Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі центрального офісу УДМС у Тернопільській області**

Виконав: студент VII курсу, групи КІб-703

Спеціальності **123 Комп'ютерна інженерія**
(шифр і назва спеціальності)

_____ Антон БЕЗКОРОВАЙНИЙ
(ім'я та прізвище)

Керівник _____ Андрій ЛЯПАНДРА
(ім'я та прізвище)

Рецензент _____ _____
(ім'я та прізвище)

Тернопіль – 2026

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення **телекомунікацій та електронних систем**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"18" травня 2026 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Безкоровайному Антону Павловичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі центрального офісу УДМС у Тернопільській області**

керівник роботи Ляпандра Андрій Степанович
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 18.05.2026р № 4/9-252

2. Строк подання студентом роботи: 22 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - "Commercial Building Telecommunications Wiring Standart" і ANSI/EIA/TIA 569 - "Commercial Building Standart for Telecommunications Pathwais and Spaces

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Охорона праці та безпека життєдіяльності.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- модель мережі
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Ірина ЛЕЩИК методист, викладач		
Безпека життєдіяльності. основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	18.05	
2	Збір і узагальнення інформації	21.05	
3	Написання першого розділу	25.05	
4	Розробка технічного та робочого проекту	1.06	
5	Написання спеціального розділу	8.06	
6	Розрахунок економічної частини	11.06	
7	Написання розділу охорони праці	12.06	
8	Виконання графічної частини	14.06	
9	Оформлення проекту	18.06	
10	Погодження нормоконтролю	19.06	
11	Попередній захист роботи	22.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 18 травня 2026 року

Студент _____ Антон БЕЗКОРОВАЙНИЙ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Андрій ЛЯПАНДРА
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Безкоровайний А.П. Розробка проекту комп'ютерної мережі УДМС у Тернопільській області: кваліфікаційна робота на здобуття освітнього ступеня бакалавр за спеціальністю «123 – Комп'ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2026. 103 с.

Кваліфікаційна робота передбачає розробку проекту комп'ютерної мережі УДМС у Тернопільській області згідно стандартів та вимог замовника. В проектованій мережі використано сучасні стандарти Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac та Ethernet IEEE 802.3q. При цьому реалізовано розподіл мережі на віртуальні підмережі, планування та розподіл адресного простору. Розроблено інструкції з інсталяції та налаштування сервера, VPN-шлюзу, шлюзу доступу до мережі Інтернет, віртуальних підмереж та засобів захисту мережі. Створень віртуальну модель мережі в програмі Cisco Packet Tracer.

Ключові слова: комп'ютерна мережа, сервер, точка доступу, VPN, маршрутизатор, комутатор, віртуальна мережа, VLAN, Cisco Packet Tracer

ANNOTATION

Bezkorovainyi A.P. Development of a computer network project for the UDMS in the Ternopil region: qualification work for obtaining a bachelor's degree in the specialty "123 - Computer Engineering". Ternopil: VSP "TFK TNTU", 2026. 103 p.

The qualification work involves the development of a computer network project for Department of the State Customs Service in Ternopil region according to the standards and requirements of the customer. The designed network uses modern Gigabit Ethernet IEEE 802.3ab, IEEE 802.11ac and Ethernet IEEE 802.3q standards. At the same time, the network is divided into virtual subnetworks, planning and allocation of address space are implemented. Instructions for installing and configuring a server, VPN gateway, Internet access gateway, virtual subnets and network security tools have been developed. A virtual network model was created in the Cisco Packet Tracer program.

Keywords: computer network, server, access point, VPN, router, switch, virtual network, VLAN, Cisco Packet Tracer.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DNS (Domain Name System) – сервер доменних імен.

FTP (File Transfer Protocol) – протокол передачі файлів.

HTTP (Hypertext Transfer Protocol) – протокол передачі гіпертексту.

IDS (Intrusion Detection System) – пасивна система моніторингу мережі, що аналізує трафік і сповіщає про загрози

IEEE 802.3ab – стандарт Gigabit Ethernet на витій парі UTP 5e, 6.

IEEE 802.3z – стандарт Gigabit Ethernet на оптоволоконному кабелі.

IEEE 802.3ac – стандарт, що пребачає збільшення максимального розміру фрейму до 1522 байт, яке дозволяє зберігати інформації про VLAN стандарту IEEE 802.1Q та пріоритету стандарту IEEE 802.1p.

IP (Internet Protocol) – Інтернет-протокол.

IPS (Intrusion Prevention System) – активна система моніторингу мережі, що аналізує трафік і сповіщає про загрози.

IPSec (Internet Protocol Security) – це набір протоколів, які забезпечують безпеку даних, що передаються по IP-мережах.

LAN (Local Area Network) – локальна мережа.

MAC (Media Access Control) - апаратна адреса ПК.

NAT (Network Address Translation) –технологія в мережах TCP/IP, яка дозволяє маршрутизатору змінювати IP-адреси в заголовках пакетів

OU (Organization Unit) – організаційна одиниця групових політик безпеки.

SNMP (Simple Network Management Protocol) – простий протокол мережевого управління. Протокол мережевого адміністрування.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол;

VPN (Virtual Private Network) – узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри

ОС – операційна система.

ВСТУП

В умовах стрімкої цифровізації державних послуг та розвитку інфраструктури електронного урядування в Україні, критично важливим стає забезпечення високого рівня надійності, безперебійності та кібербезпеки інформаційно-телекомунікаційних систем. Особливої уваги в цьому контексті потребують державні установи, діяльність яких пов'язана з обробкою та зберіганням значних масивів персональних і біометричних даних громадян. До таких структур належить Державна міграційна служба (ДМС) України.

Управління ДМС у Тернопільській області щоденно забезпечує роботу з Єдиним державним демографічним реєстром, обробку запитів на оформлення паспортних документів та функціонування систем відеоспостереження. Це вимагає наявності сучасної, надійної та масштабованої комп’ютерної мережі, здатної підтримувати інтенсивний та безпечний обмін даними. Застарілі мережеві рішення не здатні повною мірою протистояти сучасним кіберзагрозам та забезпечувати необхідну швидкість доступу до зовнішніх і внутрішніх інформаційних ресурсів. Саме тому проектування модернізованої локальної мережі з урахуванням новітніх стандартів інформаційної безпеки, відмовостійкості та економічної доцільності є актуальним науково-практичним завданням.

Метою дипломної роботи є розробка проекту сучасної комп’ютерної мережі для центрального офісу Управління ДМС у Тернопільській області, яка повною мірою відповідатиме актуальним вимогам щодо продуктивності, надійності, масштабованості та інформаційної безпеки, а також науково-технічне обґрунтування вибору оптимального апаратного та програмного забезпечення для її практичної реалізації.

.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Об’єктом розробки у даній кваліфікаційній роботі є модернізація локальної обчислювальної мережі (ЛОМ) Управління Державної міграційної служби України у Тернопільській області. Проект передбачає створення цілісної інформаційно-телекомунікаційної інфраструктури, яка виступає технічною основою для повсякденної діяльності підрозділів установи.

Область застосування проектованої мережі охоплює адміністративні та операційні процеси Управління, зокрема забезпечення стабільної роботи з Єдиним державним демографічним реєстром та автоматизованими системами оформлення біометричних документів. Розроблена мережа має стати середовищем для функціонування внутрішніх сервісів: захищеного електронного документообігу, систем IP-телефонії та інтелектуального відеоспостереження. Впровадження системи орієнтоване на використання співробітниками територіального органу ДМС для підвищення швидкості та безпеки надання державних послуг громадянам, а також для організації захищеної взаємодії з іншими державними інформаційними ресурсами в умовах високої інтенсивності обміну даними.

Система розрахована на інтенсивну експлуатацію різними категоріями користувачів: державними службовцями, які забезпечують роботу з Єдиним державним демографічним реєстром та надають послуги громадянам, спеціалістами з безпеки, відповідальними за моніторинг та захист даних, а також системними адміністраторами, які здійснюють технічний супровід інфраструктури. Крім того, архітектура мережі передбачає створення окремих захищених сегментів для надання контрольованого доступу до інформаційних ресурсів відвідувачам установи.

З огляду на специфіку роботи державного органу та необхідність постійного функціонування систем відеоспостереження й критичних баз даних, мережа розрахована на безперебійний цілодобовий режим експлуатації (24/7). Впровадження системи орієнтоване на підвищення швидкості та безпеки надання державних послуг, забезпечуючи високу доступність сервісів та захищену взаємодію з державними реєстрами в умовах постійного навантаження.

1.1.2 Призначення розробки

Основним призначенням розробки є створення сучасної, високотехнологічної інформаційної інфраструктури для Управління ДМС у Тернопільській області, що забезпечить ефективну автоматизацію службової діяльності та надання адміністративних послуг.

Функціональне призначення системи полягає у:

- забезпеченні надійного каналу зв’язку для роботи з державними реєстрами та базами даних персональної інформації;
- організації спільного доступу до мережевих ресурсів, периферійного обладнання та систем електронного документообігу;
- створенні середовища для функціонування систем безпеки, включаючи IP-відеоспостереження та контроль доступу;
- наданні сегментованого доступу до мережі Інтернет для співробітників та відвідувачів установи із дотриманням політик безпеки.

Експлуатаційне призначення проекту спрямоване на досягнення таких цілей:

- мінімізація затримок при передачі великих обсягів даних (наприклад, цифрових фото та біометричних параметрів);
- захист внутрішнього трафіку від несанкціонованого доступу та мережевих атак;
- забезпечення безперервної роботи критичних сервісів у режимі 24/7;

- можливість розширення мережі та впровадження нових технологій без повної заміни існуючої архітектури;

- програмне забезпечення має підтримувати стандартизовані інтерфейси взаємодії (API) для безперешкодного обміну даними між внутрішніми системами ДМС та зовнішніми державними реєстрами

1.1.3 Вимоги до апаратного і програмного забезпечення

Вимоги до технічних та програмних засобів сформовані з урахуванням необхідності створення відмовостійкої інфраструктури, здатної забезпечити стабільну роботу специфічних державних сервісів та захист персональних даних.

Апаратне забезпечення мережі має базуватися на сучасному телекомунікаційному обладнанні корпоративного класу. Основні вимоги включають:

- використання керованих комутаторів другого та третього рівнів (L2/L3) із підтримкою технології PoE (Power over Ethernet) для живлення IP-телефонів та камер відеоспостереження. Пропускна здатність магістральних каналів повинна становити не менше 10 Гбіт/с, а клієнтських підключень – 1 Гбіт/с;

- апаратні засоби повинні підтримувати роботу з існуючою кабельною інфраструктурою та периферійними пристроями попередніх поколінь, що вже експлуатуються в Управлінні;

- використання відкритих міжнародних стандартів та протоколів (таких як TCP/IP, IEEE\802.1Q для VLAN, SNMP для моніторингу), що дозволяє об’єднувати обладнання різних виробників у єдину екосистему;

- у серверній інфраструктурі – використання серверів із надлишковими блоками живлення та RAID-масивами для забезпечення збереження даних;

- обов'язкова наявність джерел безперебійного живлення (ДБЖ) з можливістю автономної роботи критичних вузлів мережі протягом не менше 30 хвилин;

- периферійне обладнання повинно підтримувати сучасні засоби біометричного зчитування та спеціалізованих принтерів для друку документів;

Програмне забезпечення має бути ліцензійним та мати відповідні сертифікати (або експертні висновки) у сфері захисту інформації. До складу програмного забезпечення повинні входити:

- серверні операційні системи з підтримкою доменної архітектури (наприклад, Windows Server) для централізованого керування користувачами та політиками безпеки;

- спеціалізовані антивірусні пакети, програмні брандмауери та системи виявлення вторгнень (IDS/IPS);

- клієнтські додатки для доступу до ЄДДР, системи криптографічного захисту каналів зв'язку (VPN) та програмні комплекси для керування архівом відеоспостереження.

1.1.4 Вимоги до документації

Процес розробки та впровадження комп’ютерної мережі Управління ДМС у Тернопільській області має супроводжуватися оформленням повного пакету технічної документації. Документація повинна бути складена державною мовою та надана як у паперовому, так і в електронному вигляді.

