координатори проєктів	15
Волонтери	Змінна кількість (не менше 50)

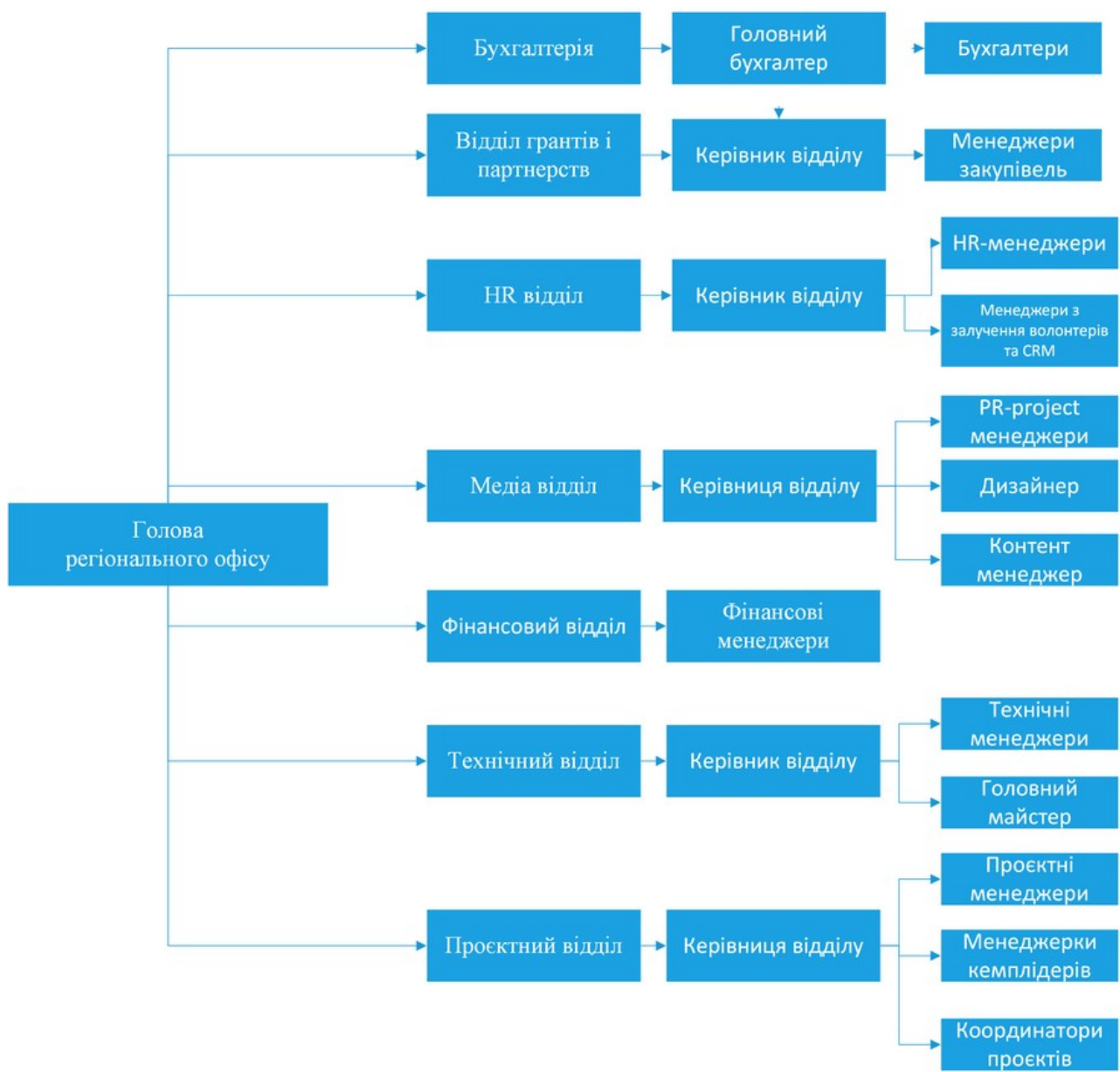


Рисунок 1.1 – Організаційна структура регіонального офісу ГО

Функціонал співробітників:

1. Функції голови:

- Керування регіональним офісом.
- Узгодження роботи усіх відділів .
- Представництво організації на заходах.
- Звітування .
- Затвердження операційних планів.
- Представлення організації іноземним партнерам.

2. Функції бухгалтерії:

- Розрахунок заробітної плати.
- Підрахунок витрат.
- Узгодження бюджетів проєктів з фінансовим та проєктним відділами.
- Обробка надходжень у вигляді грантів.
- Підготовка звітів для податкової.

3. Функції відділу грантів і партнерств:

- Пошук та вкладання партнерств.
- Комунікація з іноземними партнерами.
- Комунікація з партнерськими організаціями.
- Заповнення та обробка грантових заявок.
- Комунікації з громадами, які потребують допомоги.
- Звітуванням по грантовим програмами разом з проєктним та фінансовим відділами.

4. Функції відділу кадрів:

- Пошук нових працівників.
- Комунікація з командою.
- Розрахунок виїздів команди на заходи поза офісом.
- Комунікація з волонтерами.
- Обробка даних волонтерів в CRM системі.

5. Функції медіа відділу:

- Висвітлення діяльності в соціальних мережах.
- Розробка комунікаційних стратегій.
- Комунікація з інформаційними партнерами.
- Звітування по грантовим проєктам в соціальних мережах.
- Менторинг ініціативних груп в містах.
- Піар заходів, які відбуваються в інших містах.

6. Функції фінансового відділу:

- Розрахунок бюджету для проєктів.
 - Закупи необхідних матеріалів разом з технічним відділом.
 - Менторинг ініціативних груп.
 - Закупівля мерчу.
7. Функції відділу регіонального розвитку:
- Поширення ініціатив в регіонах.
 - Комунікація з громадами.
 - Комунікація та підтримка ініціативних груп в регіонах.
 - Співпраця з регіональними офісами.
 - Пошук можливостей для розширення діяльності в регіонах.
8. Функції технічного відділу:
- Розрахунок потрібних матеріалів для відбудов.
 - Комунікація з майстрами.
 - Комунікація з громадами, де проводяться відбудови.
 - Розрахунок кількості заїздів відбудовчих таборів.
9. Функції проєктного відділу:
- Розробка культурно-освітніх проєктів.
 - Реалізація культурно-освітніх проєктів.
 - Комунікація зі спікерами.
 - Розробка бюджету проєктів разом з фінансовим відділом.

1.3 Стислі відомості про технології збору й передачі даних та топологічна схема розміщення структурних підрозділів регіонального офісу громадської організації

Для ефективної роботи регіонального офісу громадської організації застосовуються сучасні технології збору та передачі даних, які забезпечують швидкий і надійний обмін інформацією між структурними підрозділами та зовнішніми партнерами:

Хмарні сервіси та цифрові інструменти (Google Workspace, Microsoft 365) дозволяють зберігати, обробляти й обмінюватися документами, електронною поштою, календарями та іншими даними в режимі онлайн з будь-якого місця [7].

Безпроводні технології передачі даних: Wi-Fi, мобільний інтернет (4G/5G), а також VPN-з'єднання для захищеного доступу до внутрішніх ресурсів офісу.

CRM-системи та інформаційні системи підтримки діяльності ГО використовуються для збору, обробки та аналізу даних про членів організації, донорів, волонтерів, що підвищує ефективність комунікації та управління.

Технології резервного копіювання та захисту даних забезпечують збереження інформації та мінімізацію ризиків втрати даних.

Топологія мережі регіонального офісу громадської організації має ієрархічну структуру (рис.1.2):

- Центральний офіс (головний сервер, центральна база даних, основні робочі станції) – ядро мережі, де зосереджені основні ресурси та управління.
- Відокремлені структурні підрозділи (філії, місцеві осередки, регіональні офіси) підключені до центрального офісу через захищені канали зв'язку (VPN, захищені Wi-Fi мережі, мобільний інтернет).
- Користувачі та робочі місця у кожному підрозділі мають доступ до локальних ресурсів і центральної бази даних через мережу.
- Інтеграція з хмарними сервісами забезпечує гнучкість і мобільність роботи, дозволяючи співробітникам працювати віддалено.

Така топологія забезпечує надійність, безпеку передачі даних і ефективно координує діяльність між підрозділами регіонального офісу.

Використання сучасних технологій збору і передачі даних у поєднанні з продуманою топологією мережі дозволяє регіональному офісу громадської

організації ефективно виконувати свої функції, забезпечуючи швидкий доступ до інформації, її безпеку та зручність роботи співробітників.

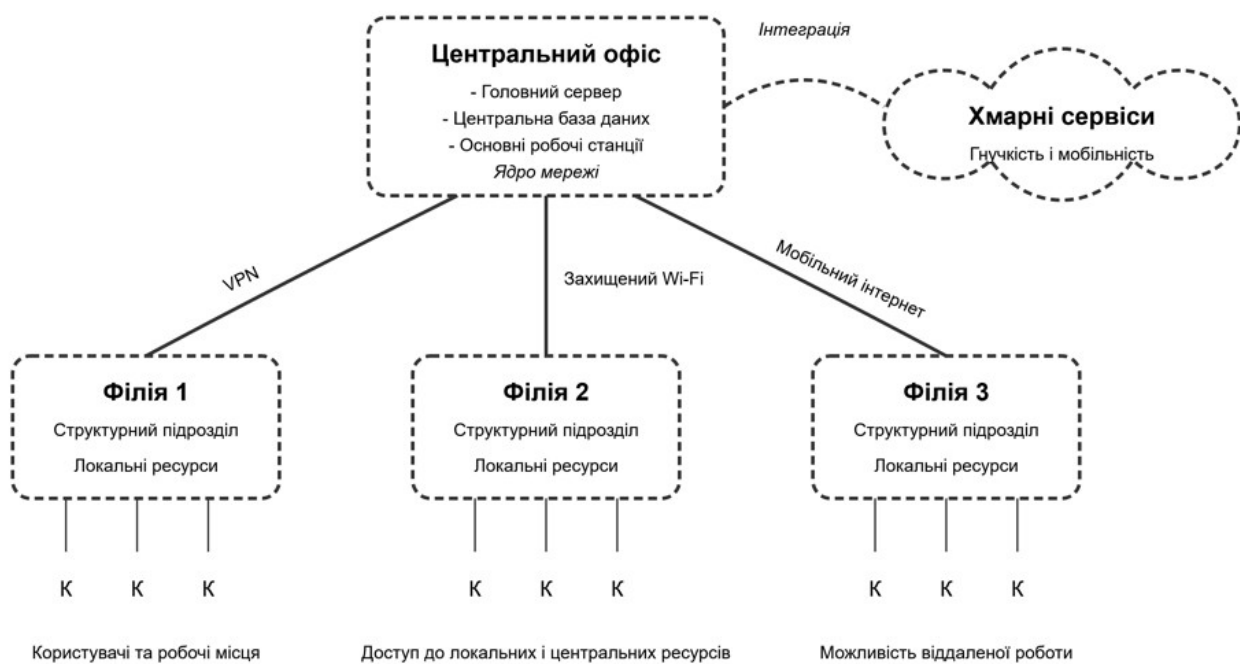


Рисунок 1.2 – Топологія комп’ютерної мережі громадської організації

Відділ грантів та партнерств займається пошуком донорів, оформленням грантових заявок, оформленням бюджетів разом з бухгалтерією та фінансовим відділом.

HR відділ займається залученням волонтерів, комунікацією з ними, збором та обробкою даних пов’язаних з волонтерами та їх діяльністю.

Проектний відділ займається розробкою, аналізом та втіленням проєктів громадської організації. Також відділ займається комунікацією з волонтерами/контрактними працівниками, які зайняті на період втілення певних проєктів.

Медіа відділ займається розробкою та втіленням комунікаційних стратегій в соціальних мережах, медіа, радіо.

Технічний відділ разом з проєктним та фінансовим відділами займаються створенням та розрахунком планів відбудови. Та комунікують з волонтерами/майстрами з допомогою HR відділу під час проєктів організації.

Фінансовий відділ займається виконанням умов співпраці з донорами та допомагає розраховувати та фіналізувати фінансові розрахунки під час втілення проєктів.