До складу обов'язкового пакету документів входять:

- пояснювальна записка з обґрунтуванням технічних рішень, специфікація обладнання та програмного забезпечення, а також розрахунок вартості реалізації проекту;

- структурні та логічні схеми мережі, плани розміщення обладнання та прокладання кабельних трас у приміщеннях Управління;

- інструкції для системних адміністраторів щодо налаштування та підтримки мережі, а також короткі посібники для користувачів стосовно роботи з мережевими ресурсами;

- регламенти доступу до інформаційних ресурсів, опис налаштувань засобів захисту інформації та копії сертифікатів відповідності на програмне та апаратне забезпечення;

- протоколи випробувань, акти приймання-передачі виконаних робіт та результати тестування мережі на відповідність вимогам продуктивності та надійності.

1.1.5 Техніко-економічні показники

Розробка та впровадження проекту модернізації мережі спрямовані на досягнення оптимального співвідношення між витратами на розгортання системи та її функціональною ефективністю. Основними показниками, що визначають доцільність проекту, є:

- основний провідний сегмент мережі базується на стандарті Gigabit Ethernet (IEEE 802.3ab). Для усунення затримок при пікових навантаженнях пропускна здатність магістральних каналів (Core/Uplink) становить не менше 10 Гбіт/с, тоді як підключення кінцевих користувачів забезпечується на швидкості 1 Гбіт/с;

- система розрахована на обслуговування 41 робочої станції. Як середовище передачі даних використовується кабель «вита пара» категорії 6 (Cat 6), що забезпечує необхідну смугу частот для підтримання гігабітних швидкостей;

- реалізація механізмів створення захищених шифрованих каналів (VPN) через мережу Інтернет, що дозволяє безпечно з'єднувати територіальні підрозділи та забезпечувати доступ до централізованих ресурсів ДМС;

- використання захищених шифрованих каналів з’єднання між окремим територіальними підрозділами та Управлінням ДМС в Тернопільській області через загальнодоступні ресурси Інтернет;

- загальна вартість проекту, що включає активне мережеве обладнання з підтримкою 10G та монтаж пасивної частини, не повинна перевищувати 700 тис. грн;

- використання сучасних компонентів та ієрархічної структури дозволить мінімізувати час простою державних сервісів, що прямо впливає на якість обслуговування громадян.

1.1.6 Стадії та етапи розробки

Процес проектування та впровадження комп'ютерної мережі Управління ДМС у Тернопільській області реалізується як комплексна послідовність етапів, спрямованих на створення відмовостійкої та захищеної інфраструктури. Кожна стадія передбачає виконання специфічних науково-практичних завдань.

Аналітико-передпроектна стадія полягає у проведені детального обстеження об'єкта, що включає аналіз архітектурних особливостей приміщень та оцінку існуючих технічних засобів. Основна увага приділяється формуванню вимог до підключення 41 робочої станції та визначенню точок концентрації трафіку для забезпечення максимальної ефективності топології.

На другому етапі технічного проектування розробляється архітектурне рішення мережі. Він включає проектування магістральних сегментів із пропускною здатністю 10 Гбіт/с та розрахунок структурованої кабельної системи на базі «витої пари» категорії 6. Важливим аспектом є розробка логічної структури (VLAN) та інтеграція засобів криптографічного захисту для організації VPN-каналів.

Етап ресурсного планування та підготовки передбачає складання остаточних специфікацій обладнання та програмного забезпечення. Вибір активних пристроїв (комутаторів, маршрутизаторів) здійснюється шляхом зіставлення їхніх технічних характеристик із бюджетом проекту [2].

Наступна стадія реалізації та налагодження включає фізичні роботи з монтажу кабельних трас, встановлення активного обладнання у серверних

вузлах та його програмну конфігурацію. На цьому етапі реалізуються політики безпеки, налаштовується пріоритезація трафіку та забезпечується стабільне гігабітне з'єднання для кінцевих користувачів.

Завершальний етап стадія контрольно-випробувальних робіт, під час якого проводиться комплексне тестування мережі на відповідність заявленим показникам швидкості та надійності. За результатами випробувань оформлюється повний пакет технічної документації та здійснюється введення системи в промислову експлуатацію [4].

Ще в одну окрему стадію можна віднести супровід. Незважаючи на те, що цей етап не входить в сам процес проектування та впровадження, він теж є важливим для забезпечення функціонування мережі.

1.1.7 Порядок контролю та прийому

Процедура контролю якості та офіційного приймання модернізованої мережі Управління ДМС у Тернопільській області являє собою комплексний процес верифікації, що гарантує відповідність системи вимогам безпеки та продуктивності.

Процес розпочинається з інструментальної перевірки пасивної частини мережі, де кожна з точок підключення піддається тестуванню на відповідність стандартам Gigabit Ethernet. Використання кабелю Cat 6 вимагає особливої уваги до параметрів затухання сигналу та цілісності екранування, що перевіряється за допомогою спеціалізованих мережевих аналізаторів.

Після підтвердження якості фізичного рівня контроль переходить до активного обладнання та логічної структури. На цій стадії комісія перевіряє стабільність магістральних каналів на швидкості 10 Гбіт/с, коректність маршрутизації між сегментами мережі (VLAN) та функціонування засобів захисту.

Окремим важливим етапом є випробування захищених VPN-каналів, під час яких імітуються різні умови навантаження та можливі розриви з'єднання для

перевірки стійкості шифрування та швидкості автоматичного відновлення зв’язку.

Завершальна фаза контролю полягає у проведенні приймально-здавальних випробувань під реальним навантаженням протягом 72 годин. Протягом цього часу ведеться моніторинг помилок у мережі та затримок пакетів. За результатами випробувань формується підсумковий протокол відповідності, який містить:

Особливе значення у процесі приймання мають протоколи результатів тестування. Ці документи є офіційним підтвердженням того, що кожен компонент системи відповідає заявленим технічним характеристикам [2].

Протоколи містять детальні звіти пропускної здатності, рівні затримок (latency) та відсоток втрати пакетів при пікових навантаженнях. Для кабельної системи протоколи включають «карти прозвонки» та графіки амплітудно-частотних характеристик кожної лінії.

Лише на основі цих об’єктивних даних, за умови відсутності відхилень від проекту та дотримання бюджету, комісія складає підсумковий акт приймання-передачі. Це гарантує, що мережа готова до безперебійної експлуатації у режимі 24/7 та надійно захищає персональні дані громадян.

Особлива увага приділяється стадії передачі документації та навчання персоналу. На цьому етапі перевіряється повнота, актуальність та якість розробленої експлуатаційної документації (згідно з розділом 1.1.4), а також оцінюється ефективність проведеного навчання співробітників замовника. Повний комплект документації передається замовнику у паперовому та електронному вигляді.

1.2 Аналіз інформаційних потреб та структури підприємства

Управління Державної міграційної служби (УДМС) у Тернопільській області функціонує як територіальна ланка центрального органу виконавчої влади, на яку покладено завдання з реалізації державної міграційної політики на регіональному рівні.

Організаційна структура установи є розгалуженою та дворівневою: вона складається з головного офісу (апарату управління) та мережі територіальних підрозділів. Адміністративний центр Управління структурований за функціональним принципом і налічує 4 спеціалізовані відділи, тоді як безпосередню взаємодію з населенням забезпечують 17 віддалених територіальних підрозділів, розміщених у районних та міських центрах області.

В кваліфікаційній роботі згідно із технічним завданням необхідно розробити мережу саме для головного офісу Управління ДМС в Тернопільській області.

Для побудови ефективної архітектури Управління ДМС було проведено аналіз ключових підрозділів, кожен з яких формує специфічні вимоги до мережевого середовища:

- апарат управління та секретаріат – забезпечує стратегічне керівництво та документообіг. Потребує безперебійного доступу до корпоративних поштових сервісів та баз звітності. Пріоритетом тут є стабільність з'єднання для роботи з внутрішніми наказами;

- сектор паспортної роботи та реєстрації – це найбільш навантажений сегмент, що взаємодіє з Єдиним державним демографічним реєстром (ЄДДР). Робота з біометричними даними та оформлення закордонних паспортів вимагає найвищого рівня захисту каналів зв'язку;

- підрозділ міграційного контролю та громадянства – оперує даними іноземців та осіб без громадянства. Специфіка роботи з міжвідомчими базами даних диктує необхідність логічної ізоляції цього сегмента від загальної мережі;

- фінансово-економічна служба – опрацьовує конфіденційну бухгалтерську інформацію та платіжні операції. Вимагає створення окремого захищеного контуру, ізольованого від загального документообігу;

- канцелярія та архів – відповідає за реєстрацію вхідної кореспонденції та оцифрування документів. Основне навантаження припадає на систему електронного документообігу та мережеві ресурси друку;

- служба IT-підтримки та кіберзахисту – має повні адміністративні привілеї для моніторингу серверної інфраструктури та управління віртуальними мережами (VLAN);

- географічно розподілені підрозділи – віддалені філії, що підключаються до центрального вузла через публічні мережі. Це вимагає впровадження криптографічно захищених VPN-тунелів для безпечного доступу до ЄДДР.

Розподіл комп'ютерного обладнання по відділах представлено в таблиці 1.1

Таблиця 1.1 Розподіл комп'ютерної техніки по відділах підприємтсва

№	Відділ	Кількість ПК	Периферійне Обладнання
1	Адміністративний	2	1 БФП.
2	Паспортно-реєстраційний	18	4 БФП, 9-10 Комплектів біометрії (сканери, камери).
3	Громадянства та Імміграції	9	2 БФП, 1 Пристрій верифікації документів.
4	Фінансово-Господарський	5	1 БФП, 1 Швидкісний принтер.
5	Документообігу	5	1 БФП/Сканер.
6	IT-Відділ	2	1 ПК адміністратора, 1 Тестовий
Разом		41	

Специфіка діяльності Управління ДМС, що пов'язана з опрацюванням персональних даних, біометричних показників та службової інформації з обмеженим доступом, висуває суворі вимоги до архітектури проектованої мережі. Ключовим пріоритетом є створення системи, що відповідає державним стандартам у сфері технічного захисту інформації (ТЗІ) та забезпечує високу продуктивність сервісів.

З огляду на ці фактори, проектне рішення базується на таких принципах:

- впровадження технології VLAN для глибокої сегментації мережі. Це дозволяє ізолювати трафік критично важливих служб (наприклад, роботу з ЄДДР) від загальних сегментів, мінімізуючи ризики внутрішніх загроз;

- використання багатофункціональних міжмережевих екранів (Firewall) як на зовнішній межі мережі, так і для фільтрації потоків даних між внутрішніми сегментами. Це забезпечує повний контроль над доступом до мережевих ресурсі;

- обов'язкове застосування протоколів шифрування для всіх даних, що виходять за межі локальної інфраструктури Головного управління. Створення захищених VPN-тунелів гарантує цілісність інформації при взаємодії з віддаленими підрозділами через публічні канали зв'язку

Детальні параметри необхідної пропускної здатності для забезпечення стабільної роботи зазначених сервісів наведено у таблиці 1.2.

Таблиця 1.2 Вимоги до пропускної здатності та затримки

Сфера діяльності	Мережеві вимоги	Кількісна оцінка
Реєстрація та видача документів	Висока пропускна здатність (для передачі пакетів біометричних даних), низька затримка (<50 мс) для транзакцій з центральними реєстрами.	З’єднання PC - Комутатор: 1 Гбіт/с; Сервер - Комутатор ядра: 10 Гбіт/с.
Внутрішній документообіг	Надійний доступ до файлових та поштових серверів.	Стандартний офісний трафік (до 100 Мбіт/с на користувача).
Забезпечення безпеки	Гарантована пропускна здатність для потокового відео (QoS) та ізоляція трафіку (VLAN).	Постійний потік даних (близько $4-6$ Мбіт/с на камеру).
Зовнішня комунікація	Висока швидкість зовнішнього каналу (забезпечення потреб усіх ТП через ГУ).	100 Мбіт/с – 1Гбіт/с.