Регіональний офіс громадської організації винаймає приміщення в передмісті (рис.1.3). Окремі кабінети мають голова офісу, бухгалтерія та технічний відділ. Інша частина офісу це так званий «openspace» зручний для роботи, враховуючи, що співробітники постійно спільно працюють над реалізацією різноманітних проєктів. Також в офісі є великий коворкінг та невелика кімната для нарад.

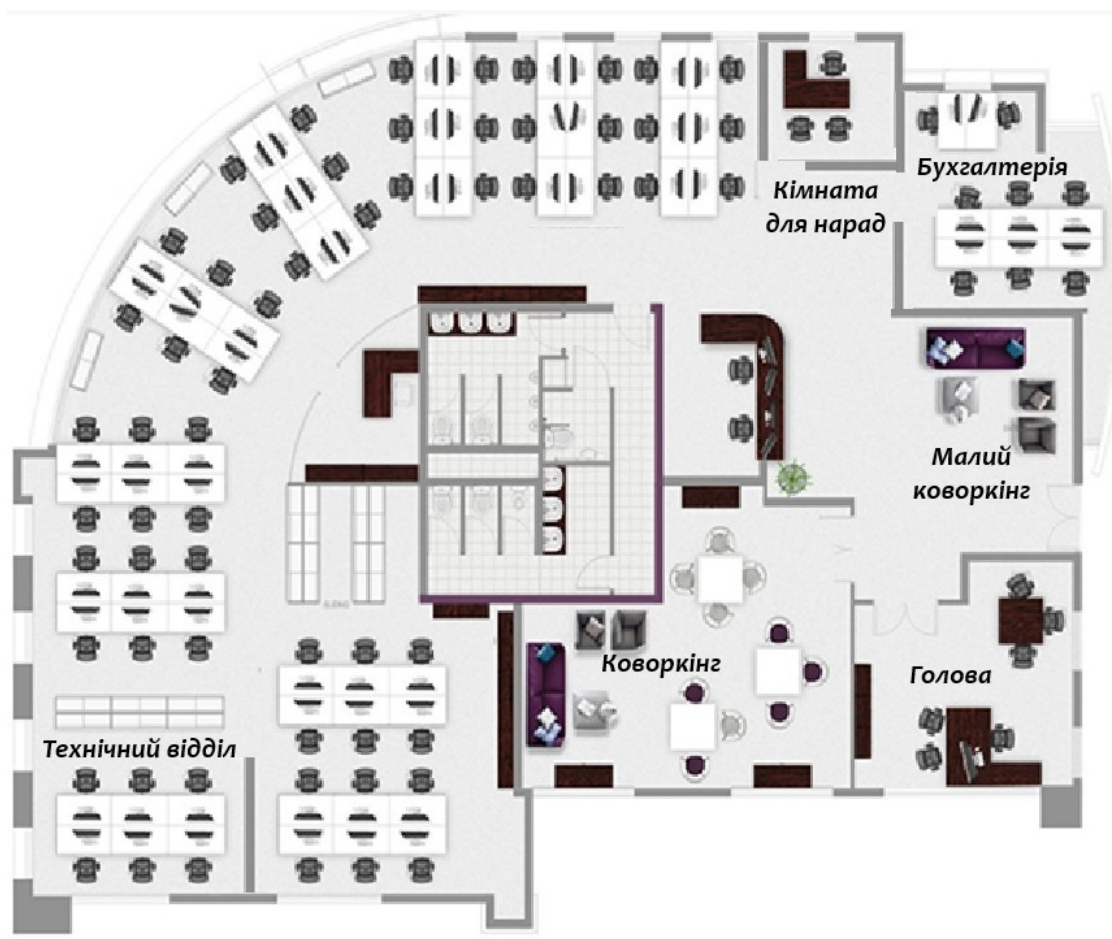


Рисунок 1.3 – План приміщення регіонального офісу ГО

1.4 Принципи та технічні способи інформаційного забезпечення роботи регіонального офісу громадської організації

Інформаційне забезпечення роботи регіонального офісу громадської організації базується на принципах достовірності, координації, захисту та відкритості інформації, а технічні способи включають комплекс сучасних інформаційних систем, мережевих технологій і заходів безпеки, що забезпечують ефективну підтримку діяльності організації.

Основними принципами інформаційного забезпечення роботи регіонального офісу ГО є [8]:

Інформативність – забезпечення своєчасного, достовірного і повного інформування всіх учасників процесу діяльності організації відповідно до їхніх функцій та завдань.

Організаційна координація – сприяння координованості дій структурних підрозділів та членів організації для ефективного виконання завдань.

Управлінська підтримка – надання інформації, необхідної для прийняття управлінських рішень, контролю за їх виконанням та планування діяльності.

Комунікативність – забезпечення ефективного обміну інформацією між підрозділами, членами організації, партнерами та громадськістю.

Достовірність і актуальність – інформація має бути правдивою, своєчасно оновлюваною та відповідати реальному стану справ.

Захист інформації – дотримання заходів безпеки для запобігання несанкціонованому доступу, втраті чи пошкодженню даних.

Доступність і відкритість – забезпечення вільного доступу до інформації для членів організації та, за потреби, для громадськості, з урахуванням законодавчих вимог.

Ці принципи забезпечуються технічними способами такими як:

Автоматизовані інформаційні системи (АІС) – програмно-апаратні комплекси для збору, обробки, зберігання та поширення інформації, що підвищують оперативність і якість інформаційних процесів.

Локальні та мережеві комп'ютерні системи – забезпечують обмін даними між структурними підрозділами офісу, інтеграцію з центральними базами даних та зовнішніми ресурсами.

Інтернет-технології та хмарні сервіси – дозволяють організувати дистанційний доступ, спільну роботу над документами, електронний документообіг та комунікацію з партнерами і громадськістю.

Системи управління базами даних (СУБД) – для централізованого зберігання, структуризації та швидкого пошуку інформації про членів, партнерів, фінанси тощо.

Засоби інформаційної безпеки – антивірусне програмне забезпечення, міжмережеві екрани (фаєрволи), системи контролю доступу, резервне копіювання даних для захисту інформації.

Офіційний веб-сайт та електронні платформи – для інформування громадськості, публікації звітів, новин, організації зворотного зв'язку.

Спроектовані рішення мають гарантувати надійність і стабільність роботи системи, забезпечувати захист від збоїв, мінімізувати втрати даних, а також підтримувати конфіденційність, цілісність і доступність інформації за допомогою відповідних програмних та апаратних засобів захисту. Крім того, система повинна бути гнучкою для адаптації до нових вимог і інтеграції з іншими комп'ютерними системами. Важливо також забезпечити ефективне використання ресурсів під час впровадження та експлуатації системи.

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

Сучасні інформаційні системи для громадських організацій будуються на основі системного підходу, автоматизації ключових процесів, забезпечен-

ня безпеки та зручності користування. Вибір конкретних рішень залежить від розміру організації, її структури, бюджету та специфічних потреб, але основними тенденціями залишаються автоматизація, інтеграція з сучасними сервісами та орієнтація на користувача.

Сучасні підходи до обробки інформації у громадських організаціях базуються на використанні інформаційно-комунікаційних технологій (ІКТ), які забезпечують автоматизацію збору, обробки, аналізу та передачі даних для підвищення ефективності діяльності. Основні підходи включають [9, 10]:

Автоматизація інформаційних процесів – впровадження інформаційних систем підтримки діяльності, які дозволяють оперативно збирати, зберігати та обробляти великі обсяги даних, що сприяє якісній організації роботи громадських організацій.

Використання онлайн-платформ і соціальних мереж – ці інструменти слугують для комунікації, поширення інформації, залучення нових учасників та координації спільнот, що значно розширює вплив організацій.

Інформаційно-комунікаційні технології нової публічної служби – підхід, що передбачає не лише обмін інформацією, а й активну кооперацію між комунікатором і реципієнтом для спільного вирішення суспільних проблем, підвищення прозорості та підзвітності.

Впровадження інформаційно-аналітичних систем, які автоматизують обробку інформаційних масивів, забезпечують оперативний доступ до даних і підтримують прийняття управлінських рішень.

Застосування кібернетичного підходу – створення спеціалізованих інформаційних систем, які інтегрують обробку інформації з управлінськими функціями, що підвищує ефективність координації та контролю діяльності.

Використання сучасних інтернет-сервісів і Web 2.0 технологій – соціально орієнтовані сервіси, форуми, веб-платформи для колективної комунікації, що забезпечують накопичення, обмін і поширення інформації в режимі реального часу.

Таким чином, громадські організації активно впроваджують комплексні інформаційні системи, що поєднують автоматизацію, інтерактивність і аналітичну підтримку, що дозволяє підвищити ефективність управління, залучення громадськості та прозорість діяльності.

Комп'ютерна мережа регіонального офісу громадської організації – це сукупність комп'ютерів та інших пристроїв, об'єднаних для забезпечення ефективного обміну даними, координації роботи співробітників і доступу до спільних ресурсів у межах офісу та між віддаленими підрозділами. Це локальна мережа з ієрархічною структурою, що забезпечує надійний, безпечний і ефективний обмін інформацією між співробітниками і підрозділами, сприяючи оптимізації роботи організації. Основні характеристики:

Тип мережі. Локальна комп'ютерна мережа (LAN), яка охоплює приміщення регіонального офісу, з можливістю інтеграції з віддаленими підрозділами через захищені канали (VPN, шифровані тунелі).

Структура. Ієрархічна топологія з ядром мережі, яке забезпечує маршрутизацію і захист (наприклад, маршрутизатор Mikrotik RB2011UIAS-2Hnd-IN), а також комутатори доступу для підключення робочих станцій і периферійних пристроїв.

Кількість робочих станцій. 70 комп'ютерів, об'єднаних в групи відповідно до структурних підрозділів (голова РО, бухгалтерія-фінансовий відділ, технічний відділ, openspace).

Обмін інформацією. Мережа забезпечує спільне використання файлів, доступ до централізованих баз даних, роботу з програмним забезпеченням (наприклад, бухгалтерські або CRM-системи), а також організацію внутрішньої електронної пошти і комунікацій (чат, відеозв'язок).

Безпека. Використання міжмережевих екранів (фасрволів), систем контролю доступу, шифрування даних і резервного копіювання для захисту інформації від несанкціонованого доступу та втрат.

Для роботи КМ ГО потрібно таке обладнання: комутатори з достатньою кількістю портів і підтримкою швидкості 1 Гбіт/с (з урахуванням мож-

ливості масштабування, наприклад, Ruijie Reye RG-NBS5100-24GT4SFP-P);⁷ маршрутизатори для підключення до Інтернету та організації VPN-з'єднань між офісами; точки доступу Wi-Fi для бездротового підключення мобільних пристроїв; якісні кабелі для забезпечення стабільної швидкості (категорії не нижче Cat5e або Cat6).

Переваги використання комп'ютерної мережі в регіональному офісі ГО:

1. Економія часу та ресурсів за рахунок централізованого доступу до інформації.
2. Підвищення продуктивності працівників через швидкий обмін даними.
3. Можливість одночасної роботи кількох користувачів з одним програмним забезпеченням.
4. Забезпечення віддаленого доступу до робочих файлів і систем.
5. Підвищення рівня координації та комунікації між структурними підрозділами.

1.6 Завдання і мета роботи

Мета даної кваліфікаційної роботи полягає в розробці комп'ютерної системи регіонального офісу громадської організації з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Для реалізації поставленої мети кваліфікаційної роботи необхідно виконати комплекс наступних завдань:

1. Здійснити аналіз існуючих технічних та організаційних рішень у сфері реалізації КС громадських організацій.
2. Провести детальне вивчення структури та розміщення підрозділів регіонального офісу ГО.
3. Розробити топологію корпоративної мережі з урахуванням специфіки організації.

4. Сформувати схему комплексу технічних засобів, що забезпечують функціонування мережі.
5. Виконати підбір оптимального апаратного забезпечення, що відповідає вимогам проекту.
6. Провести оптимізацію процесів передачі даних для підвищення ефективності мережі.
7. Забезпечити коректну адресацію мережевих пристроїв відповідно до розробленої топології.
8. Передбачити можливість масштабування мережі з метою забезпечення подальшого розвитку ГО.