Архітектура проектованої мережі Управління ДМС передбачає інтеграцію декількох типів кінцевих пристроїв, кожен з яких формує специфічні запити [3]:

- серверна група (Центральний вузол) – виступає ядром системи, що потребує найвищого рівня відмовостійкості. Для цих вузлів є обов'язковим апаратне резервування (дублювання блоків живлення та мережевих інтерфейсів) у поєднанні з максимальною пропускною здатністю магістральних каналів;

- спеціалізовані станції біометричного контролю – оскільки швидкість обробки великих масивів біометричних даних безпосередньо корелює з часом обслуговування громадян, ці вузли вимагають стабільного підключення на швидкості 1 Гбіт/с без затримок у передачі пакетів;

- типові робочі місця спеціалістів – стандартні станції, призначені для роботи з реєстрами та електронним документообігом, що забезпечуються підключенням на рівні 1 Гбіт/с для комфортної щоденної експлуатації;

- система IP-відеоспостереження – камери інтегруються в мережу з використанням технології PoE (Power over Ethernet), що дозволяє передавати дані та живлення одним кабелем. Це спрощує розгортання та забезпечує необхідну швидкість 1 Гбіт/с для трансляції відеопотоку високої чіткості.

1.3 Аналіз інформаційних потоків

Дослідження інформаційних потоків дозволяє визначити ключові параметри руху даних: інтенсивність, рівень критичності та необхідні заходи безпеки. Ці дані є базовими для формування топології мережі та налаштування політик міжсегментної фільтрації трафіку. Інформаційну структуру УДМС класифіковано за трьома векторами: внутрішні, зовнішні та спеціалізовані.

Внутрішні інформаційні потоки здійснюються в середині головного офісу Управління:

- транзакції ЄДДР (I1) – найбільш інтенсивний потік, що включає операції читання/запису між відділом реєстрації та СКБД. Вимагає мінімальних затримок (latency) та обов'язкової ізоляції у виділеному VLAN;

- документообіг та поштові сервіси (I2) – стабільний обмін даними серед усіх відділів. При середній інтенсивності має високі вимоги до конфіденційності, контролю доступу та регулярності бекапування;

- управління інфраструктурою (I3) – трафік адміністрування мережевих пристроїв з боку IT-відділу. Незважаючи на низьку інтенсивність, має критичне значення для життєдіяльності мережі;

- відеоспостереження (I4) – постійний потік високої щільності від IP-камер до відеосервера. Чутливий до втрат пакетів, тому ізолюється в окремий сегмент для запобігання перевантаженню робочих каналів.

Зовнішні магістральні потоки реалізуються через прикордонний маршрутизатор та Firewall для зв'язку із зовнішніми ресурсами:

- канал із Центральним апаратом (E1) – потік максимальної пріоритетності для доступу до загальнонаціональних баз ЄДДР. Захищається через VPN-тунелі з використанням сертифікованих криптографічних засобів;

- зв'язок із територіальними підрозділами (E2) – потік високої критичності зі змінною інтенсивністю. Забезпечує цілісність даних між ГУ та філіями через корпоративні Site-to-Site VPN;

- загальний доступ до мережі Інтернет (E3) – трафік для веб-серфінгу та оновлень. Підлягає обов'язковій фільтрації через веб-фільтри та проксі-сервери на базі Firewall.

На основі проведеного аналізу сформульовано наступні вимоги:

- створення мінімум п'яти логічних сегментів (VLAN): серверний, адміністративний, відеоспостереження, гостьовий та сегмент безпеки;

- маршрутизатор повинен мати апаратну потужність для шифрування VPN-трафіку (E1, E2) та виконання NAT без зниження швидкості.

- висока інтенсивність потоку I1 обґрунтовує впровадження 10 Гбіт/с магістралей у ядрі мережі;

- критичність потоків E1 та I1 вимагає дублювання каналів зв'язку та серверних потужностей.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Аналіз та обґрунтування вибору топології та технології мережі

З огляду на результати аналізу інформаційних потоків здійснений в розділі 1.3, до фізичної архітектури локальної мережі Управління ДМС у Тернопільській області висувається низка критичних вимог. Зокрема, необхідність забезпечення безперервної роботи з ЄДДР та стабільності VPN-тунелів вимагає зведення до мінімуму єдиних точок відмови (Single Points of Failure). Крім того, інфраструктура має бути гнучкою: підключення нових вузлів чи віддалених підрозділів не повинно потребувати реорганізації ядра мережі. Додатковими критеріями є підтримка централізованого управління, логічної ізоляції трафіку (VLAN) та гарантування високошвидкісного обміну даними, що є вкрай важливим для своєчасної обробки біометричної інформації.

Враховуючи масштаб мережі (41 робоча станція) та високу значущість серверного сегмента, оптимальним рішенням є впровадження класичної ієрархічної топології. Вона будується за трирівневою еталонною моделлю: «Ядро (Core) – Розподіл (Distribution) – Доступ (Access)» (див. рис. 2.1).

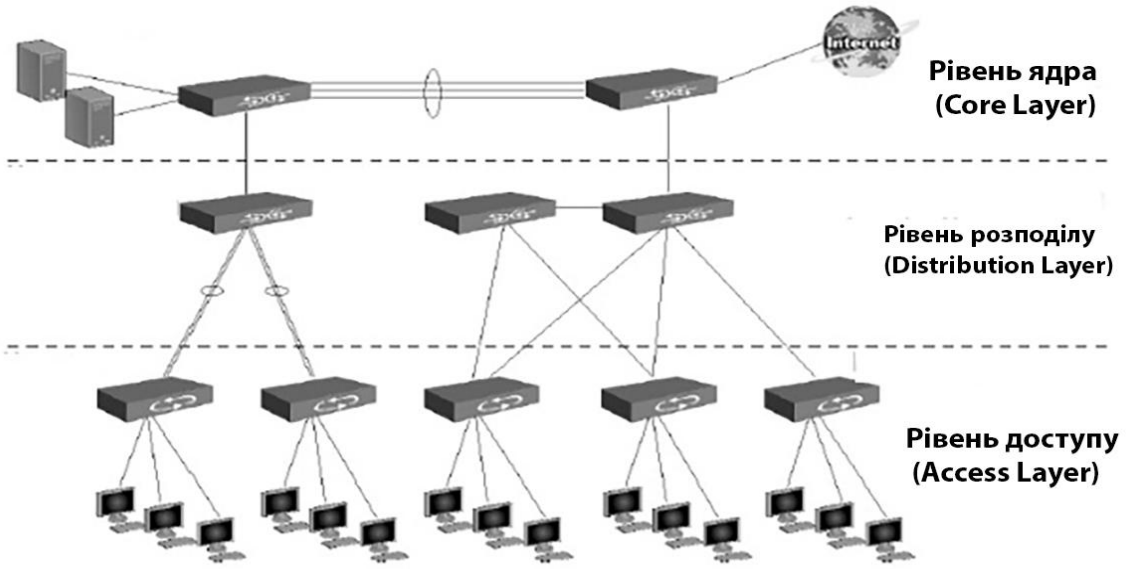


Рисунок 2.1 – Ієрархічна зіркоподібна топологія та трирівнева модель мережі

Цей підхід є де-факто стандартом для корпоративних мереж, оскільки забезпечує найвищі показники відмовостійкості, керованості та дозволяє модульно нарощувати потужності без впливу на суміжні сегменти інфраструктури.

Базовим рівнем цієї архітектури є рівень доступу (Access Layer), який відповідає за фізичне підключення кінцевого обладнання: робочих станцій, IP-камер та периферії. Для його реалізації застосовуються комутатори другого рівня (Layer 2 Access Switches). До цих пристроїв висуваються суворі технічні вимоги: забезпечення пропускної здатності 1 Гбіт/с на кожному клієнтському порту, підтримка технології живлення через Ethernet (PoE) для функціонування систем відеоспостереження, а також можливість маркування трафіку для його подальшої сегментації (VLAN). Зібраний клієнтський трафік комутатори доступу консолідують та передають магістральними каналами на вищий щабель – комутатори рівня розподілу [4].

Рівень розподілу (Distribution Layer) виконує функцію консолідації трафіку, що надходить від комутаторів доступу, та слугує логічною межею для маршрутизації між віртуальними мережами (Inter-VLAN Routing). Оптимальним апаратним рішенням для цього сегмента є багатофункціональні комутатори 3-го рівня (Layer 3 Switches). Вони забезпечують високошвидкісну обробку пакетів, застосування списків контролю доступу (ACL) для міжсегментної фільтрації, а також підтримку політик якості обслуговування (QoS). Крім того, цей рівень є ключовою точкою для впровадження механізмів резервування [4].

Рівень ядра (Core Layer) призначений для максимально швидкого та надійного транспортування великих масивів даних між рівнем розподілу та критично важливими серверними ресурсами. Технічна реалізація цього рівня базується на високопродуктивних комутаторах 3-го рівня або спеціалізованих маршрутизаторах, що здатні підтримувати пропускну здатність магістралей до 10 Гбіт/с. Головними вимогами тут є апаратна надмірність (резервування каналів), мінімальні затримки передачі (latency) та інтеграція з прикордонними міжмережевими екранами для виходу в зовнішні мережі [4].

Зазначена трирівнева архітектура фізично реалізується у вигляді ієрархічної (деревоподібної) зірки. На відміну від класичної зіркоподібної топології з єдиним центром, ієрархічна структура передбачає каскадне з'єднання мережевих вузлів. Такий підхід гарантує низку експлуатаційних переваг [7]:

- завдяки резервуванню на рівнях розподілу та ядра, локальні збої на рівні доступу не порушують глобальну працездатність системи;
- інтеграція нових клієнтських сегментів здійснюється шляхом простого підключення додаткових комутаторів доступу, що не впливає на продуктивність ядра;
- логічні політики безпеки (ACL) та пріоритезації (QoS) концентруються на рівні розподілу, значно спрощуючи управління;
- внутрішньосегментний обмін даними (в межах одного VLAN) локалізується на комутаторах доступу, розвантажуючи магістральні канали;
- рівень розподілу діє як надійний бар'єр, що строго регламентує рух трафіку між різними функціональними підрозділами.

У додатку Б представлено розроблену логічну топологію мережі.

При проектуванні локальної обчислювальної мережі (ЛОМ) для Управління ДМС було проаналізовано базові мережеві архітектури. З огляду на моральне застарівання технологій Token Ring та FDDI, а також враховуючи сучасні вимоги до пропускної здатності, масштабованості та економічної доцільності, єдиним раціональним вибором є родина стандартів Ethernet [3].

Вибір технології Ethernet (IEEE 802.3) для реалізації даного проекту в УДМС Тернопільської області базується на таких стратегічних факторах:

- універсальність та сумісність – будучи світовим стандартом, Ethernet підтримується абсолютною більшістю сучасного обладнання (сервери, АРМ, IP-камери), що спрощує інтеграцію та обслуговування;
- гнучкість швидкісних режимів – технологія дозволяє масштабувати швидкість передачі від 10 Мбіт/с до 100 Гбіт/с і вище в межах однієї інфраструктури;

- економічна ефективність: висока доступність компонентів (комутаторів та кабельної продукції) суттєво оптимізує капітальні витрати на реалізацію проекту;

- підтримка PoE – можливість дистанційного живлення IP-камер та іншого периферійного обладнання безпосередньо через інформаційний кабель значно спрощує монтаж та знижує витрати на електромережу.

Стандарти, що впроваджуються у проекті:

- Gigabit Ethernet (1000BASE-T) – використовується для організації доступу кінцевих користувачів. Швидкість 1 Гбіт/с повністю задовольняє потреби офісних програм та інтенсивного трафіку транзакцій ЄДДР;

- 10 Gigabit Ethernet (10GBASE-R) – застосовується для побудови магістральної підсистеми між рівнями ядра та розподілу, а також для підключення серверного парку. Це нівелює ризик виникнення «вузьких місць» при агрегації потоків даних.

Впровадження ієрархічної топології у поєднанні з гібридним середовищем передачі даних Ethernet створює стійкий фундамент для надійної роботи інфраструктури Управління ДМС у Тернопільській області.

2.2 Вибір кабельного середовища та розташування вузлів мережі

У проекті реалізовано комбінований підхід до вибору кабельної інфраструктури:

- мідна вита пара (UTP Cat 6) – формує горизонтальну підсистему (від комутатора до робочого місця);

- оптоволоконний кабель (Fiber Optic) – складає вертикальну (магістральну) підсистему. Забезпечує стійкість до електромагнітних завад, підтримку швидкості 10 Гбіт/с та надійний зв'язок між телекомунікаційними вузлами на великих відстанях.

Для побудови горизонтального сегмента структурованої кабельної системи (СКС) обрано неекрановану виту пару (UTP) категорії 6 (Cat 6). Дане

рішення є оптимальним балансом між економічною доцільністю та відповідністю актуальним вимогам до продуктивності мережі.