1.7 Визначення можливих напрямків рішення поставлених завдань

Проектування комп'ютерної мережі громадської організації має враховувати особливості її діяльності, масштаби, технічні вимоги та ресурси. Основні напрямки рішення проектування КМ можуть включати [11-13]:

1. Створення відповідального підрозділу або призначення відповідальної особи за інформаційні технології та проектування мережі, що дозволить централізовано управляти процесом і координувати дії між різними відділами.
2. Визначення функцій і повноважень підрозділу або фахівців, які відповідатимуть за планування, впровадження та підтримку мережі, а також за навчання персоналу і забезпечення технічної підтримки.
3. Врахування інтеграції з іншими інформаційними системами організації (CRM, бухгалтерія, документообіг), що потребує продуманого вибору мережевої архітектури і обладнання для забезпечення сумісності та ефективності.
4. Планування масштабованості та гнучкості мережі, щоб забезпечити можливість розширення, підключення нових підрозділів або від-

далених користувачів, а також адаптації до змін у технологіях і потребах організації.

5. Забезпечення інформаційної безпеки, включаючи використання міжмережевих екранів (фаєрволів), систем контролю доступу, шифрування даних і резервного копіювання для захисту конфіденційної інформації.
6. Використання сучасних технологій збору і передачі даних, зокрема хмарних сервісів і безпроводних мереж, що дозволяє підвищити мобільність працівників і ефективність комунікації.
7. Розробка детальної топологічної схеми мережі, що враховує розміщення структурних підрозділів, їхню взаємодію і канали зв'язку, для забезпечення надійності і швидкості обміну інформацією [14-15].
8. Документування проєкту мережі з описом обладнання, налаштувань, процедур безпеки і планів розвитку, що є важливим для подальшої підтримки і модернізації системи.

Ці напрямки відповідають сучасним підходам до проектування інформаційної інфраструктури в громадських організаціях і сприяють створенню надійної, безпечної та ефективної комп'ютерної мережі, яка підтримує їхню діяльність і розвиток.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

Комп'ютерна система регіонального офісу громадської організації повинна бути комплексно спроектована з урахуванням сучасних стандартів апаратного забезпечення, мережевої інфраструктури, безпеки інформації та зручності експлуатації, що забезпечить ефективну підтримку діяльності ГО.

Вимоги до комп'ютерної системи регіонального офісу громадської організації охоплюють технічні, мережеві, безпекові та експлуатаційні аспекти, що забезпечують ефективну, надійну та безпечну роботу офісу в цілому.

2.1.1.1 Вимоги до структури і функціонування системи

Комп'ютерна мережа має бути поділена на 4 підсистеми:

1. Підсистема адміністрації. Використовується для адміністративного забезпечення діяльності регіонального офісу ГО, в тому числі координація роботи проектних менеджерів, через автоматизовані системи документообігу. Для кожного вузла необхідно забезпечити мінімальні параметри мережевого підключення до глобальної мережі: пропускна здатність не менше 1 Мбіт/с, затримка не більше 150 мс, втрата пакетів – не більше 5%.
2. Підсистема фінансового відділу та бухгалтерії. У цю підсистему повинні надходити текстові звіти та статуси з усіх підмереж компанії, а також з неї мають відправлятися текстові інструкції. Через цю підсистему здійснюється моніторинг всіх фінансових потоків: фіксація операцій із надходження та використання коштів.. Для кожного вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі: пропускна здатність не менше 1 Мбіт/с, затримка не більше 150 мс, втрата пакетів не перевищує 5%.

3. Підсистема загального робочого простору з достатньою кількістю робочих місць з вільним доступом до електроживлення та мережевих розеток. Дана підсистема, крім робочих станцій, повинна бути оснащена принтерами, сканерами, багатофункціональними пристроями для спільного використання і сервером TFTP. Мережа підсистеми має відповідати базовим вимогам: забезпечувати сталий доступ до інтернет з мінімальною швидкістю передачі даних 45 Мб/с, затримку не більше 100 мс та втрату пакетів не вище 1% для кожного вузла.
4. Підсистема технічного відділу. Крім робочих станцій, підсистема повинна бути оснащена DNS-сервером. Для кожного вузла необхідно забезпечити мінімальні параметри мережевого з'єднання з доступом до глобальної мережі: пропускна здатність не менше 1 Мбіт/с, затримка не більше 150 мс, втрата пакетів – не більше 5%.

Розроблена комп'ютерна мережа має бути встановлена та налаштована таким чином, аби була можливість розширення, тобто, повинна бути можливість додання нових робочих станцій чи серверів до існуючих підсистем, так і додання нових підсистем.

2.1.1.2 Вимоги до показників призначення

У підмережах компанії має бути забезпечена максимальна швидкість передачі даних до 100 мегабайт на секунду. При цьому максимальна швидкість обміну інформацією між підмережами має становити не менше 1000 мегабайт на секунду.

Необхідно забезпечити регулярне технічне обслуговування робочих станцій, серверів та мережевого обладнання кожні 3-6 місяців. Забезпечення безперебійної роботи мережі та серверів має становити не менше 99% часу, без зупинок і перебоїв.

Система повинна гарантувати стабільне функціонування всього обладнання, підключеного до комп'ютерної мережі. Крім того, комп'ютерна мережа має бути інтегрована з глобальною мережею Інтернет.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи

Експлуатаційні вимоги:

- Надійність і масштабованість. Система повинна підтримувати розширення мережі, додавання нових користувачів і пристроїв без значного впливу на продуктивність.
- Моніторинг і управління. Використання систем моніторингу мережі (SNMP), централізоване управління конфігураціями обладнання.
- Резервне копіювання і відновлення. Наявність регулярних процедур резервного копіювання даних та планів відновлення після збоїв.

Умови та порядок експлуатації системи.

Система має забезпечувати виконання своїх функцій з високим рівнем надійності та безпеки. Необхідно гарантувати захист системи від несанкціонованого доступу, втручання або пошкоджень. Система повинна бути оснащена автоматичними засобами діагностики, контролю, корекції та відновлення у разі виникнення помилок чи збоїв. Обов'язковим є наявність резервних копій даних та програмного забезпечення для запобігання втраті інформації. Система має підтримувати можливість оновлення та модернізації без припинення її роботи.

Вимоги до параметрів електроживлення та заземлення:

- Живлення системи повинно бути стабільним від мережі 220 В з частотою 50 Гц.
- Система має бути захищена від перепадів напруги, коротких замикань, перегріву та перевантажень.

- Аварійне живлення від акумуляторних батарей або генератора, що забезпечує роботу системи не менше 2 годин при відключенні основного живлення.
- Надійне заземлення для запобігання впливу статичної електрики та електромагнітних завад.

Планове технічне обслуговування системи проводиться кожні 6 місяців і включає перевірку апаратної частини, очищення вентиляторів і фільтрів, заміну зношених або пошкоджених компонентів, контроль параметрів живлення та заземлення, перевірку роботи програмного забезпечення, оновлення драйверів та антивірусних баз, дефрагментацію жорсткого диску тощо.

У разі виявлення несправностей або збоїв система підлягає позаплановому обслуговуванню, що передбачає детальну діагностику причин, усунення несправностей, заміну компонентів або програмного забезпечення, а також тестування і налаштування системи.

Для проведення ремонту та обслуговування система повинна мати комплект запасних деталей і приладів, що включає модулі, плати, кабелі, конектори, індикатори, перемикачі тощо. Цей комплект підлягає постійному обліку та інвентаризації, 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

Система має бути забезпечена достатньою кількістю кваліфікованого обслуговуючого персоналу для підтримки її безперебійної роботи. Мінімальна кількість працівників повинна включати не менше 2х системних адміністраторів.

Обслуговуючий персонал повинен мати високий рівень професійної підготовки та досвід роботи з комп'ютерними системами, а також пройти спеціальне навчання і атестацію перед початком роботи з системою.

2.1.1.5 Додаткові вимоги

Система повинна бути здатна надійно функціонувати в умовах підвищеної вологості повітря до 60 % та температури навколишнього середовища, що може сягати до 45°C, забезпечуючи стабільність роботи обладнання в таких кліматичних умовах.

Електричні розетки мають бути стандарту Schuko з чітким позначенням робочої напруги та максимально допустимого струму. Вони також повинні розташовуватися на висоті не менше 0,5 метра від підлоги та на відстані не більше 2 метрів від відповідних електропристроїв для забезпечення безпечного та зручного підключення.

Інформаційні розетки слід використовувати типу RJ-45 або DB-9 залежно від конкретних технічних вимог, при цьому кожна розетка має бути чітко маркована номером порту для полегшення ідентифікації. Розетки повинні бути встановлені на висоті не менше 0,5 метра від рівня підлоги, а відстань між розетками та підключеними до них пристроями не повинна перевищувати 2 метри, що забезпечує зручність експлуатації та мінімізує ризик пошкодження кабелів.

Комунікаційне обладнання необхідно розміщувати в спеціалізованих металевих шафах, які відповідають стандарту захисту IP65, що забезпечує захист від пилу та вологи. Такі шафи мають бути обладнані дверцятами, системами вентиляції та освітлення для підтримки оптимальних умов експлуатації обладнання. Для підвищення рівня безпеки приміщення або шафи повинні бути оснащені замками та системами контролю доступу, що обмежує несанкціонований доступ до критичних мережевих компонентів.

Кабельні канали мають бути виготовлені з металу та обладнані кришками для захисту прокладених кабелів. Вони повинні відповідати стандарту захисту IP65, що гарантує захист від пилу та водяних струменів. Для зручності підключення пристроїв кабельні канали повинні мати спеціальні отвори, через які кабелі можуть виходити у відповідних точках підключення.

Таким чином, ці вимоги гарантують надійність, безпеку та довговічність роботи комп'ютерної системи в регіональному офісі громадської організації навіть в умовах підвищеної вологості та температурних коливань, а також забезпечують зручність і безпеку експлуатації мережевої та електричної інфраструктури.

2.1.2 Вимоги до функцій, виконуваних системою

Функції технічного відділу забезпечують ефективне, безпечне та надійне адміністрування комп'ютерної мережі регіонального офісу громадської організації, сприяючи стабільній роботі інформаційної інфраструктури та захисту даних. Вимоги до функцій підсистеми адміністрування та технічного відділу:

- Управління доступом і аутентифікація користувачів.
- Моніторинг і діагностика мережі.
- Управління мережевими пристроями.
- Забезпечення безпеки мережі.
- Адміністрування IP-адресації.
- Резервування та відновлення.
- Логування та звітність.
- Підтримка масштабованості.

Основні функції підсистеми фінансового відділу та бухгалтерії:

- Автоматизація облікових процесів (забезпечення ведення бухгалтерського та фінансового обліку відповідно до чинного законодавства та внутрішніх стандартів організації).
- Управління бюджетом і фінансовим плануванням.
- Обробка платіжних та фінансових документів.
- Звітність і аудит.
- Контроль за рухом грошових коштів: відстеження надходжень і витрат, управління касовими операціями, банківськими рахунками та іншими фінансовими потоками.

- Оновлення програмного забезпечення відповідно до змін у законодавстві та бухгалтерських стандартах.
- Облік податкових зобов'язань, формування податкової звітності, розрахунок податків і зборів.
- Впровадження заходів щодо захисту конфіденційної фінансової інформації.
- Аналіз витратної частини бюджету, контроль за дотриманням фінансової дисципліни.

Ці функції забезпечують ефективне управління фінансовими ресурсами регіонального офісу громадської організації, підвищують прозорість і контроль фінансової діяльності, а також сприяють дотриманню нормативних вимог.

Основні функції підсистеми адміністрації КМ регіонального офісу громадської організації спрямовані на ефективне управління людськими ресурсами, забезпечення виконання законодавства, координацію діяльності, соціальний захист працівників та підтримку організаційної діяльності офісу в регіоні, а саме:

- Адміністративне забезпечення діяльності офісу: ведення кадрової документації, організація внутрішнього документообігу, забезпечення інформаційної підтримки.
- Планування та організація кадрової роботи, визначення потреб у персоналі, формування штатного розпису, підбір, розстановка та мотивація кадрів для ефективного виконання завдань організації.
- Забезпечення виконання законодавчих та нормативних актів, контроль за дотриманням законів.
- Підтримка управлінських функцій: забезпечення інформаційної підтримки прийняття рішень, планування, контролю і аналізу діяльності регіонального офісу ГО.

- Організація документообігу, реєстрація, обробка, зберігання і контроль виконання документів, що підтримує управлінську діяльність офісу.
- Координація діяльності структурних підрозділів, організація взаємодії між відділами, контроль виконання кадрових завдань, методичне забезпечення та підтримка.
- Підвищення кваліфікації та мотивація персоналу, формування корпоративної культури.
- Контроль за дотриманням трудових прав, організація соціальних програм, взаємодія з органами соціального захисту населення.
- Забезпечення антикорупційних заходів і дотримання етичних норм.
- Забезпечення обміну даними з адміністративною, офісною та іншими підсистемами для узгодженості інформації та ефективної координації діяльності.

Основні функції підсистеми загального робочого простору (openspace) регіонального офісу громадської організації (ГО) полягають у створенні організаційно-технічних умов для ефективної спільної роботи співробітників офісу. До них належать:

- Організація робочих місць (оснащення робочих місць необхідними меблями, технічними засобами обробки інформації, створення комфортних і безпечних умов роботи).
- Надання засобів комунікацій для внутрішнього і зовнішнього зв'язку, що сприяє спільному виконанню завдань і обміну інформацією.
- Створення умов для ефективного використання робочого часу співробітників.
- Централізоване управління ресурсами: використання серверів для зберігання даних і надання мережевих сервісів дозволяє організувати контроль доступу, захист інформації і координацію роботи робочих станцій.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до інформаційного забезпечення

Інформаційне забезпечення має містити повні, достовірні та актуальні дані, необхідні для виконання завдань організації, що забезпечує ефективність прийняття рішень.

Важливо забезпечити захист інформації від несанкціонованого доступу, втрати чи пошкодження, що включає використання систем інформаційної безпеки та контролю доступу.

Комп'ютерна система повинна підтримувати автоматизацію основних функцій організації, таких як облік, контроль, управління, комунікації та аналітика, що підвищує ефективність діяльності, та забезпечувати сумісність та обмін інформацією між різними підсистемами та реєстрами, що сприяє створенню єдиної інформаційної бази ГО.

Система має бути зручною для користувачів, забезпечувати автоматизовані робочі місця з відповідним функціоналом і інтерфейсом.

Впровадження електронних засобів для обробки, зберігання та передачі документів підвищує оперативність і зменшує паперовий документообіг.

Інформаційне забезпечення має відповідати законодавчим та нормативним актам, що регламентують діяльність громадських організацій, зокрема щодо збереження персональних даних та звітності.

2.1.3.2 Вимоги до лінгвістичного забезпечення

Лінгвістичне забезпечення комп'ютерної системи громадської організації має гарантувати якісну, коректну та зручну роботу з текстовою інформацією, забезпечуючи ефективну комунікацію та документообіг відповідно до мовних потреб організації.

Система має забезпечувати повноцінну роботу з державною мовою, включаючи правильне відображення, введення, обробку та зберігання текстової інформації. Лінгвістичне забезпечення повинно включати словники,

гларарії, термінологічні бази, які уніфікують терміни, що використовуються в діяльності організації, для уникнення неоднозначностей.

Необхідне забезпечення автоматичного аналізу текстів (розпізнавання частин мови, синтаксичний розбір) для підтримки пошуку, класифікації та обробки інформації.

Враховуючи співпрацю з міжнародними організаціями, в тому числі, грантодавцями, необхідна підтримка багатомовності, система має підтримувати переклад, транслітерацію, а також інтерфейс користувача кількома мовами, засоби перевірки орфографії, граматики, стилістики, а також можливостей машинного перекладу чи розпізнавання мови.

Лінгвістичне забезпечення повинно бути тісно інтегроване з інформаційною системою для забезпечення ефективної комунікації, обробки документів і звітності.

Лінгвістичне забезпечення має відповідати державним стандартам щодо використання мови в офіційних документах і звітності громадських організацій.

2.1.3.3 Вимоги до технічного забезпечення

Для DNS-сервера необхідно забезпечити мінімум 128 ГБ оперативної пам'яті та 2 ТБ основного накопичувача, а також процесор з не менше ніж 2 ядрами і тактовою частотою від 1,7 ГГц.

DHCP-сервер повинен мати щонайменше 16 ГБ оперативної пам'яті, 2 ТБ основного диска та процесор з 2 ядрами і частотою від 1,7 ГГц.

Обраний маршрутизатор Cisco має бути оснащений мінімум чотирма портами RJ-45 і підтримувати розширення для модулів NIM-1T або NIM-4T.

Мережа підприємства повинна включати чотири комутатори з 24 портами RJ-45 кожен.

Робочі станції мають бути оснащені не менше ніж 16 ГБ оперативної пам'яті DDR4 та твердотільним накопичувачем SSD об'ємом 240 ГБ з форм-фактором 2,5 дюйма.

Монітори. Роздільна здатність Full HD (1920x1080) з діагоналлю близько 22 дюймів для комфортної роботи.

Периферія. Наявність USB-портів (USB 2.0, USB 3.0), Ethernet-портів для підключення до мережі, а також інших необхідних інтерфейсів.

2.1.3.4 Вимоги до організаційного забезпечення

Новий персонал повинен пройти навчання на основі заздалегідь підготовлених інструкцій та документації, що охоплюють як обладнання, з яким вони працюватимуть, так і інформаційне забезпечення системи, перш ніж розпочати виконання своїх обов'язків.

Регулярно мають проводитися інструктажі з аналізом типових помилок та повторенням матеріалів із документації й інструкцій для підвищення компетентності співробітників компанії.

2.1.3.5 Вимоги до методичного забезпечення

Повинні бути розроблені нормативні документи з експлуатації, які встановлюватимуть правила та рекомендації щодо використання комп'ютерної системи та її складових, а також заходи з попередження і усунення несправностей та аварійних ситуацій. Такі нормативи мають включати розділи, присвячені технічному обслуговуванню, діагностиці, ремонту, модернізації та іншим відповідним аспектам.

2.1 Розробка апаратної частини комп'ютерної системи

2.2.1 Визначення та обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи на основі врахування структури та топологічних особливостей об'єкту розробки

Відповідно до організаційної структури підприємства та розроблених технічних вимог було спроектовано топологічну схему розміщення обладнання КМ ГО (рис. 2.1).

Таким чином, кожна підсистема була виділена в окрему підмережу. Було вирішено розмістити маршрутизатори та сервери у спеціальній шафі в кімнаті технічного відділу, або в нішах в бухгалтерії, офісі голови та спільному робочому просторі. Кімната, як і всі шафи, мають дверці, які закриваються на замок, доступ до них мають системні адміністратори та голова.

До підмережі LAN1 відносяться дві кімнати - офіс голови та коворкінг. Комутатори та маршрутизатори встановлені в офісі голови у спеціальній шафі. Шафа, має дверці, які закриваються на замок, доступ до них мають системні адміністратори та голова.

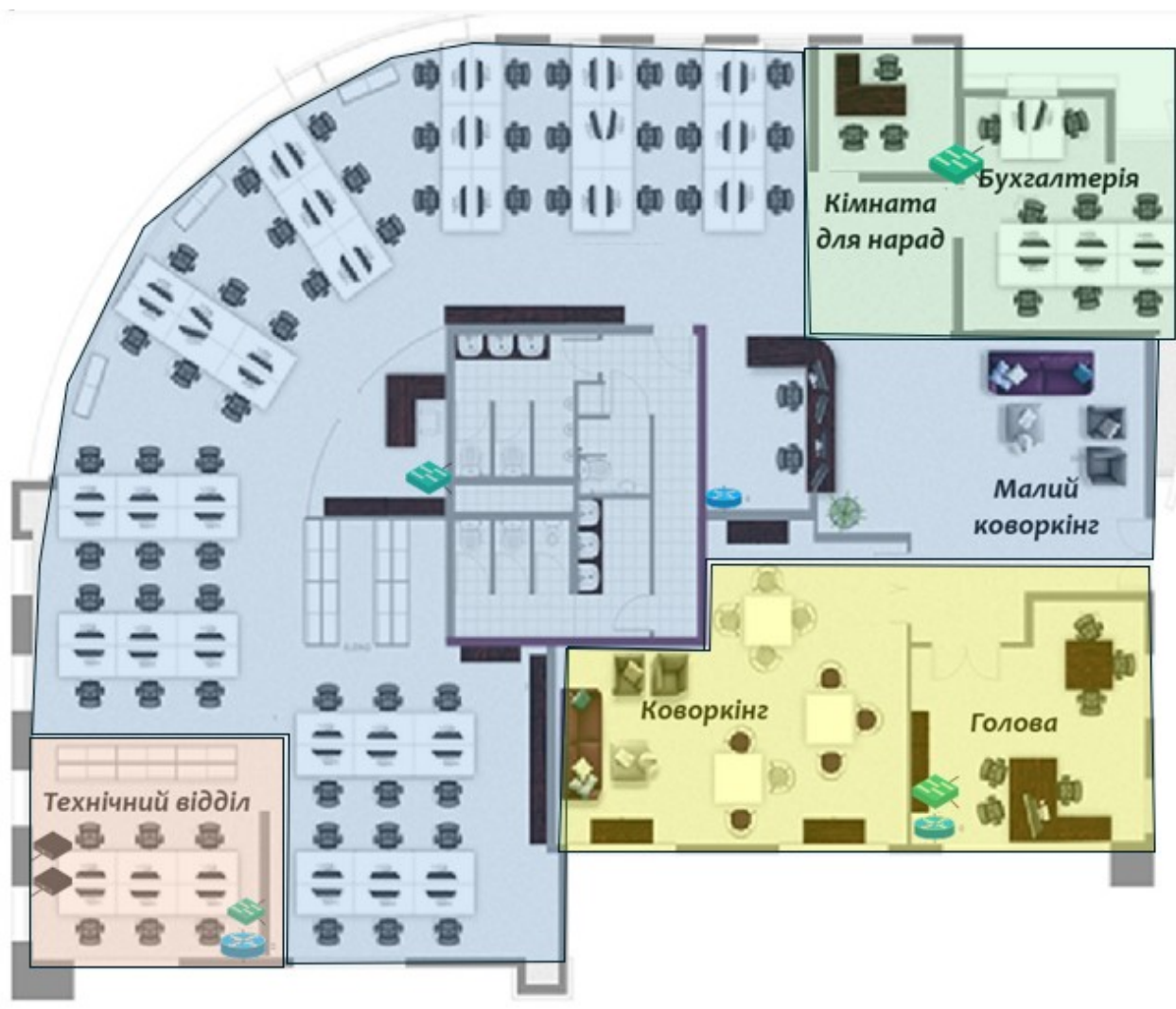


Рисунок 2.1 – Топологічна схема розміщення обладнання КМ ГО

До підмережі LAN2 відносяться дві кімнати – бухгалтерія та фінансові менеджери і кімната для нарад. Комутатори та маршрутизатори встановлені в бухгалтерії у спеціальній шафі. Шафа, має дверці, які закриваються на замок, доступ до них мають системні адміністратори та голова.

До підмережі LAN3 відноситься кімната технічного відділу. Комутатори та маршрутизатори встановлені у спеціальній шафі. Шафа, має дверці, які закриваються на замок, доступ до них мають системні адміністратори та голова.

До підмережі LAN4 відноситься спільний робочий простір та малий коворкінг. Комутатори та маршрутизатори встановлені у спеціальній шафі в ніші. Шафа, має дверці, які закриваються на замок, доступ до них мають системні адміністратори та голова.

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 серверної частини комп'ютерної системи було обрано два сервери Cisco UCS C220 M3 LFF у різних конфігураціях, що наведені в таблиці 2.1. Cisco UCS C220 M3 LFF – це стоечний сервер формату 1U, призначений для роботи як із віртуалізованими, так і з традиційними додатками. Сервер відзначається високою продуктивністю, масштабованістю та надійністю при компактних розмірах. Модель підтримує до двох процесорів Intel Xeon серії E5-2600 та до 512 ГБ оперативної пам'яті, а також може містити до восьми 3,5-дюймових жорстких дисків або SSD. Завдяки своїм характеристикам Cisco UCS C220 M3 LFF підходить для широкого спектра завдань, включаючи сервери баз даних, веб-сервери та віртуалізацію, що робить його оптимальним рішенням для дата-центрів із обмеженим простором.

Окрім високої продуктивності та надійності, сервер Cisco UCS C220 M3 LFF оснащений розширеними функціями для спрощення управління та обслуговування. Зокрема, він підтримує Cisco UCS Manager, що забезпечує централізоване керування кількома серверами через єдиний інтерфейс, а також Cisco Integrated Management Controller (IMC), який надає можливості віддаленого моніторингу та управління обладнанням.