Ключові переваги обраного середовища передачі:

- кабель Cat 6 забезпечує повноцінну підтримку стандарту Gigabit Ethernet (1000BASE-T) на відстанях до 100 метрів, що повністю покриває потреби робочих місць у центральному офісі та територіальних підрозділах;

- завдяки кращим показникам захисту від перехресних перешкод (crosstalk) та системних шумів порівняно з категорією 5e, цей кабель гарантує високу стабільність сигналу та створює технологічний запас для переходу на 10 Gigabit Ethernet на коротких дистанціях у майбутньому;

- даний тип кабелю буде використаний як єдиний стандарт для підключення автоматизованих робочих місць (АРМ) користувачів, систем IP-відеоспостереження та точок доступу Wi-Fi;

- використання Cat 6 дозволяє ефективно реалізувати технологію Power over Ethernet (PoE), забезпечуючи живленням відеокамери та мережеве обладнання безпосередньо через інформаційний кабель, що спрощує монтаж та знижує витрати на електромережу

На основі комплексного аналізу технічних завдань та з урахуванням бюджетних лімітів проекту, для побудови горизонтальної підсистеми обрано кабель U/UTP Cat.6 4Pr вітчизняного виробника «Одескабель». Даний вибір зумовлений високою якістю продукції та її повною відповідністю міжнародним інженерним регламентам, зокрема ISO/IEC 11801 та ANSI/TIA/EIA-568 [11].

Технічні особливості обраного провідника [14]:

- кабель складається з чотирьох пар мідних дротів діаметром 0,57 мм (стандарт 23 AWG);

- кожна жила захищена поліетиленовим шаром (загальний діаметр 1,05 мм), що забезпечує необхідні діелектричні властивості та механічну тривалість;

- параметри кабелю гарантують стабільну роботу мережі на гігабітних швидкостях із високим запасом міцності сигналу.

Для забезпечення надійного фізичного з'єднання та термінації ліній у проекті використовуються наступні компоненти:

- конектори: Обрано модульні вилки ATCOM RJ45 CAT.6 UTP, які мають конфігурацію 8P8C. Вони спеціально розроблені для роботи з кабелем Категорії 6, що мінімізує перехресні завади у точці контакту;

- мережеві розетки: в усіх точках доступу встановлюються уніфіковані розетки стандарту RJ45. Це створює гнучку систему підключення та спрощує можливу перепланову робочих місць у майбутньому;

- комутаційні шнури (патч-корди): для з'єднання АРМ із розетками обрано готові рішення довжиною 1,5 метра – модель 2E CAT6 UTP 26AWG. Використання заводських патч-кордів гарантує кращу якість передачі даних порівняно з власноруч виготовленими аналогами. Зовнішній вигляд обраного виробу наведено на рисунку 2.2.

Рисунок 2.2 – Патч-корд 2E CAT6 UTP RJ-45 26AWG

Для оформлення робочих місць (РМ) обрано двопортові інформаційні розетки стандарту RJ-45 (Cat 6). Таке рішення є галузевим стандартом для сучасних офісних мереж. Наявність двох незалежних точок підключення дозволяє раціонально розподілити ресурси: один порт виділяється для стабільного підключення персонального комп'ютера, а другий – для забезпечення роботи IP-телефонії. Це дозволяє фізично розділити мережу для передачі даних та мережу для голосу (Voice VLAN) вже на рівні розетки.

Найбільш раціональний вибір з точки зору бюджету та сумісності з кабелем є вибір двопортової розетки Одескабель (OK-Net), представлений на рисунку 2.3.

Рисунок 2.3 – Мережева розетка OK-net 6 UTP

Дане рішення базується на наступних технічних та експлуатаційних перевагах:

- накладний тип виконання дозволяє оперативно розгортати мережеву інфраструктуру без проведення складних загальнобудівельних робіт (штроблення стін), що є критичним для діючих офісних приміщень;

- розетка сертифікована для роботи з кабелем Категорії 6, що гарантує підтримку гігабітних швидкостей та збереження характеристик сигналу на всьому тракті;

- забезпечує максимально чистий сигнал, що критично для біометричних даних та відео високої чіткості;

- найкраще співвідношення «ціна/якість» для державних установ.

Для побудови магістральної підсистеми обрано волоконно-оптичний кабель ОПТ-24М виробництва заводу «Південкабель». Дана модель спроектована для високонадійних ліній зв'язку та має наступні технічні характеристики:

- тип волокна: найсучаснішими стандартами є OM3 (бірюзовий колір оболонки) та OM4 (фіолетовий). Вони оптимізовані для роботи з лазерами типу VCSEL;

- на швидкості 10 Гбіт/с волокно OM3 працює на відстані до 300 метрів, а OM4 – до 400-550 метрів

- серцевина має більший діаметр (50 мкм), що полегшує стикування кабелів та робить систему менш чутливою до мікрозабруднень конекторів.

Для багатомодового волокна стандартним рішенням вибору SFP+ трасниверів є модулі типу SR (Short Range).

Трансивер SFP-10G-SR – це один із найпопулярніших модулів для побудови сучасних локальних мереж. Назва розшифровується досить просто: SFP+ вказує на форм-фактор, 10G – на швидкість, а SR означає "Short Range" (мала відстань).

Для організації вузла комутації в мережі УДМС ми обрали стандартні підлогові серверні шафи висотою 42U. Таке рішення забезпечує надійний фізичний захист обладнання від стороннього втручання завдяки замкам на дверцятах, а інтегровані вентиляційні модулі гарантують оптимальний температурний режим для активних пристроїв. Висота 42U також створює необхідний простір для впорядкованого розміщення всіх компонентів системи. Проаналізувавши співвідношення ціна-якість вирішено обрати модель Hypernet WMNC-18U-FLAT, зовнішній вигляд якої представлено на рисунку 2.4.

Рисунок 2.4 – Комутаційна шафа Hypernet WMNC-18U-FLAT

Важливим елементом пасивної інфраструктури в шафі є патч-панелі. Вирішено використати 24-портові моделі категорії 6, що повністю відповідає обраному раніше кабелю. Патч-панель виконує роль точки термінації (закінчення) стаціонарних ліній, що йдуть від робочих місць. Це дозволяє адміністратору оперативно змінювати конфігурацію мережі та проводити діагностику несправностей, не пошкоджуючи основні кабельні траси.

Надзвичайно важливим аспектом при проєктуванні топології мережі є забезпечення функціональної доступності робочих зон. Необхідно організувати простір так, щоб кожен співробітник мав безперешкодний доступ як до свого автоматизованого робочого місця (АРМ), так і до спільної периферійної техніки – принтерів та сканерів. На рисунку 2.5 представлено план приміщення Управління ДМС в Тернопільській області.

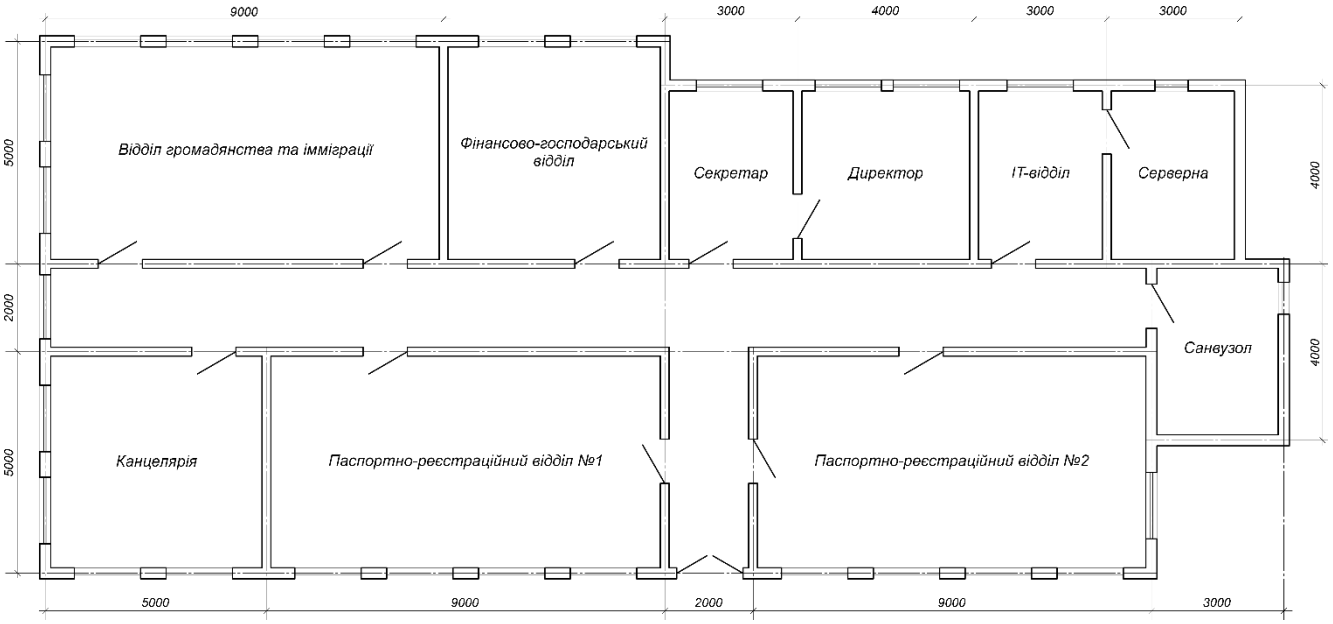


Рисунок 2.5 – План приміщення УДМС в Тернопільській області

Для забезпечення централізованого управління та безпеки, ключові вузли мережі організовані наступним чином:

- серверна кімната – тут зосереджено основне активне обладнання (маршрутизатор та комутатор ядра), розміщене в головній телекомунікаційній шафі. З огляду на топологію, у цій же шафі встановлюються комутатори доступу для ІТ-відділу, адміністрації та системи відеоспостереження. Фізичні сервери також розташовуються в цьому приміщенні для обмеження стороннього доступу;

- розподіл робочих станцій по окремих відділах організації УДМС представлено в таблиці 1.1. При цьому слід врахувати, що паспортно-реєстраційний відділ розташований в двох окремих кімнатах, відповідно по 10 та 8 ПК;

- локальні комутаційні вузли – комутатори доступу для відділів громадянства, документообігу та фінансового сектора встановлюються безпосередньо в робочих зонах у настінних шафах. Аналогічне рішення передбачено для другого офісу паспортно-реєстраційного відділу.

Центральним вузлом мережі обрано комутаційну шафу в захищеній серверній кімнаті, де зосереджується все ключове обладнання рівня ядра та маршрутизації. Завдяки територіальній близькості, у цій же шафі доцільно розмістити комутатори рівня доступу для ІТ-відділу та адміністрації, включаючи робочі місця директора та секретаріату. Також тут встановлюється окремий комутатор для агрегації трафіку з камер відеоспостереження, а для гарантування безпеки та обмеження фізичного доступу в цьому приміщенні розташовуються і мережеві сервери.

Для підрозділів, що знаходяться в інших частинах будівлі, передбачено децентралізовану схему розміщення. Комутатори доступу для відділів громадянства, документообігу та фінансового сектору встановлюються безпосередньо в їхніх робочих зонах у компактних настінних шафах. Окремий комутаційний вузол паспортно-реєстраційного відділу буде змонтований у приміщенні другого офісу для оптимізації довжини кабельних ліній (див. рис. 2.6).