В якості маршрутизаторів у комп'ютерній системі було вибрано три пристрої Cisco Catalyst 8300-1N1S-4T2X у різних конфігураціях, наведені в таблиці 2.1. Cisco Catalyst 8300-1N1S-4T2X – це модульний корпоративний маршрутизатор для філій, що входить до серії периферійних платформ Cisco Catalyst 8300 і призначений для прискореного надання мережевих послуг. Пристрій має форм-фактор 1U, оснащений одним слотом PIM, одним NIM та одним SM, а також підтримує 10Gig WAN Cisco SD-WAN із можливістю роботи з 5G/LTE мережами. Маршрутизатор підтримує як статичну, так і динамічну маршрутизацію, а також функції DHCP, що забезпечує гнучке керування мережею.

Коли для з'єднання маршрутизаторів використовувався послідовний кабель, було встановлено додаткові модулі NIM-1T або NIM-4T. Модуль Cisco NIM-1T забезпечує один послідовний WAN-порт, тоді як Cisco NIM-4T має чотири послідовні WAN-порти.

Для мережевої інфраструктури було вибрано чотири комутатора Cisco Catalyst 9300 IE-9320-24P4S-E. Цей захищений комутатор забезпечує високу швидкість Ethernet-з'єднань у компактному форм-факторі та оснащений 24 гігабітними портами. Максимальна пропускна здатність комутації в повнодуплексному режимі досягає 56 Гбіт/с, що повністю відповідає вимогам організації.

Для організації більших підмереж було обрано два стекові комутатори Meraki MS355-48X-HW, які забезпечують високопродуктивне підключення у корпоративних мережах. Кожен комутатор оснащений 48 портами RJ45 зі швидкістю до 1 Гбіт/с та двома QSFP+ портами для високошвидкісних

з'єднань. Пристрій має загальну пропускну здатність 544 Гбіт/с та пропускну здатність стекування до 400 Гбіт/с. Крім того, комутатор підтримує маршрутизацію рівня 3 та технологію UPoE для живлення підключених пристроїв.

Для персональних комп'ютерів співробітників було обрано такі комплектуючі: процесор AMD Ryzen 3, дві планки оперативної пам'яті DDR4 по 8 ГБ 2666 МГц від Goodram, а також твердотільний накопичувач SSD 2.5" об'ємом 240 ГБ AS350X Araser та HDD на 1 ТБ. Обраний процесор має 2 ядра та 4 потоки з тактовою частотою 3,2 ГГц, що разом із 16 ГБ оперативної пам'яті та інтегрованою відеокартою забезпечує комфортну роботу і задовольняє базові технічні вимоги необхідного програмного забезпечення.

Було лазерний принтер Canon i-SENSYS MF275dw, який поєднує функції друку, копіювання, сканування та факсу. Принтер забезпечує високу швидкість друку до 29 сторінок на хвилину у форматі А4. Пристрій оснащений процесором із тактовою частотою 1200 МГц і має пам'ять обсягом 256 МБ, що забезпечує стабільну та швидку роботу. Роздільна здатність друку – до 2400 x 600 dpi – гарантує чіткість і якість документів. Крім того, пристрій підтримує інтерфейси Wi-Fi, LAN та USB.

Для організації локальної обчислювальної мережі було обрано Ethernet-кабель виробництва компанії ATcom, що відповідає категорії 6. Кабель складається з чотирьох пар скручених мідних провідників діаметром 0,51 мм і має екранування типу FTP (Foil Twisted Pair), що знижує вплив електромагнітних завад. Зовнішня оболонка виготовлена з ПВХ, що забезпечує його придатність для внутрішнього монтажу. Кабель підтримує передачу даних на швидкостях до 1 Гбіт/с із пропускну здатністю до 250 МГц і сумісний із кабелями категорій 5 та 5e. Він оптимально підходить для застосувань у Gigabit Ethernet та Fast Ethernet. Загальна довжина закупівлі становить 610 метрів, з яких 215 метрів залишено як резерв для ремонту, розширення мережі або непередбачених потреб.

Для з'єднання частини маршрутизаторів послідовним кабелем було використано кабель Smart Serial Back-to-Back Smart Serial DCE DTE, який при-

значений для підключення двох маршрутизаторів Cisco з інтерфейсами Smart Serial. Цей кабель оснащений роз'ємом 12-в-1 Smart Serial, розробленим компанією Cisco, а його мережеві кінці мають стандартні фізичні роз'єми, що найчастіше застосовуються для відповідних інтерфейсів.

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

По- зи- ція	Найменування	Технічна характеристика	Кі- лькіст ь	Порти	Примітки
1	Cisco UCS C220 M3 LFF	2 процесори E5-2650 v2 1.7-2.1 GHz, 8 модулів оперативної пам'яті на 32 GB 1333Mhz, 1 SSD на 100GB, 2 жорстких диски на 3 TB кожен	1	2 RJ-45	DNS 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	DHCP сервер
3	Cisco Catalyst 8300- 1N1S-4T2X	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 9300 IE-9320-24P4S-E	4 GB оперативної пам'яті, 8 GB флеш-пам'яті	2	24 RJ-45, 4 SFP	Для підмереж
5	Meraki MS355-48X- HW	-	1	48 RJ-45, 2 QSFP+	Для підмереж
6	PC	AMD Ryzen 3, загальна відеокарта AMD Radeon Graphics, 16 GB операти- вної пам'яті DDR4 - 2666 МГц, HDD 1 ТБ, SSD 240 ГБ Роздільна здатність: 2400x600 dpi,	50	1 RJ-45	Робочі станції
7	Canon i-Sensys MF275dw	формат: A4, технологія друку: лазерна, кількість картреджів: 4	3	RJ-45, USB	Принтер
8	ATcom FTP cat.6 ССА 4 pairs 0.51 mm, internal, PVC	250Мг, 4 пари по 0.51 мм	1000м	RJ-45	Для поєднання мере- жевих пристроїв

По- зи- ція	Найменування	Технічна характеристика	Кі- лькіст ь	Порти	Примітки
9	Smart Serial Back-to- Back Smart Serial DCE DTE Cable	0.75 м	4	DB-25	Для поєднання маршрутизаторів

2.2.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Відповідно до технічних вимог, і структури громадської організації «Будуємо Україну Разом», найбільшою локальною мережею має бути підмережа LAN 4, де на етапі розгортання має бути розміщено 50 ПК в спільному робочому просторі.

Для проведення розрахунків відомі наступні дані:

- середня довжина вихідного повідомлення в локальній мережі LAN 4 (l) дорівнює 650 байтам, або 5200 бітам;
- затримка передачі пакету в локальній мережі LAN 4 ≤ 6 мс;
- середня інтенсивність вихідного трафіку в локальній мережі LAN 4 (μ) = 108 кадрів/с;
- кількість вузлів в локальній мережі LAN 4 (N) = 50;
- кількість портів в комутаторів рівня доступу в локальній мережі LAN 4 (n) = 80;
- пропускна здатність ліній передачі даних в локальній мережі LAN 4 (C) = 100000000 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 μ – середня інтенсивність вихідного трафіку в локальній мережі LAN 4;

l – середня довжина вихідного повідомлення в локальній мережі LAN 4⁷
;

n – Кількість портів в комутаторі рівня доступу в локальній мережі LAN 4

Тобто $Pp.p = 108 * 5200 * 80 = 44928000$ (біт/с) = (44.928 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 4;

l – середня довжина вихідного повідомлення в локальній мережі LAN 4.

Тобто $\mu_{\text{вих}} = 1000000000$ біт/с / 5200 біт = 192307 (пакетів/с).

Було розраховано максимальну кількість кінцевих вузлів, яких локальна мережа LAN 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 4;

μ – середня інтенсивність вихідного трафіку в локальній мережі LAN 4.

Тобто $N = 192307 / 108 \approx 1780$ одиниць.

Було розраховано інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 3 за формулою 2.4.

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

де N – кількість вузлів в мережі в локальній мережі LAN 4;

μ – середня інтенсивність вихідного трафіку в локальній мережі LAN 4.

Тобто $\lambda = 50 * 108 = 5400$ 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 4 було застосовано формулу 2.5.

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

де λ – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 4;

$\mu_{\text{вих}}$ – значення інтенсивності виходу пакетів на секунду в локальній мережі LAN 4.

Тобто $\rho = 5400 / 192307 \approx 0,028$.

Було розраховано коефіцієнт зайнятості комутаторів в локальній мережі LAN 4, для цього було застосовано формулу 2.6.

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

де ρ – коефіцієнту затримки на рівні розподілу в локальній мережі LAN 4.

Тобто $r = 0,028 / (1 - 0,028) \approx 0,0288$.

Було розраховано значення середньої затримки кадру в локальній мережі LAN 4, 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 LAN 4;

λ – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 4.

$$T = 1 / (192307 - 5400) \approx 5,35 * 10^{-6} \text{ секунд}$$

Використовуючи попередні розрахунки, було розраховано середню довжину черги в локальній мережі LAN 4. Для цього було використано формулу 2.8.

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

де ρ – коефіцієнту затримки на рівні розподілу в локальній мережі LAN 4.

$$\text{Тобто } L_{\text{черги}} = (0,0288)^2 / (1 - 0,0288) \approx 8,54 * 10^{-4}$$

Було розраховано середній час перебування пакета в черзі в локальній мережі LAN 4 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 4;

λ – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 4.

$$\text{Тобто } T_{\text{очік}} = 0,0008539 / 5400 = 1,58 * 10^{-7} \text{ (секунди)} \approx 0,0007 \text{ мілісекунд}$$

Було розраховано пропускну здатність каналу в локальній мережі LAN 4, для цього було застосовано формулу 2.10.

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

де λ – інтенсивність вихідного трафіку для всіх вузлів у локальній мережі LAN 4;

l – середня довжина вихідного повідомлення в локальній мережі LAN 4.

Тобто $b = 5400 * 5200 = 28080000$ біт/с ≈ 28.08 Мбіт/с.

В результаті проведення розрахунків було з'ясовано що усі значення розрахованих показників задовільняють технічним вимогам.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ РЕГІОНАЛЬНОГО ОФІСУ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ

3.1 Розрахунок схеми адресації корпоративної мереж

Згідно з завданням, у мережах LAN1-LAN3 для зв'язку між маршрутизаторами було використано блок адрес 10.25.80.0/22, що зображено на таблиці 3.1.

Таблиця 3.1 – Схема адресації мережі

Блок адрес	LAN 1 Голова організації + адміністрація	LAN 2 Бухгалтерія та фінансові менеджери	LAN 3 Технічний відділ	LAN 4 Спільний робочий простіі
10.23.20.0/22	9	13	6	50

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 9 візулів, необхідна маска підмережі /24, доступні адреси 10.23.20.1-10.23.20.254, широкомовлення за адресою 10.23.20.255. Для мережі LAN2, в яку входить 13 вузла, необхідна маска підмережі /26, доступні адреси 10.23.21.01 - 10.23.21.62, широкомовлення за адресою 10.23.21.63. Для мережі LAN3, в яку входить 6 вузла, необхідна маска підмережі /26, доступні адреси 10.23.21.65 - 10.23.21.126, широкомовлення за адресою 10.23.21.127. Для мережі LAN4, в яку входить 6 вузла, необхідна маска підмережі /26, доступні адреси 10.23.21.129 - 10.23.21.190, широкомовлення за адресою 10.23.21.191. 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	LAN4	254/50	10.23.20.0	/24	10.23.20.1	10.23.20.254

Найменша	LAN3	62/6	10.23.21.0	/26	10.23.21.1	10.23.21.62
	LAN2	62/13	10.23.21.64	/26	10.23.21.65	10.23.21.126
	LAN1	62/9	10.23.21.128	/26	10.23.21.129	10.23.21.190

Згідно з завданням, для зв'язку між маршрутизаторами нами було використано блок адрес 10.1.10.0 /24. В 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
LAN4	254/50	10.23.20.0	/24	10.23.20.254	10.25.80.254
LAN3	62/6	10.23.21.0	/26	10.23.21.1	10.23.21.62
LAN2	62/13	10.23.21.64	/26	10.23.21.65	10.23.21.126
LAN1	62/9	10.23.21.128	/26	10.23.21.129	10.23.21.190
ISP 1	2/2	209.165.202.0	/30	209.165.202.1	209.165.202.2

Серверам було привласнено IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+9. Адресація серверів зображена на таблиці 3.4

Таблиця 3.4 – Адресація інтерфейсів серверів

Назва серверу	Назва інтерфейсу	IP-адреса	Маска	Шлюз
Radius Server	Fa0	10.23.21.9	26	10.23.21.1
Server DNS	Fa0	10.23.21.10	26	10.23.21.1

3.2 Розробка топологічної схеми корпоративної мережі

У програмі Cisco Packet Tracer була розроблена топологічна схема, що складається із 4 підмереж, а саме з голови та адміністрації, бухгалтерії та фінансових менеджерів, технічного відділу і загального робочого простору. Загальну архітектуру мережі зображено на рисунку 3.1.