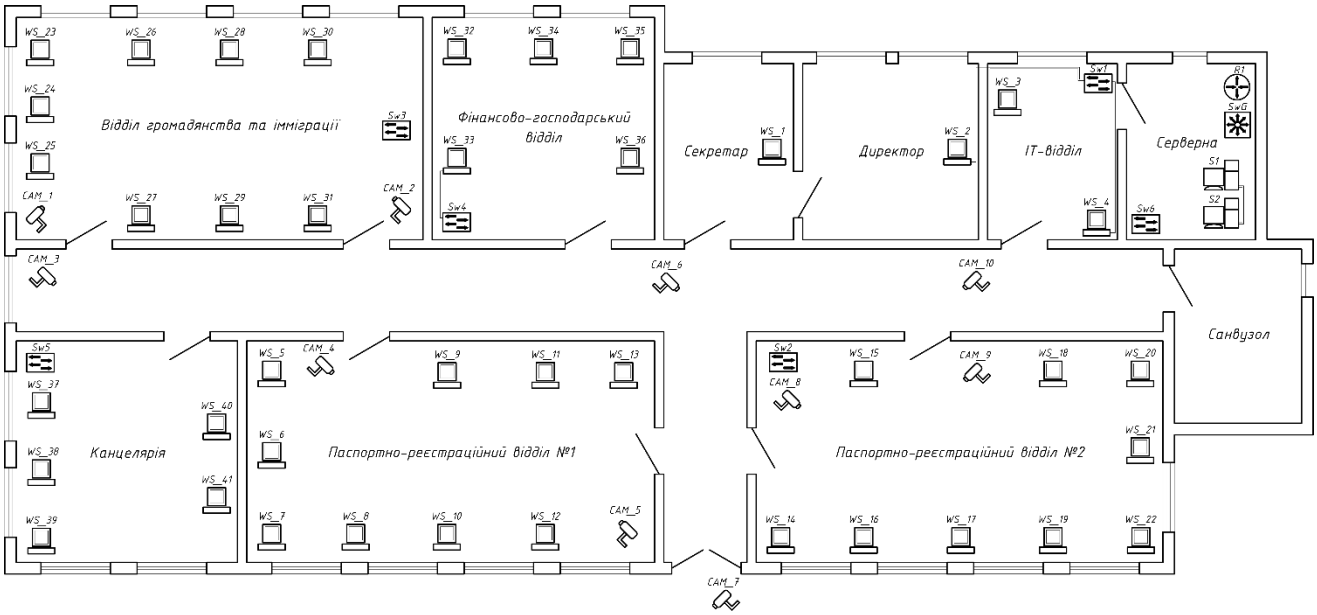


Рисунок 2.6 – Розташування мережевого обладнання на плані приміщення

2.3 Обґрунтування вибору комунікаційного обладнання

Правильний вибір активного мережевого обладнання є важливим для забезпечення продуктивності, безпеки та безперебійного функціонування мережі УДМС. Його вибір базується на ієрархічній моделі та аналізі інформаційних потоків (див. розділ 1.3).

До комплексу активного комунікаційного обладнання розроблюваної мережі входять: високопродуктивні головні комутатори (які формують ядро мережі при використанні топології «розширена зірка»), комутатори доступу для підключення кінцевих вузлів робочих груп, а також маршрутизатори з інтегрованими функціями міжмережевого екранування (Next-Generation Firewall).

З огляду на архітектуру мережі, до головного шлюзу безпеки висуваються наступні наступні вимоги [6]:

- висока пропускна здатність. Пристрій повинен забезпечувати швидкість обробки трафіку Firewall/VPN на рівні не менше 1.5 Гбіт/с. Цей запас продуктивності є надзвичайно важливим для безперебійної обробки основного гігабітного (1 Гбіт/с) каналу зв'язку без внесення апаратних затримок, навіть за умов максимального мережевого навантаження;

- надійне криптографічне забезпечення. Обов’язковою є апаратна підтримка побудови віртуальних приватних мереж за технологією Site-to-Site VPN (на базі протоколу IPsec). Висока швидкість шифрування необхідна для гарантованого захисту конфіденційних інформаційних потоків E1 (трафік центрального апарату) та E2 (дані територіальних підрозділів) під час їх передачі через відкриті канали зв'язку;

- резервування та балансування навантаження. Необхідна вбудована підтримка технологій Failover та Load Balancing між двома незалежними зовнішніми WAN-інтерфейсами. Це гарантує безперервність бізнес-процесів та автоматичне перемикання на резервного провайдера у разі аварії на основній лінії;

- комплексний аналіз на прикладному рівні. Маршрутизатор повинен здійснювати поглиблену інспекцію пакетів (Deep Packet Inspection), мати модулі системи виявлення та запобігання вторгненням (IPS/IDS), а також здійснювати URL-фільтрацію. Це дозволить ефективно контролювати та безпечно маршрутизувати інформаційний потік Е3 (загальний доступ до мережі Інтернет), блокуючи шкідливе програмне забезпечення та несанкціонований доступ.

На основі проведеного аналізу ринку та співставлення технічних характеристик із вищезазначеними критеріями, для реалізації проєкту було обрано міжмережевий екран нового покоління FortiGate FG-100F (див. рис. 2.7). Цей пристрій повністю задовольняє потреби корпоративної мережі УДМС у швидкодії та комплексному захисті.

Рисунок 2.7 – Міжмережевий екран FortiGate FG-100F

Обрана модель вирізняється надлишковою продуктивністю, що є важливим фактором для стабільної роботи мережі УДМС. Зокрема, пропускна здатність VPN (IPSec) сягає 10 Гбіт/с, що дозволяє без втрат швидкості шифрувати інтенсивні інформаційні потоки категорій Е1 та Е2. Загальна пропускна здатність пристрою у 18 Гбіт/с у поєднанні з наявністю двох високошвидкісних портів 10GE SFP+ гарантує відсутність «вузьких місць» при передачі даних. Окрім швидкодії, пристрій забезпечує комплексний контроль потоку Е3 завдяки розширеним функціям шлюзу безпеки нового покоління (NGFW), включаючи системи запобігання вторгненням (IPS/IDS) та інтелектуальну веб-фільтрацію.

Враховуючи масштаби мережі УДМС та її топологічну структуру, було прийнято рішення про об’єднання рівнів ядра (Core) та розподілу (Distribution) в

межах одного високопродуктивного пристрою – комутатора 3-го рівня (Layer 3 Switch). Така архітектура дозволяє оптимізувати витрати на обладнання без втрати продуктивності та спростити адміністрування мережі.

Для виконання ролі центрального вузла комутації до пристрою висуваються наступні вимоги:

- високошвидкісні магістральні інтерфейси. Для забезпечення швидкої обробки критичного інформаційного потоку І1 (ЄДДР) комутатор повинен підтримувати швидкість 10 Гбіт/с на всіх магістральних SFP+ портах. Це гарантує мінімальні затримки при взаємодії між серверами та комутаторами рівня доступу;

- маршрутизація між логічними сегментами (Inter-VLAN Routing). Оскільки мережа розділена на декілька функціональних сегментів (VLAN 10, 20, 30, 40, 50, 60, 90, як визначено в розділі 2.3), пристрій має забезпечувати ефективну маршрутизацію трафіку між ними на апаратному рівні;

- відмовостійкість та усунення петель. Обов'язковою є підтримка протоколів резервування шлюзу (наприклад, VRRP) для забезпечення безперервності зв'язку, а також протоколів сімейства Spanning Tree (STP) для запобігання виникненню широкомовних штормів у топологіях із надлишковими зв'язками;

- керування трафіком та безпека. Повна підтримка налаштування віртуальних мереж (VLAN), списків контролю доступу (ACL) для розмежування прав доступу та механізмів якості обслуговування (QoS). Останні є критичними для пріоритизації чутливого до затримок VoIP-трафіку (потік І4);

- достатня щільність портів. Конфігурація пристрою має передбачати не менше 10 портів SFP+ (10 Гбіт/с): 4 – для безпосереднього підключення серверної ферми та 6 – для агрегації каналів від комутаторів доступу;

На основі детального співставлення технічних характеристик із зазначеними вимогами, для реалізації проекту обрано стекований комутатор Cisco Catalyst C9300-24S (див. рис. 2.8). Ця модель поєднує в собі високу щільність оптичних портів та розширений функціонал безпеки й автоматизації.

Рисунок 2.8 – Головний комутатор Cisco Catalyst C9300-24S

Обраний пристрій є високонадійним комутатором 3-го рівня (Layer 3), головною особливістю якого є потужна комутаційна матриця з ємністю 480 Гбіт/с. Така продуктивність гарантує миттєву обробку даних навіть при пікових навантаженнях. Наявність 24 портів стандарту 10G SFP+ є вирішальним фактором при виборі, оскільки це забезпечує необхідну пропускну здатність для магістрального потоку I1. Окрім швидкодії, комутатор підтримує критично важливі протоколи відмовостійкості та керування топологією, такі як STP (для усунення петель) та VRRP (для резервування шлюзу), а також забезпечує апаратну маршрутизацію між віртуальними мережами (Inter-VLAN Routing).

Комутатори рівня доступу відіграють важливу роль у мережевій ієрархії УДМС, оскільки саме вони забезпечують безпосереднє підключення кінцевих вузлів: робочих станцій персоналу та камер відеоспостереження. Основним критерієм вибору для цього сегмента є використання керованих комутаторів 2-го рівня (Layer 2) з підтримкою технології дистанційного живлення PoE/PoE+.

Відповідно до технічного завдання, до пристроїв доступу висуваються такі функціональні вимоги:

- наявність щонайменше 24 портів стандарту RJ-45 з підтримкою швидкості 1 Гбіт/с (1000BASE-T). Це гарантує стабільну роботу комп’ютерної мережі та відсутність затримок при передачі даних користувачів;

- підтримка живлення через Ethernet на більшості портів є критично важливою для розгортання IP-камер (інформаційний потік I4). Це не лише спрощує монтаж обладнання, позбавляючи потреби у додаткових розетках, а й підвищує загальну відмовостійкість системи;

- наявність мінімум двох портів SFP/SFP+ для підключення до центрального комутатора ядра за допомогою оптоволоконних ліній зв'язку. Це забезпечує необхідну пропускну здатність для агрегації трафіку з усього рівня доступу;

- повна підтримка функцій 2-го рівня, зокрема тегування трафіку (VLAN Tagging 802.1Q) для логічної ізоляції сегментів, механізмів якості обслуговування (QoS) та функцій безпеки портів (Port Security), що блокують несанкціоноване підключення стороннього обладнання.

Враховуючи, що ядро мережі побудоване на базі Cisco Catalyst C9300, найбільш раціональним рішенням для рівня доступу є використання обладнання тієї ж лінійки – Cisco Catalyst C9200L-24P-4X. Це дозволяє зберегти цілісність мережевої екосистеми, гарантує повну апаратну сумісність та значно спрощує процес централізованого управління через систему Cisco DNA Center. Зовнішній вигляд обраної моделі представлено на рисунку 2.9.

Рисунок 2.9 – Комутатор рівня доступу Cisco Catalyst C9200L-24P-4X

Обраний комутатор спроєктований для забезпечення максимальної продуктивності та відмовостійкості безпосередньо на межі мережі. Апаратна платформа пристрою включає 24 порти стандарту Gigabit Ethernet (10/100/1000Base-T), кожен з яких повноцінно підтримує технологію PoE+ (IEEE 802.3at). Це дозволяє подавати до 30 Вт потужності на порт, що є важливим для стабільного живлення сучасних точок доступу Wi-Fi та купольних IP-камер високої роздільної здатності. Стандартний бюджет потужності становить 370 Вт, проте архітектура пристрою передбачає можливість резервування: встановлення додаткового блоку живлення дозволяє подвоїти доступний енергоресурс, гарантуючи роботу системи навіть при максимальному навантаженні.

Для організації високошвидкісних магістральних каналів зв'язку з ядром мережі (Cisco Catalyst C9300) модель C9200L-24P-4X оснащена чотирма фіксованими аплінками 10 Gigabit Ethernet (10G SFP+). Висока комутаційна ємність у 128 Гбіт/с та швидкість пересилання пакетів на рівні 190.4 Mpps дозволяють пристрою без затримок обробляти щільні потоки даних від кінцевих користувачів.

Окремої уваги заслуговують технології масштабування та управління:

- технологія StackWise-80 – дозволяє об'єднувати до восьми фізичних комутаторів у єдиний логічний юніт із пропускною здатністю стекування 80 Гбіт/с. Це спрощує адміністрування та створює високу стійкість до відмов на рівні стійки;
- програмна платформа Cisco IOS XE – забезпечує не лише розширений функціонал 2-го рівня, а й базові можливості маршрутизації (Layer 3). Завдяки ліцензіям Network Essentials/Advantage реалізується глибока інтеграція з екосистемою Cisco DNA Center, що відкриває широкі можливості для автоматизації налаштувань та інтелектуального моніторингу безпеки.

2.4 Обґрунтування вибору кінцевих вузлів мережі

На основі детального аналізу інформаційних потреб підрозділів (див. розділ 1.3) та функціональної класифікації користувачів, робочі станції мережі УДМС розподілені на дві категорії. Кожна група має індивідуальні системні вимоги, зумовлені специфікою програмного забезпечення та інтенсивністю мережевих потоків.

Перша група – спеціалізовані робочі станції – ця категорія охоплює робочі місця співробітників, які безпосередньо взаємодіють із базою ЄДДР та здійснюють обробку біометричних даних. Саме ці вузли генерують найбільш критичний трафік (потік I1), а їхня продуктивність є визначальним фактором швидкості обслуговування громадян. До них ставляться наступні вимоги:

- використання процесорів рівня Intel Core i5 / AMD Ryzen 5 останніх поколінь є обов'язковим для швидкої роботи спеціалізованого ПЗ (сканування та криптографічна обробка);

- обсяг оперативної пам'яті 16 ГБ (DDR4/DDR5) забезпечує стабільну багатозадачність між клієнтами СУБД та системними додатками. Застосування швидкісних накопичувачів 512 ГБ NVMe SSD є критичним для мінімізації затримок (latency) при завантаженні операційної системи та обробці масивних файлів біометрії;

- підключення здійснюється через адаптер 1 Гбіт/с Ethernet, що відповідає вимогам до пропускної здатності кінцевого вузла;

- додатково кожне місце комплектується біометричним сканером та вебкамерою високої роздільної здатності.

До другої групи відносяться вузли, призначені для загального документообігу, роботи з електронною поштою (потік І2) та засобів моніторингу мережі (потік І3). Вимоги до них оптимізовані для типових офісних завдань:

- процесори рівня Intel Core i3 / AMD Ryzen 3 у поєднанні з 8 ГБ RAM забезпечують комфортну роботу в середовищі MS Office, браузерах та системах електронного документообігу (СЕДО);

- наявність SSD-накопичувача на 256 ГБ гарантує швидкий відгук системи, що є стандартом сучасного корпоративного середовища.

Окрім персональних комп'ютерів, важливим сегментом мережі є підсистема відеоспостереження, що складається з 10 IP-камер. Оскільки інфраструктура побудована на обладнанні Cisco, вибір зупинено на професійних рішеннях, що підтримують стандарт ONVIF для повної інтеграції. Для внутрішнього моніторингу приміщень обрано купольні камери (DOME) від лідера ринку – Hikvision (модель DS-2CD2143G2-IS), які мають наступні характеристики:

- роздільна здатність 4 МП (2688x1520) дозволяє отримати високий рівень деталізації для ідентифікації осіб;

- технологія AcuSense на базі штучного інтелекту дозволяє фільтрувати хибні тривоги та класифікувати об'єкти (людина/транспорт), що значно знижує навантаження на оператора;

- повна підтримка стандарту 802.3af (PoE) дозволяє отримувати живлення безпосередньо від комутаторів доступу, що було обґрунтовано у попередньому розділі.

Зовнішній вигляд камери Hikvision DS-2CD2143G2-IS представлено на рисунку 2.10.

Рисунок 2.10 – Камера Hikvision DS-2CD2143G2-IS

2.5 Обґрунтування вибору серверів та визначення їх функцій

Серверне обладнання виступає центральною ланкою для обробки критичних інформаційних потоків, зокрема даних ЄДДР (потік І1) та внутрішнього документообігу (потік І2). Проектування серверної частини базується на принципах консолідації ресурсів через віртуалізацію та забезпеченні максимальної відмовостійкості системи. Для реалізації обрано стійкові сервери (Rack-mounted) з апаратною підтримкою технологій віртуалізації.

Концептуальні вимоги до серверного вузла:

- віртуалізація: використання промислового гіпервізора (VMware ESXi або Microsoft Hyper-V) дозволяє розмістити 5–6 логічних серверів на базі 2 фізичних хостів, що оптимізує використання заліза та спрощує процедуру резервного копіювання.

- застосування багатоядерних процесорів та швидкісних накопичувачів NVMe SSD є критичним для мінімізації затримок при роботі з базами даних (СКБД);

- наявність мінімум двох інтерфейсів 10 Гбіт/с із підтримкою агрегації каналів (LACP) гарантує високу пропускну здатність підключення до ядра мережі;

- обов'язкова наявність дубльованих блоків живлення з можливістю гарячої заміни (Hot-swap) та побудова дискових масивів RAID.

Для стабільного функціонування УДМС розраховано необхідні ресурси для кожної віртуальної машини (ВМ). Розрахунок проводиться шляхом сумування потреб віртуальних та резервування ресурсів для роботи хостової ОС (гіпервізора). Результати підрахунків представлені в таблиці 2.1

Таблиця 2.1 – Підрахунок необхідних ресурсів севрера

Тип сервера (роль)	К-сть ядер CPU	RAM (Гб)	Призначення та особливості
1	2	3	4
Контролер домену (AD/DNS/DHCP)	2	8	Висока надійність, стандартне навантаження.
База даних (СКБД/ЄДДР)	8	64	Максимальне навантаження на RAM та транзакції.
Файловий сервер	4	16	Кешування файлів, інтенсивні дискові операції.
Документообіг (СЕДО / Mail)	4	16	Стабільна підтримка поштових служб.
Відеоспостереження (VMS)	2	8	Обробка потоку I4, переважно запис на диск.
Моніторинг та управління	2	8	Незалежне адміністрування системи.
РАЗОМ (мінімум):	22	120	Сумарні потреби програмного комплексу.

Проаналізувавши результати розрахунгків таблиці 2.1 можна встановити наступні вимоги до конфігурації:

- оперативна пам'ять: з врахуванням принципу модульності та резервування (N+1), кожен фізичний сервер комплектується 128 ГБ RAM, що забезпечує загальний обсяг 256 ГБ на кластер;

- процесори: для покриття потреби у 22 ядрах та забезпечення запасу продуктивності обираються два процесори серії Intel Xeon Scalable (Gold або Silver). Кожен процесор має 12 фізичних ядер, що сумарно дає 24 ядра на кластер;

- дискова підсистема: реалізується за гібридним принципом: Tier 1 (СУБД) – RAID 10 на базі 4-х NVMe SSD по 1.6 ТБ для досягнення найвищої швидкості та відмовостійкості, Tier 2 (Архів/Відео) – RAID 6 на базі 6-ти SAS/SATA дисків по 2.4 ТБ для забезпечення великої ємності та виживання масиву при відмові двох дисків одночасно.

На основі проведених розрахунків обрано сервер Dell PowerEdge R760 у корпусі 2U Rack (див. рис. 2.11), який повністю задовольняє вимоги щодо масштабованості та надійності.

Рисунок 2.11 – Сервер Dell PowerEdge R760 (2U Rack)

Сервер Dell PowerEdge R760 виділяється високою надійністю, надмірністю живлення та охолодження. Підтримка RAID та великих обсягів RAM для ефективного функціонування критичної СУБД (потік І1, див. розділ 1.1). Його конфігурація:

– процесори – 2 x Intel Xeon (12+ ядер кожен);

– RAM – 128 ГБ (з можливістю розширення);

– мережеві адаптери –2 x 10G SFP + NIC (для магістралі Core Switch);

– дискова підсистема – гібридна конфігурація RAID 10 (NVMe) та RAID 6 (SAS/SSD).

2.6 Особливості монтажу мережі

Етап фізичного розгортання комп'ютерної мережі УДМС є одним із ключовим у процесі встановлення мережі, оскільки від точності його виконання безпосередньо залежать пропускна здатність, експлуатаційна надійність та термін служби всієї IT-інфраструктури. Суворе дотримання міжнародних стандартів структурованих кабельних систем (СКС) під час інсталяції дозволяє превентивно уникнути апаратних збоїв та забезпечити стабільну маршрутизацію даних..

Основою горизонтальної розводки є мідний кабель U/UTP Категорії 6. Для збереження естетики офісних приміщень та захисту провідників від фізичного пошкодження, магістралі прокладаються у спеціальних пластикових кабель-каналах перерізом 50×35 мм уздовж плінтусів та стін. У приміщеннях із фальшстелями або гіпсокартонними конструкціями застосовується метод прихованого монтажу.

Схема прокладання кабелів у мережі УДМС в Тернопільській області на плані приміщення представлено у додатку В.

Для забезпечення безперебійної передачі сигналів застосовуються жорсткі правила монтажу:

– при перетині капітальних стін формуються отвори діаметром 16 мм. У них обов'язково закладаються гофровані труби – це захищає кабель від перетирання та значно спрощує його заміну в майбутньому. Аналогічним чином (у гофротрубах 16 мм за підвісною стелею) підводяться траси по коридорах приміщення;

– категорично заборонено перевищувати допустимий радіус зламу крученої пари (норматив становить 4–8 зовнішніх діаметрів кабелю). Порушення цього правила призводить до незворотної зміни геометрії пар, що викликає деградацію сигналу та втрату швидкості;

– для унеможливлення перехресних наведень (EMI), слабкострумові інформаційні кабелі прокладаються на чітко регламентованій відстані від силових ліній електроживлення.

Централізація обладнання в головному офісі та філіях реалізується на базі комутаційних шаф. Для запобігання «кабельному хаосу» всередині стійок впроваджується суворий кабельний менеджмент із використанням горизонтальних органайзерів, маркування та фіксаційних стяжок.

Згідно з проєктом, у головній комутаційній шафі, розташованиій в серверній, компактно розміщується такий апаратний комплекс:

– міжмережевий екран: FortiGate FG-100F;

– ядро мережі: головний комутатор Cisco Catalyst C9300-24S;

– комутатор рівня доступу Cisco Catalyst C9200L-24P-4X для під’єднання вузлів директора, секретаря та IT-відділу;

– сервер Dell PowerEdge R760 (форм-фактор 2U Rack);

– лінійно-інтерактивне ДБЖ APC Back-UPS Pro 1500VA;

– 24-портова патч-панель Panduit (19 дюймів, Cat.6) та відповідні кабельні організатори.

На робочих місцях персоналу, а також у зонах підключення IP-телефонії монтуються накладні двопортові розетки OK-net стандарту 8P8C (RJ45) Категорії 6. Використання накладного (зовнішнього) форм-фактора значно пришвидшує процес розгортання мережі в умовах готового ремонту.

Завершальним етапом інсталяції є забезпечення захисного заземлення. Усі металеві напрямні комутаційних шаф, патч-панелі та металеві корпуси активного обладнання надійно підключаються до єдиного контуру заземлення будівлі, що відповідає державним та міжнародним нормам електробезпеки.

2.7 Обґрунтування вибору програмного забезпечення

Проєктування ІТ-інфраструктури для потреб Управління Державної міграційної служби (ДМС) вимагає впровадження серверної операційної системи, що відповідає найсуворішим стандартам безперебійності, захищеності та раціонального використання бюджетних коштів. З огляду на специфіку функціонування державного органу – зокрема, безперервну обробку, зберігання та передачу конфіденційних персональних і біометричних даних громадян — вибір програмної платформи є стратегічним рішенням.

На сучасному ринку корпоративного програмного забезпечення найбільш доцільними варіантами є дві архітектури: Windows Server та серверні рішення на базі ядра Linux (Ubuntu Server, CentOS/AlmaLinux).

Вибір конкретної ОС безпосередньо залежить від архітектурних вимог до мережі та переліку критичних сервісів, які має забезпечувати центральний обчислювальний вузол, а саме:

– розгортання та керування ієрархічною службою каталогів (Active Directory) для управління правами користувачів;

– організація надійного, масштабованого та стійкого до збоїв файлового сервера;

– інтеграція надійних механізмів криптографічного захисту, аудиту подій та багаторівневого розмежування доступу до реєстрів.

Основні переваги вибору Microsoft Windows Server [2]:

– служба каталогів Active Directory (AD DS): виступає галузевим стандартом для побудови централізованої моделі управління. AD DS забезпечує механізми єдиного входу (SSO), групові політики безпеки та комплексне адміністрування облікових записів, що є критично важливим для структури державного сектору;

– гарантується повна сумісність із клієнтськими робочими станціями, пакетами прикладних програм Microsoft Office та специфічним програмним забезпеченням, що використовується в ДМС.

– більшість системних адміністраторів державних установ мають підтверджений досвід експлуатації Windows-середовищ, що знижує витрати на навчання та прискорює розгортання;

– у версії 2025 впроваджено багаторівневі засоби захисту на рівні заліза та прошивки, що забезпечує підвищений захист конфіденційних реєстрів.

Серед недоліків варто виділити: значні витрати на ліцензування (серверні ліцензії) та вищу енергозатратність щодо апаратних ресурсів.