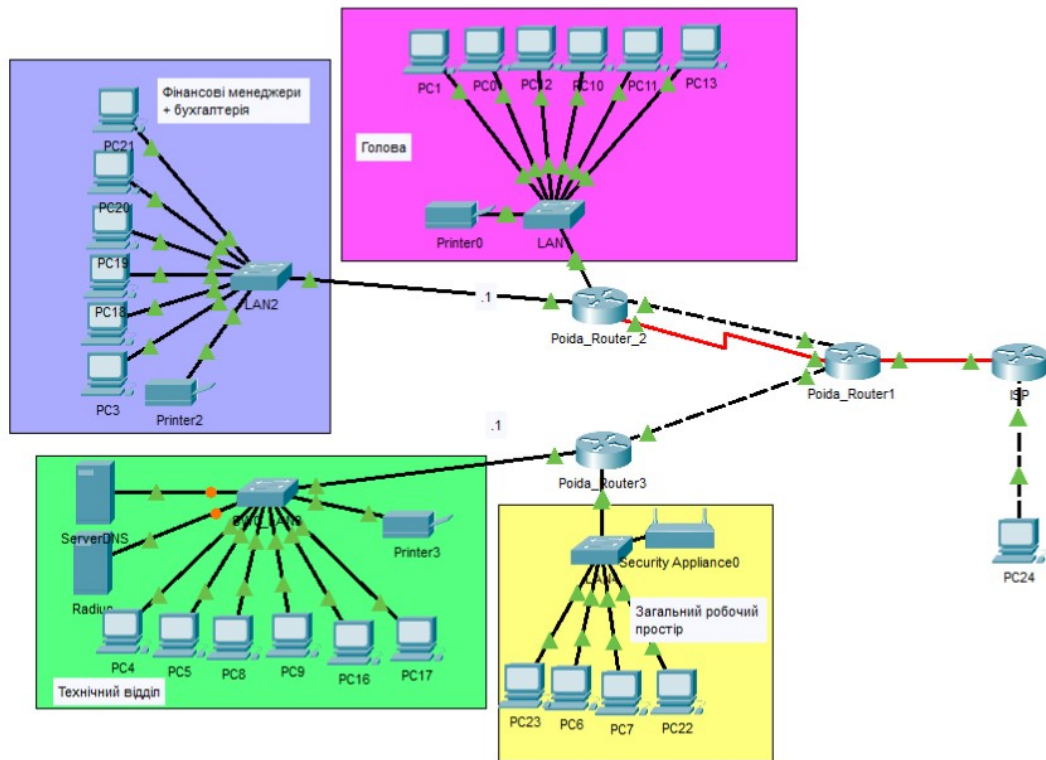


Рисунок 3.1 – Топологія мережі

3.3 Налаштування мережі

3.3.1 Базове налаштування

На початку роюоти необхідно виконати базове налаштування пристроїв. Згідно рекомендацій порядок дій:

- назначити назви пристроям за наступним правилом:

Прізвище студента_тип пристрою_номер пристрою, наприклад, Poida_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 12321_Poida, 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 Poida_Router_2.

Призначимо назву за правилом Poida_Пристрій_Номер.

```
Poida_Router_2(config)#hostname Poida_Router_2
```

Призначимо пароль cisco до консолі і vty.

```
Poida_Router_2(config)#line console 0
```

```
Poida_Router_2(config-line)#password cisco
```

```
Poida_Router_2(config-line)#login
```

```
Poida_Router_2(config-line)#exit
```

```
Poida_Router_2(config)#line vty 0 15
```

```
Poida_Router_2(config-line)#password cisco
```

```
Poida_Router_2(config-line)#login
```

```
Poida_Router_2(config-line)#
```

Призначимо пароль class до привілейованого режиму

```
Poida_Router_2(config)#enable secret class
```

Паролі, що зберігаються у відкритому вигляді зашифруємо.

```
Poida_Router_2(config)#service password-encryption
```

Розробимо банер MOTD.

```
Poida_Router_2(config)#banner motd "Welcome to Poida_Router_2"
```

Призначимо на усіх лініях vty використання протоколу ssh.

```
Poida_Router_2(config)#line vty 0 15
```

```
Poida_Router_2(config-line)#transport input ssh
```

Призначимо на всіх пристроях користувача за правилом: 12321_Poida з паролем adminisco.

```
Poida_Router_2(config)#username 12321_Poida privilege 15 secret adminisco
```

В якості імені домена використаємо ім'я пристрою.

```
Poida_Router_2(config)#ip domain name Poida_Router_2
```

Для шифрування даних створимо ключ RSA завдовжки 1024 біт.

```
Poida_Router_2(config)#crypto key generate rsa
```

```
The name for the keys will be: Poida_Router_2. Poida_Router_2
```

```
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.

```
Poida_Router_2(config-if)#clock rate 128000
```

Після налаштування збережемо конфігурацію пристрою.

```
Poida_Router_2#copy running-config startup-config
```

3.3.2 Налаштування маршрутизації корпоративної мережі

У мережевих системах розрізняють два основних типи маршрутизації: статичну та динамічну. Статична маршрутизація полягає у ручному внесенні маршрутів адміністратором, що дозволяє повністю контролювати маршрутизацію та спрощує налаштування, проте такий підхід не забезпечує гнучкості й погано підходить для масштабованих мереж, оскільки не реагує на зміни топології. Динамічна маршрутизація, навпаки, базується на використанні спеціалізованих протоколів (наприклад, RIP, OSPF, BGP), які автоматично

визначають оптимальні маршрути, що підвищує адаптивність і дозволяє ефективно масштабувати мережу. Водночас, динамічна маршрутизація вимагає глибших знань для налаштування та споживає більше ресурсів через постійний обмін маршрутною інформацією. У цьому проєкті для забезпечення масштабованості обрано динамічну маршрутизацію із застосуванням протоколу OSPF.

Переваги протоколу OSPF є:

- Висока швидкість збіжності;
- Відсутність петель маршрутизації;
- Динамічна адаптація;
- 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:

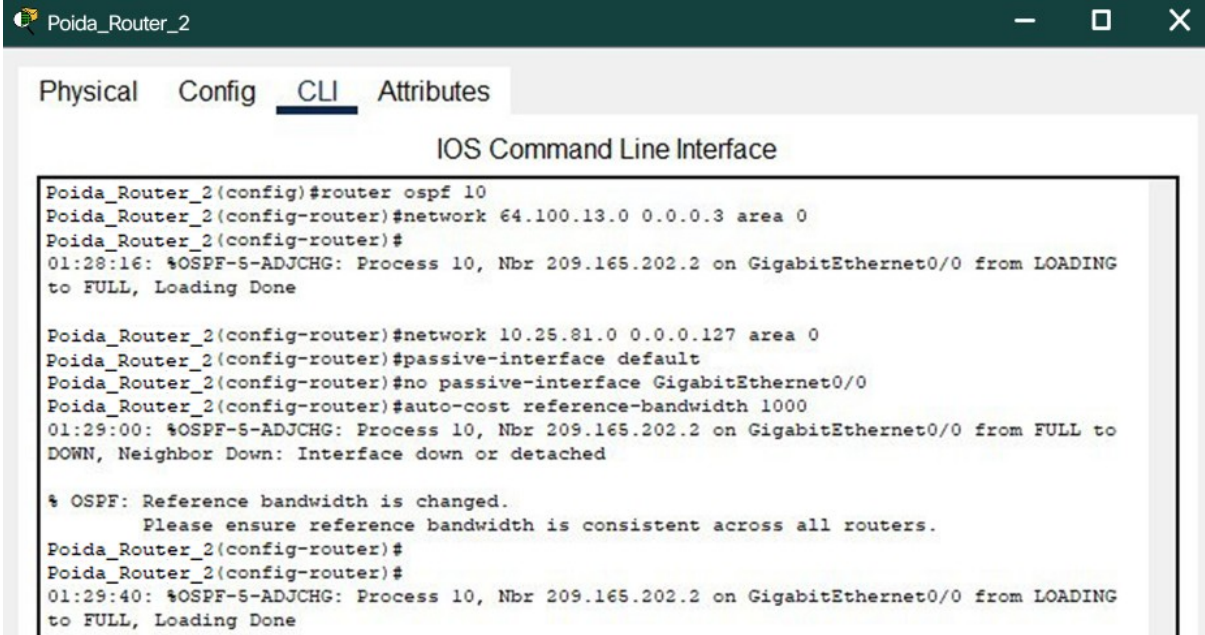
```
Poida_Router_2(config)#interface назва_інтерфейсу
```

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

```
Poida_Router_2(config-if)#ip address IP-адреса маска_підмережі.
```

Після цього можна приступати до налаштування інтерфейсу OSPF.

Приклад налаштування OSPF на роутері Poida_Router_5 зображено на рисунку 3.2.



```
Poida_Router_2
Physical Config CLI Attributes
IOS Command Line Interface
Poida_Router_2(config)#router ospf 10
Poida_Router_2(config-router)#network 64.100.13.0 0.0.0.3 area 0
Poida_Router_2(config-router)#
01:28:16: %OSPF-5-ADJCHG: Process 10, Nbr 209.165.202.2 on GigabitEthernet0/0 from LOADING
to FULL, Loading Done
Poida_Router_2(config-router)#network 10.25.81.0 0.0.0.127 area 0
Poida_Router_2(config-router)#passive-interface default
Poida_Router_2(config-router)#no passive-interface GigabitEthernet0/0
Poida_Router_2(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.
Poida_Router_2(config-router)#
Poida_Router_2(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 3.2 – 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 VTU 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 DHCP, що дозволяє зменшити витрати на технічне обладнання та спростити роботу системного адміністратора. Виконане налаштування Radius сервера зображено на рисунку 3.3.

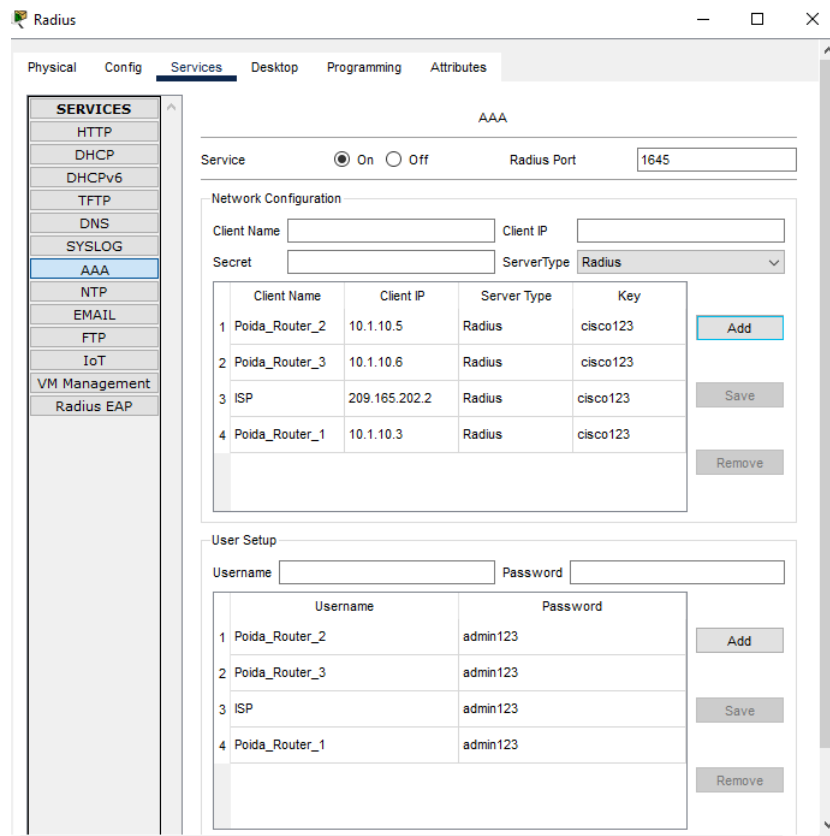


Рисунок 3.3 – Виконані налаштування Radius сервера

3.3.3 Налаштування NAT

Наступним кроком конфігурації мережі є впровадження стандарту NAT (Network Address Translation, трансляція мережевих адрес). Основна мета NAT – надати можливість декільком пристроям використовувати одну публічну IP-адресу для виходу в Інтернет. Для цього необхідно виконати перетворення приватних IP-адрес у 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.