Як альтернатива на базі відкритого коду, Ubuntu Server пропонує наступні переваги [2]:

– відсутність ліцензійних платежів суттєво оптимізує бюджет проєкту;

– висока стійкість до відмов та оперативне усунення вразливостей спільнотою розробників роблять Linux ідеальним для ролей веб-серверів або проксі-шлюзів;

Ключові обмеження: складність адміністрування через командний рядок (CLI) та неповна функціональна заміна Active Directory при використанні Samba, що може спричинити конфлікти з внутрішнім ПЗ служби.

Враховуючи необхідність суворого дотримання групових політик та інтеграції в наявну державну інфраструктуру, найбільш раціональним вибором є Microsoft Windows Server 2025 Standard Edition.

Оскільки проєкт передбачає консолідацію серверних ролей на віртуальних машинах, важливим є вибір гіпервізора – програмного шару, що абстрагує апаратні ресурси фізичного хоста для одночасного запуску кількох систем.

Згідно з класифікацією [2], розрізняють два типи гіпервізорів:

– Тип 1 (Bare Metal / Нативний) – встановлюється безпосередньо на "голе залізо". Це забезпечує прямий доступ до процесора та пам'яті, гарантуючи максимальну продуктивність та ізоляцію;

– Тип 2 (Hosted / Хостовий) – працює як додаток поверх існуючої ОС. Використовується переважно для тестування, оскільки має додаткові затримки через проміжний шар операційної системи.

Для серверного сегмента УДМС обрано гіпервізор 1-го типу. Серед лідерів ринку (VMware ESXi та Microsoft Hyper-V) перевагу віддано Microsoft Hyper-V.

Це рішення обумовлене наступними факторами:

– Hyper-V є рідною технологією для обраної ОС Windows Server 2025, що спрощує менеджмент через єдину консоль;

– наявність вбудованої ролі Hyper-V у Windows Server дозволяє уникнути додаткових витрат на стороннє ПЗ віртуалізації.

– гіпервізор забезпечує високу швидкість роботи ВМ, що необхідно для стабільного функціонування бази даних ЄДДР та інших критичних служб.

Враховуючи архітектурні особливості інформаційної системи УДМС у Тернопільській області, а також необхідність забезпечення максимальної сумісності з серверною платформою, як базову операційну систему для робочих станцій пропонується використовувати Microsoft Windows 11 Professional.

Вибір даної ОС зумовлений наступними стратегічними факторами:

– Windows 11 є галузевим стандартом, що гарантує безшовну інтеграцію в доменну структуру Active Directory (AD). Це дозволяє адміністраторам ефективно впроваджувати групові політики (GPO) для автоматизованого налаштування безпеки та прав доступу на всіх вузлах мережі;

– платформа забезпечує повну підтримку драйверів для біометричних сканерів, камер високої роздільної здатності та іншої периферії, необхідної для оформлення паспортних документів;

– робота з державними реєстрами та системами електронного документообігу потребує стабільної інтеграції з пакетом Microsoft Office Professional Plus, що є інструментом для підготовки звітності та офіційної комунікації;

– більшість співробітників державної служби вже мають досвід роботи з інтерфейсом Windows, що мінімізує витрати часу на адаптацію персонал та знижує кількість помилок при експлуатації систем.

Для захисту клієнтських машин, що мають доступ до конфіденційних даних, передбачено впровадження наступного програмного стеку:

– антивірусний захист корпоративного класу: використання рішень із централізованим управлінням (Endpoint Protection) для запобігання поширенню шкідливого ПЗ та моніторингу загроз у реальному часі.

– засоби криптографічного захисту інформації (КЗІ): інсталяція спеціалізованих бібліотек та програм для роботи з електронним цифровим підписом (ЕЦП), що є обов'язковим для юридично значущого підписання документів;

– VPN-клієнти: забезпечення захищених тунелів для доступу до віртуальних приватних мереж та віддалених державних реєстрів у разі роботи поза внутрішнім контуром.

2.8 Розподіл адресного простору мережевих вузлів

Для створення структурованої та безпечної екосистеми в межах корпоративної мережі УДМС було прийнято рішення про використання приватного адресного простору IPv4 згідно зі стандартом RFC 1918. Як базу обрано мережу класу C – 192.168.0.0/24.

Вибір даного діапазону зумовлений наступними чинниками:

– мережа з маскою підмережі 255.255.255.0 дозволяє призначити до 254 унікальних IP-адрес для хостів. Це повністю задовольняє поточні потреби установи та створює значний технологічний резерв для майбутнього розширення інфраструктури;

– на момент проєктування мережа об'єднує 41 робочу станцію та 10 IP-камер відеоспостереження, що загалом становить 51 клієнтський вузол;

– враховуючи наявність двох фізичних серверів (на базі яких розгорнуто віртуалізований кластер), загальна кількість вузлів, що потребують статичної або динамічної адресації, становить 53 одиниці.

Використання мережі /24 при поточній потребі у 53 адреси означає, що мережа завантажена лише на ~21%. Це залишає майже 80% вільного адресного

простору для впровадження нових сервісів, підключення додаткового периферійного обладнання (принтерів, сканерів) або розгортання гостьових Wi-Fi зон без необхідності реструктуризації всієї мережі.

Логічна структура мережі УДМС базується на технології віртуальних локальних мереж (VLAN, стандарту IEEE 802.1Q). Це дозволяє розділити фізичну інфраструктуру на ізольовані широкомовні домени, що є критично важливим для забезпечення кібербезпеки, мінімізації мережевого шуму та впровадження політик якості обслуговування (QoS).

Відповідно до аналізу інформаційних потоків (Розділ 1), мережу структуровано на вісім функціональних сегментів:

– VLAN 10 (адміністрування IT) – виділений сегмент для трафіку управління активним обладнанням (Management VLAN). Доступ до інтерфейсів налаштування комутаторів та маршрутизаторів обмежений виключно для авторизованого IT-персоналу, що гарантує найвищий рівень захисту від внутрішніх загроз;

– VLAN 20 (паспортно-реєстраційний сектор) – призначений для робочих станцій, що здійснюють обробку біометричних даних та запитів до ЄДДР. Для цього сегмента налаштовується пріоритезація трафіку (QoS) при взаємодії із серверним сегментом (VLAN 90). Прямий доступ із загальних мереж (VLAN 50, 10) заблокований на рівні списків контролю доступу (ACL);

– VLAN 30 (громадянство та імміграція) – забезпечує роботу фахівців з міграційного контролю. Сегмент передбачає використання захищених VPN-тунелів для зв'язку із зовнішніми міжвідомчими базами даних, при цьому трафік суворо ізольований від паспортного сектора (VLAN 20);

– VLAN 40 (фінансово-господарський відділ) – сегмент підвищеної конфіденційності для роботи бухгалтерії (системи 1С, Клієнт-Банк). Реалізована повна логічна ізоляція від усіх інших робочих груп. Доступ до зовнішньої мережі дозволено лише за списком довірених IP-адрес фіскальних та банківських установ;

– VLAN 50 (загальний документообіг та канцелярія) – стандартний рівень доступу для загальних офісних завдань, використання системи електронного документообігу та внутрішньої пошти. У цьому ж сегменті розміщується спільна периферія (мережеві принтери та сканери), доступ до яких відкритий для інших підрозділів за необхідності;

– VLAN 60 (система відеоспостереження) – повністю ізольована мережа для IP-камер та серверів відеореєстрації. Такий підхід запобігає деградації продуктивності основної мережі через інтенсивний широкомовний трафік відеопотоків. Прямий вихід в Інтернет та доступ до робочих сегментів для цього VLAN заборонено;

– VLAN 70 (дирекція) – персоналізована підмережа для керівного складу підприємства з пріоритетним доступом до всіх корпоративних ресурсів.

– VLAN 90 (серверна інфраструктура та управління) – найбільш критичний сегмент, де зосереджені основні обчислювальні ресурси (AD, бази ЄДДР, файлові сервери). Управління мережею (SSH/HTTPS) дозволено лише в межах цього сегмента, а доступ із робочих VLAN жорстко регламентується міжмережевим екраном за принципом "мінімальних привілеїв".

Оскільки кожен VLAN функціонує як окрема логічна мережа, обмін даними між ними потребує маршрутизації. Ця функція покладена на комутатор ядра 3-го рівня (Layer 3 Switch), який виступає в ролі "шлюзу останньої надії" (Default Gateway) для кожної підмережі.

Така архітектура (Inter-VLAN Routing на апаратному рівні комутатора) дозволяє здійснювати пересилання пакетів на швидкості каналу, що мінімізує затримки всередині периметра. Водночас, міжмережевий екран FortiGate виконує роль інспектора на межі мережі та між найбільш критичними сегментами, здійснюючи глибокий аналіз пакетів (DPI) та фільтрацію трафіку згідно з політиками безпеки ДМС.

При формуванні планів IP-адресації для кожного сегмента мережі враховано необхідність виділення службової адреси для шлюзу за замовчуванням (Default Gateway). Ця адреса закріплюється за відповідним

віртуальним інтерфейсом (Switch Virtual Interface, SVI) на головному комутаторі 3-го рівня, що забезпечує можливість маршрутизації трафіку між сегментами. Повний розрахунок адресного простору для кожної підмережі, із врахуванням шлюзів та резервних адрес, систематизовано у таблиці 2.2.

Таблиця 2.2 – Розподіл необхідної кількості IP-адрес по VLAN

Назва	VLAN10	VLAN20	VLAN30	VLAN40	VLAN50	VLAN60	VLAN70	VLAN90
К-сть IP-адрес	3	19	10	6	6	11	3	3

Для ефективного використання адресного простору приватної мережі 192.168.0.0/24 та забезпечення безпеки через ізоляцію трафіку застосовано метод масок змінної довжини (VLSM). Цей підхід дозволяє виділяти підмережі такого розміру, який максимально відповідає реальній кількості хостів у кожному сегменті (VLAN).

Алгоритм планування IP-адресації розпочинається із впорядкування підмереж в порядку зменшення необхідної кількості IP-адрес.

Згідно даними таблиці 2.2, найбільшим сегментом є VLAN 20 (Паспортний відділ), який потребує 18 адрес для пристроїв та 1 для шлюзу – разом 19 адрес. Отже, для забезпечення даної кількості адрес потрібно виділити 5 бітів в сегменті адреси, що відповідає за хостову частину. Дане твердження виходить із математичної залежності $2^5=32$ (4 біти буде недостатньо $2^4=16<19$).

Враховуючи, що в октеті 8 біт, то для адреси підмережі залишається 3 біти (8-5=3). Отже, для маски, в байті три старших біти становлять 1. Отримуємо, число $2^5+2^6+2^5=224$. Маска підмережі буде

255.255.255.224

Отримаємо адресу підмережі VLAN20 – 192.168.0.0/27.

Діапазон IP-адрес становить: 192.168.0.1 – 192.168.0.30

Адреса 192.168.0.31 буде бродкестом даної мережі.

Виділимо останню адресу діапазону в якості шлюзу. Отже, шлюз даної підмережі 192.168.0.30.

Наступна по необхідній кількості адрес підмережа VLAN60 (камери відеоспостереження) із 11 адрес (10 адрес для пристроїв та 1 для шлюзу).

Отже, для забезпечення даної кількості адрес потрібно виділити 4 бітів в сегменті адреси, що відповідає за хостову частину. Дане твердження виходить із математичної залежності $2^4=16$ (3 біти буде недостатньо $2^3=8<11$).

Для адреси підмережі залишається 4 біти (8-4=4). Отже, для маски, в байті чотири старших біти становлять 1. Отримуємо, число $2^7+2^6+2^5+2^4=240$. Маска підмережі буде:

255.255.255.240

Отримаємо адресу підмережі VLAN60 – 192.168.0.32/28.

Діапазон IP-адрес становить: 192.168.0.33 – 192.168.0.46.

Шлюз даної підмережі 192.168.0.46 і бродкест – 192.168.0.47.

За цим ж алгоритмом слід розрахувати адресний простір для всіх інших підмереж. В таблиці 2.3 представлено повний план IP-адресації мережі УДМС.