Налаштовано NAT, що зображено на рисунку 3.4.

```
Physical  Config  CLI  Attributes
IOS Command Line Interface
Poida_Router_2#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 3.4 – Результат перевірки роботи NAT

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.

3.3.4 Налаштування VPN

VPN (віртуальна приватна мережа) – це віртуальна приватна мережа, яка забезпечує шифрування даних, що передаються між користувачем і VPN-сервером, а також змінює IP-адресу пристрою. Під час підключення створюється захищений тунель між комп'ютером користувача та сервером VPN. У рамках цього проєкту, відповідно до завдання, було налаштовано site-to-site VPN із застосуванням протоколу IPsec для забезпечення безпечного обміну трафіком між мережами LAN3 та LAN.

Першим етапом конфігурації є створення списку доступу, що дозволяє передачу даних із підмережі організації. Далі налаштовується криптографічна політика, яка визначає метод автентифікації та алгоритми шифрування. Важливо, щоб параметри шифрування та криптографічна група співпадали на обох маршрутизаторах, що формують VPN-з'єднання. Наступним кроком є створення VPN-мапи, у якій вказується раніше створений список доступу. Після цього криптографічна мапа та Peer роутер прив'язуються до інтерфейсу Інтернету. Приклад налаштування третього маршрутизатора наведено на рисунку 3.5.

```

Poida_Router_2 (config)#ip access-list extended VPN
Poida_Router_2 (config-ext-nacl)#permit ip 10.25.81.128 0.0.0.63 10.25.81.0 0.0.0.127
Poida_Router_2 (config-ext-nacl)#permit ip 10.25.80.0 0.0.0.255 10.25.81.0 0.0.0.127
Poida_Router_2 (config-ext-nacl)#exit
Poida_Router_2 (config)#crypto isakmp policy 10
Poida_Router_2 (config-isakmp)#encryption aes
Poida_Router_2 (config-isakmp)#authentication pre-share
Poida_Router_2 (config-isakmp)#group 2
Poida_Router_2 (config-isakmp)#crypto isakmp key malov address 64.100.13.2
Poida_Router_2 (config)#crypto ipsec transform-set MAX esp-aes esp-sha-hmac
Poida_Router_2 (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.
Poida_Router_2 (config-crypto-map)#description VPN connection to R5
Poida_Router_2 (config-crypto-map)#set peer 64.100.13.2
Poida_Router_2 (config-crypto-map)#set transform-set MAX
Poida_Router_2 (config-crypto-map)#match address VPN1
Poida_Router_2 (config-crypto-map)#interface Serial0/3/1
Poida_Router_2 (config-if)#crypto map MAP
  
```

Рисунок 3.5 – Налаштування VPN

3.3.5 Налаштування VLAN

VLAN (Virtual Local Area Network) – це технологія, яка дозволяє створювати віртуальні локальні мережі всередині однієї фізичної інфраструктури. Вона забезпечує логічне групування мережевих пристроїв у сегменти незалежно від їхнього фізичного розташування. Основна мета VLAN полягає у підвищенні продуктивності мережі, посиленні безпеки та спрощенні її адміністрування.

Основні аспекти VLAN:

- Сегментація мережі: VLAN дозволяють логічно розділити одну фізичну мережу на кілька окремих сегментів, що зменшує обсяг широкомовного трафіку в кожному сегменті та підвищує загальну продуктивність мережі.
- Підвищення безпеки: Завдяки VLAN можна ізолювати різні групи користувачів, наприклад, відокремити співробітників фінансового відділу від решти мережі, що знижує ризик несанкціонованого доступу до конфіденційної інформації.
- Гнучкість і масштабованість: VLAN спрощують адміністрування мережі, дозволяючи швидко змінювати конфігурацію без необхідності фізично перепідключати пристрої, що особливо корисно у динамічних середовищах.
- Ефективне управління трафіком: VLAN дають змогу контролювати та пріоритизувати мережевий трафік, забезпечуючи оптимальну якість обслуговування для критичних додатків.

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 3.6 та 3.7.

IP Configuration

DHCP

Static

IPv4 Address 10.23.20.16

Subnet Mask 255.255.255.192

Рисунок 3.6 – Перевірка отримання вузлом адреси через DHCP

Gateway/DNS IPv4

DHCP

Static

Default Gateway 10.23.21.3

DNS Server 10.23.21.10

Рисунок 3.7 – Перевірка отримання вузлом Gateway/DNS через DHCP

3.4 Перевірка роботи комп'ютерної системи

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 3.10.

PDU List Window

Fire	Time(sec)	Last Status	Source	Destination	Type	Color	Num	Periodic	Edit	Delete
	0.000	Successful	Poida_Router1	Poida_Router2	ICMP		0	N	(edit)	
	0.000	Successful	Poida_Router1	Poida_ISP	ICMP		1	N	(edit)	
	0.000	Successful	Poida_Router2	Poida_ISP	ICMP		2	N	(edit)	
	0.000	Successful	PC1	PC6	ICMP		3	N	(edit)	
	0.000	Successful	PC1	PC4	ICMP		4	N	(edit)	
	0.000	Successful	PC1	PC3	ICMP		5	N	(edit)	

Рисунок 3.8 – Результат перевірки OSPF, NAT та маршрутизації

Для перевірки DHCP необхідно перевірити IP конфігурації на ПК у різних підмережах, це зображено на рисунках 3.9-3.12.

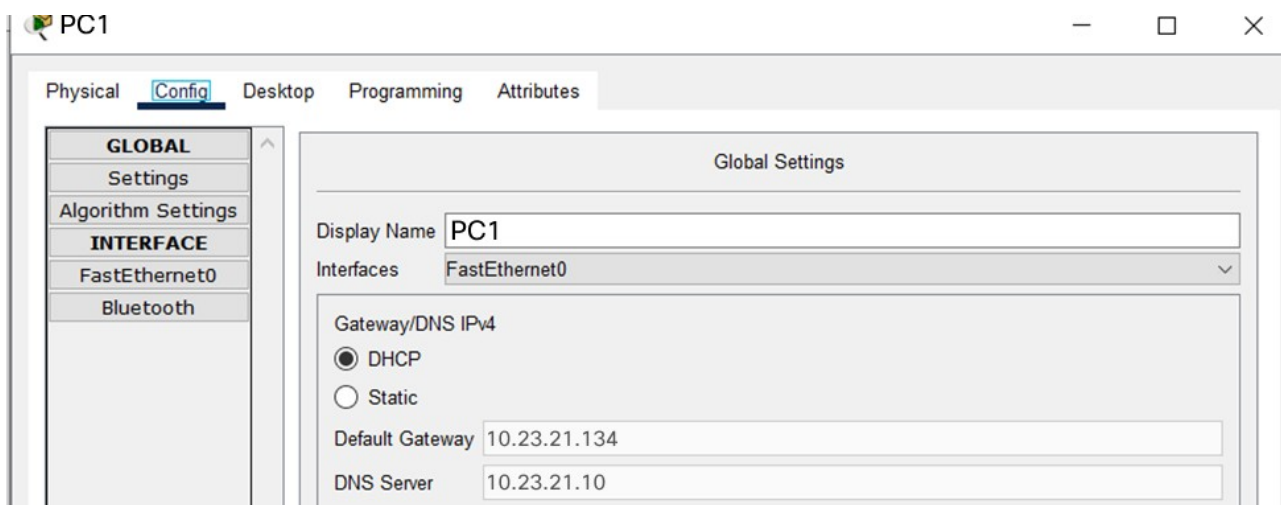


Рисунок 3.9 – Перевірка DHCP на LAN1

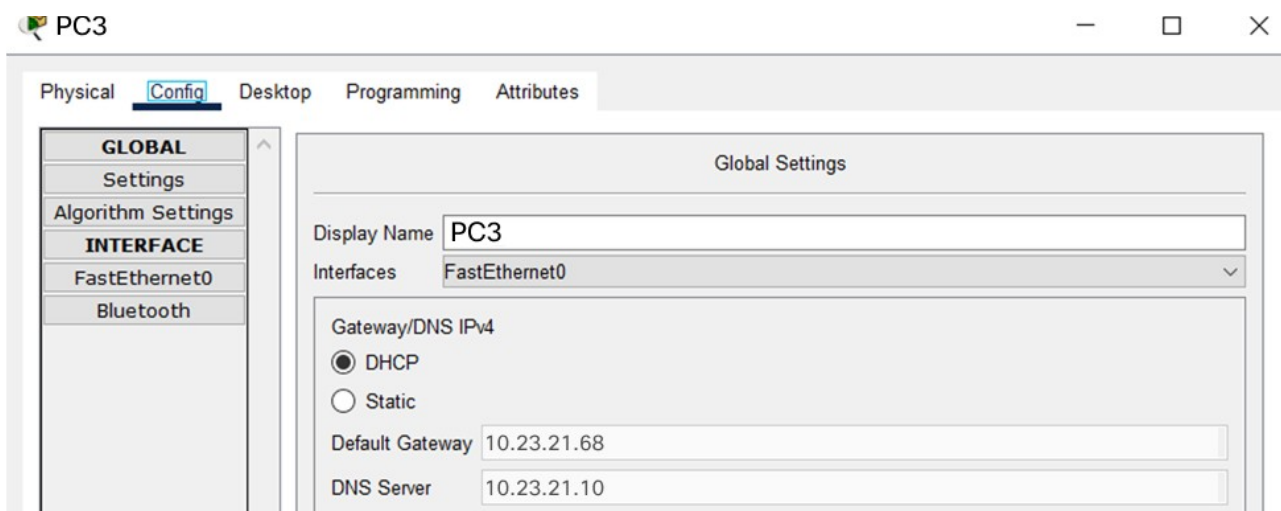


Рисунок 3.10 – Перевірка DHCP на LAN2

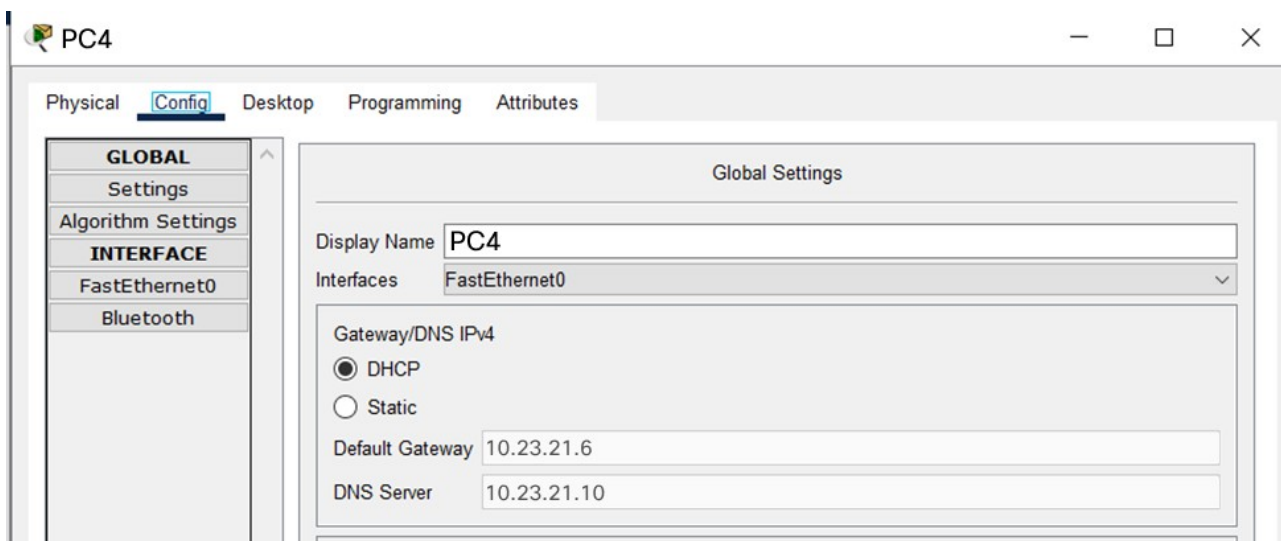


Рисунок 3.11 – Перевірка DHCP на LAN3

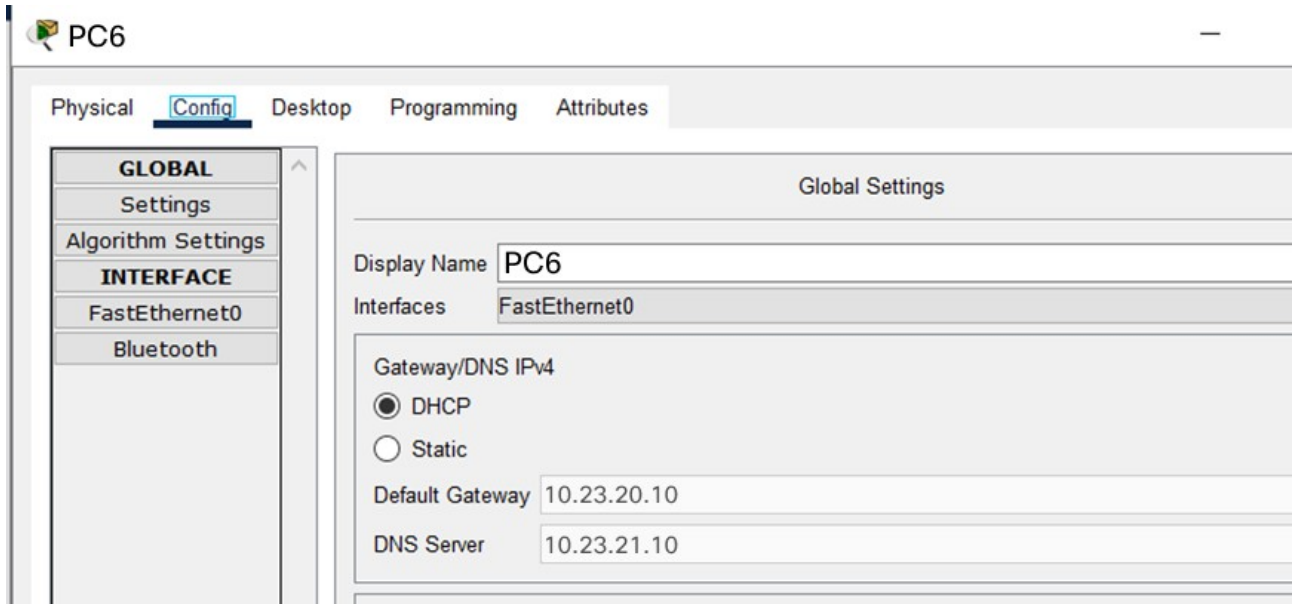


Рисунок 3.12 – Перевірка DHCP на LAN3

Для перевірки статичного NAT для серверів DNS та HTTP необхідно перейти за адресою 123.dnipro.ua, результат зображений на рисунку 3.13.

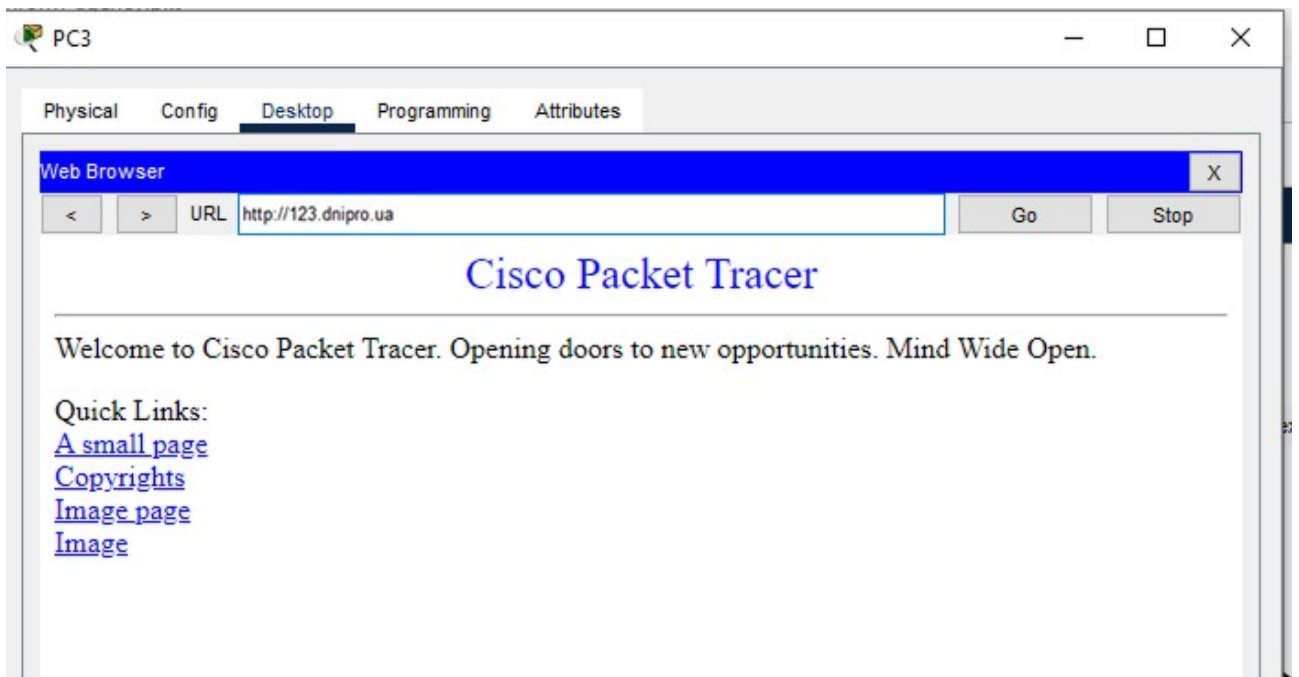


Рисунок 3.13 – Перевірка статичного NAT

Для перевірки роботи VPN була використана команда:
show crypto isakmp sa,

що відображає параметри обміну ключами Інтернету (IKE), результат цієї команди зображено на рисунку 3.14.

```

Poida_Router_2
Physical Config CLI Attributes
IOS Command Line Interface
Poida_Router_2(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 3.14 – Перевірка роботи VPN

Також було перевірено роботу VLAN, за допомогою команди `show vlan brief`, що зображено на рисунку 3.15.

```

LAN_1
Physical Config CLI Attributes
IOS Command Line Interface
Poida_Switch#
Poida_Switch#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 3.15 – Перевірка VLAN

ВИСНОВКИ

Законодавчі ініціативи останніх років спрямовані на розширення можливостей ГО, спрощення процедур їхньої діяльності та посилення їхнього впливу на місцеве самоврядування, що підвищує ефективність громадянського суспільства і сприяє сталому розвитку країни.

Отже, громадські організації є важливим інструментом розвитку демократії, соціальної справедливості та відновлення України, вони зміцнюють зв'язок між державою і суспільством, підвищують якість життя громадян і сприяють побудові відкритого, відповідального суспільства.

У ході виконання дипломної роботи було досягнуто основної мети – створення комп'ютерної системи для регіонального офісу громадської організації. Виконання цього завдання включало кілька ключових етапів, результатом яких стала розробка комп'ютерної мережі, що забезпечує ефективну діяльність організації.

Було створено комп'ютерну мережу для регіонального офісу ГО, яка забезпечує надійну взаємодію між її учасниками. Мережа складається з серверів, комутаторів, маршрутизаторів та персональних комп'ютерів, що дає змогу адміністраторам та співробітникам організації ефективно управляти робочими процесами. Високі показники пропускної здатності та надійності мережевого обладнання гарантують стабільну роботу системи й швидку передачу даних між усіма її компонентами.

Завдяки впровадженню рішень компанії Cisco було забезпечено високу якість і безпеку мережі, що є критично важливим для безперервного та захищеного функціонування офісу. Це передбачає інтеграцію систем захисту від кіберзагроз та можливість масштабування мережі в майбутньому, що дозволяє адаптувати інфраструктуру до зростання кількості користувачів і розширення організації.

Таким чином, кваліфікаційна робота успішно досягла поставленої мети і підтвердила ефективність розроблених технічних рішень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Науменко Т. Що таке громадська організація і навіщо вона потрібна? Київ – 2018. [Електронний ресурс] – Режим доступу до ресурсу: https://kubg.edu.ua/images/stories/Departaments/astreya/mk/05_gromadska_organizaciia2018.pdf
2. Закон України «Про громадські об'єднання» [Електронний ресурс]. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/4572-17>.
3. Ліпінська А. В. Інформаційно-комунікаційні технології в організації інформаційно-аналітичного забезпечення державного управління. Державне управління: удосконалення та розвиток № 10, 2015.
4. CRM система для громадських організацій – на що звернути увагу? [Електронний ресурс] – Режим доступу до ресурсу: <https://evolpe.com.ua/%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-crm-%D0%B4%D0%BB%D1%8F-%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9-%D0%BD%D0%B5%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B8%D1%85/>
5. Порядок використання комп'ютерних програм в органах виконавчої влади. постановою Кабінету Міністрів України N 1433. [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1433-2003-%D0%BF#Text>
6. БУР. ГО. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.bur.org.ua/>
7. Свистуха Д. Для доброї справи. Добірка сервісів із безплатним доступом чи знижками для громадських організацій. 2024. [Електронний ресурс] – Режим доступу до ресурсу: <https://mediamaker.me/dlya-dobroyi-spravy-dobirka-servisiv-iz-bezplatnym-dostupom-chy-znyzhkami-dlya-gromadskyyh-organizacij-9831/>
8. Ситніков Д. С. Інформаційні системи підтримки діяльності громадських організацій в Україні. Вінниця – 2021. [Електронний ресурс] – Режим доступу до ресурсу: <https://jarch.donnu.edu.ua/article/view/10516/10425>
9. Клапків А. І. Вдосконалення механізму інформаційного забезпечення органу місцевого самоврядування. Тернопіль – 2020. [Електронний ресурс] – Режим доступу до ресурсу: <https://dspace.wunu.edu.ua/jspui/bitstream/316497/38322/1/%D0%9A%D0>

[%BB%D0%B0%D0%BF%D0%BAi%D0%B2_%D0%90.I._%D0%9F%D0%A3%D0%90-41.pdf](#)

10. Ситник Г.П., Загорітня Г.П., Марутян Р.Р. Інформаційно-комунікаційні технології у сфері національної безпеки: навчальний посібник / за заг. ред. Г.П. Ситника ; ТОВ «Академпрес». – Київ, 2024. – 176 с
11. Савісько М., Гацко В. Проектний підхід в громадах. Рекомендації для керівництва громади та працівників проектних відділів. KSE. 2023. [Електронний ресурс] – Режим доступу до ресурсу: <https://kse.ua/wp-content/uploads/2023/09/Rekomendatsii---dlya-gromad.-Proyektanii---pidhid.pdf>
12. Розробка комплексних планів. Посібник для громад, а результатами пілотного Проекту USAID «Впровадження вимог Закону України №711-IX від 17.06.20. «Про внесення змін до деяких законодавчих актів України щодо планування використання земель»» 2022. [Електронний ресурс] – Режим доступу до ресурсу: https://decentralization.ua/uploads/library/file/817/%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA_%D0%B4%D0%B%D1%8F_%D0%B3%D1%80%D0%BE%D0%BC%D0%B0%D0%B4.pdf
13. Планування розвитку територіальних громад. Навчальний посібник для посадових осіб місцевого самоврядування / Г. Васильченко, І. Парасюк, Н. Єременко / Асоціація міст України – К., ТОВ «ПІДПРИЄМСТВО «ВІ ЕН ЕЙ», 2015. – 256 с.
14. Каштан В.Ю. Комп'ютерні мережі (частина 1): навч. наоч. посіб. / В.Ю. Каштан, М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Електрон. дані. – Дніпро : НТУ «ДП», 2023. – Ч.1.– 371 с.
15. Комп'ютерні мережі. Курс лекцій. [Електронний ресурс] – Режим доступу до ресурсу: <https://e-tk.lntu.edu.ua/>