Таблиця 2.3 – План IP-адресації підмереж мережі УДМС

Назва підм.	Необх. к-сть адрес	Адреса підмережі/маска	Діапазон адрес для вузлів	Шлюз	Широкосму-гова адреса
1	2	5	6	7	8
VLAN20	19	192.168.0.0/27 255.255.255.224	192.168.0.1 – 192.168.0.29	192.168.0.30	192.168.0.31
VLAN60	11	192.168.0.32/28 255.255.255.240	192.168.0.33 – 192.168.0.45	192.168.0.46	192.168.0.47
VLAN30	10	192.168.0.48/28 255.255.255.240	192.168.0.49 – 192.168.0.61	192.168.0.62	192.168.0.63
VLAN40	6	192.168.0.64/29 255.255.255.248	192.168.0.65 – 192.168.0.69	192.168.0.70	192.168.0.71
VLAN50	6	192.168.0.72/29 255.255.255.248	192.168.0.73 – 192.168.0.77	192.168.0.78	192.168.0.79
VLAN10	3	192.168.0.80/29 255.255.255.248	192.168.0.81 – 192.168.0.85	192.168.0.86	192.168.0.87

Продовження таблиці 2.3

1	2	5	6	7	8
VLAN70	3	192.168.0.88/29 255.255.255.248	192.168.0.89 – 192.168.0.93	192.168.0.94	192.168.0.95
VLAN90	3	192.168.0.96/29 255.255.255.248	192.168.0.97 – 192.168.0.101	192.168.0.102	192.168.0.103
Sw_Rout	2	192.168.0.104/30 255.255.255.252	192.168.0.105 – 192.168.0.106	-	192.168.0.107

Дана схема забезпечує стабільну роботу 53 основних вузлів та залишає понад 50% вільного простору в мережі 192.168.0.0/24 (адреси з 192.168.0.108 по 192.168.0..254) для майбутнього розширення інфраструктури без перепланування існуючих підмереж.

2.9 Тестування та налагодження мережі

Після завершення монтажу активного та пасивного обладнання настає етап верифікації системи. Цей процес підтверджує, що всі компоненти працюють коректно, відповідають технічному завданню та забезпечують необхідний рівень продуктивності й безпеки для об'єкта автоматизації.

Перш ніж подавати живлення на активне обладнання, необхідно підтвердити якість монтажу пасивних компонентів.

– за допомогою кабельних аналізаторів проводиться тестування на відсутність розривів, коротких замикань та перевірка коректності розкладки провідників (стандарти T568A/B).

– критичних ділянок проводиться вимірювання затухання, перехресних наведень та затримок. Це гарантує, що лінія здатна працювати на швидкості до 1 Гбіт/с;

– вимірювання оптичної потужності в дБм для підтвердження пропускної здатності WAN-каналів.

Наступним кроком є підготовка комутаторів та маршрутизаторів до роботи в логічній структурі підприємства.

– встановлення безпечних паролів, налаштування часу (NTP) та IP-адрес для управління;

– налаштування Access-портів для кінцевих користувачів у відповідних віртуальних мережах (VLAN) та Trunk-портів для передачі тегованого трафіку між пристроями за протоколом 802.1Q.

Тестування функціональності та продуктивності:

– використання утиліт ping та tracert для перевірки доступності шлюзів, серверів та зовнішніх ресурсів.

– за допомогою інструменту iPerf проводиться замір реальної швидкості передачі даних між ключовими вузлами.

– контроль роботи списків доступу (ACL) та стабільності VPN-тунелів для віддалених підрозділів.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з розгортання та налаштування доменного контролера

Для забезпечення централізованого управління обліковими записами, політиками безпеки (GPO) та доступом до ресурсів у мережі УДМС передбачено розгортання доменної інфраструктури. Роль основного контролера домену (Domain Controller) виконуватиме сервер під управлінням ОС Microsoft Windows Server 2025. Централізоване адміністрування здійснюватиметься через консоль Server Manager.

Першим етапом є підготовка серверної операційної системи. Адміністрування здійснюється через консоль Server Manager (див. рис. 3.1).

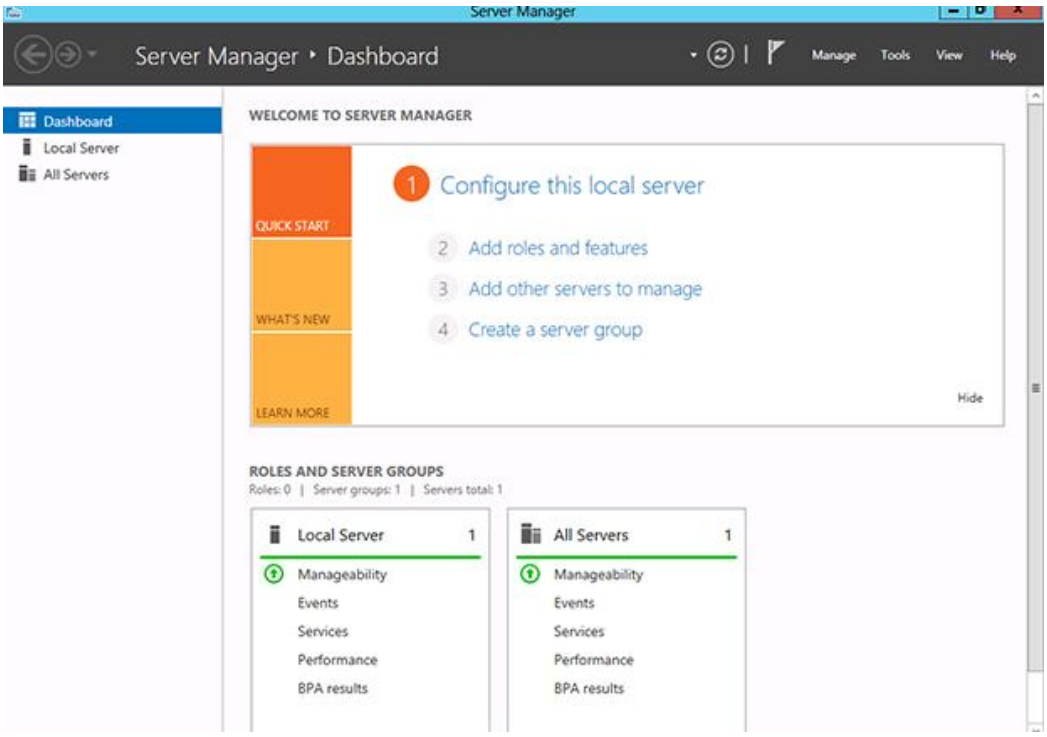


Рисунок 3.1 – Вікно Server Manger

Оскільки служби Active Directory (AD DS) залежать від системи доменних імен для локалізації ресурсів та маршрутизації клієнтських запитів, даний обчислювальний вузол інтегруватиме в собі також роль внутрішнього DNS-

сервера. З огляду на це, перед ініціалізацією служб каталогів необхідно виконати наступну підготовку мережевого інтерфейсу:

– серверу призначити статичну IP-адресу (192.168.0.97) згідно з планом адресації представленим в таблиці 2.3. Використання статичної адреси є архітектурною вимогою, оскільки зміна IP-адреси доменного контролера призведе до непрацездатності всієї інфраструктури;

– як основний DNS-сервер у налаштуваннях IPv4 вказати адресу 127.0.0.1. Це гарантує, що сервер використовуватиме власну локальну службу DNS після її інсталяції для реєстрації службових записів AD. Як резервний вказати публічний DNS (8.8.8.8) для резолвінгу зовнішніх імен;

– здійснити зміну автоматично згенерованого імені сервера на Servdomain відповідно до проєктних стандартів неймінгу.

Для призначення серверу статичної адреси, потрібно у розділі Local Server → Ethernet Properties встановити наступні параметри протоколу TCP/IPv4:

– IP-адреса – 192.168.0.97 (згідно з планом адресації представленим в таблиці 2.3).

– маска підмережі – 255.255.255.248 (відповідно до розрахунків VLSM у розділі 2.8).

– шлюз (Gateway) – 192.168.0.102 (згідно з планом адресації);

– основний DNS – 127.0.0.1 (Loopback-адреса, що вказує серверу звертатися до власної бази записів DNS);

– альтернативний DNS: 8.8.8.8 (для забезпечення виходу в Інтернет).

Встановлення необхідного програмного забезпечення виконується через майстер Add Roles and Features:

– у меню Server Roles обрати компоненти Active Directory Domain Services та DNS Server.

– система автоматично запропонує встановити додаткові інструменти управління, такі як консолі PowerShell та оснастки AD, що є необхідним для повноцінної роботи адміністратора.

Після завершення встановлення у верхній частині Server Manager з’явиться сповіщення з посиланням Promote this server to a domain controller. Натиснувши на нього, слід завантажити майстер конфігурації Active Directory Domain Services Configuration Wizard.

Оскільки розгортається домен мережі УДМС з нуля, то на першому етапі слід обрати опцію створення нового лісу (Add a new forest) і вказати доменне ім'я udms_te.local.

Вибір суфікса .local є стандартною практикою для ізольованих корпоративних мереж, що запобігає конфліктам із зовнішніми публічними доменами.

Наступне вікно конфігурації вимагає встановлення рівнів функціональності лісу та домену. Обирається найвищий доступний рівень — Windows Server 2025, що дозволяє використовувати сучасні методи шифрування Kerberos та покращені механізми захисту облікових записів. Тут же встановлюється пароль для режиму відновлення служб каталогів (DSRM), який є критично важливим для проведення аварійних робіт із базою даних NTDS.dit.

Під час перевірки системних вимог (Prerequisites Check) ігнорується попередження про делегування DNS, оскільки цей сервер є першим у структурі й сам стає авторитетним джерелом для зони udms_te.local. Після натискання кнопки «Install» сервер виконує фінальну скриптову обробку баз даних та автоматично перезавантажується для застосування змін.

Після того, як контролер домену був успішно розгорнутий, необхідно перейти до створення логічної структури об'єктів. Це виконується за допомогою оснастки Active Directory Users and Computers (ADUC), яку ми запускаємо через меню "Tools" у "Server Manager".

Першим кроком є створення Organizational Units (OU). Це контейнери, які дозволяють згрупувати об'єкти (користувачів, комп'ютери, групи) за функціональним або географічним принципом. Для УДМС слід створити створюємо ієрархію, що відображає реальну структуру управління.

У консолі ADUC слід натиснути правою кнопкою миші на домен udms_te.local, обрати New → Organizational Unit. Для забезпечення безпеки необхідно створити окремі OU для основних відділів:

– Administration – для керівництва та IT-спеціалістів;

– PassportService – для працівників паспортного сектору;

– Accounting – для відділу бухгалтерії;

– Computers – окремий контейнер для робочих станцій працівників (це дозволить застосовувати різні політики безпеки до комп'ютерів різних відділів).

Коли основа мережі створена, слід перейти до реєстрації персоналу. Процес створення користувача в кожному OU виглядає наступним чином:

– в обраному OU необхідно вибрати New → User;

– у вікні реєстрації заповнити поля First name, Last name та User logon name – це ім'я буде використовуватися для входу в систему;

– на етапі встановлення пароля ввести складний тимчасовий пароль, але обов'язково активувати опцію User must change password at next logon. Це ключовий елемент безпеки: адміністратор не знатиме особистого пароля працівника, а користувач буде змушений створити власний унікальний пароль під час першого входу.

Для того, щоб не призначати права доступу кожному користувачу окремо, слід створити Групи безпеки (Security Groups). Наприклад, створити групу G_Passport_Users у відповідному підрозділі:

– тип групи – Security;

– область дії (Group scope) – Domain Local.

Після створення групи слід додати створених користувачів до неї.

3.2 Інструкції з налаштування комутаційного обладнання та внутрішньої маршрутизації мережі

3.2.1 Інструкції з конфігурування комутаторів рівня доступу

Процес налаштування активних мережевих пристроїв розпочинається із конфігурування комутаторів, що відповідають за роботу конкретних сегментів інфраструктури. Спершу виконується налагодження комутатора робочих груп, який знаходиться у серверному приміщенні та забезпечує зв’язок для підмереж VLAN10 і VLAN70 (див. топологію у додатку В).

Робота з пристроєм розпочинається зі створення консольного підключення, після чого активується стандартний режим користувача. Процедура ідентифікації пристрою (присвоєння назви) здійснюється шляхом введення команд, перелік яких наведено на рисунку 3.2.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sw1
Sw1(config)#
```

Рисунок 3.2 – Встановлення назви комутатора

Після присвоєння пристрою ідентифікатора (ім'я), наступним важливим етапом є впровадження політики парольного захисту. Для комплексного обмеження несанкціонованого доступу необхідно налаштувати кілька рівнів безпеки [3]:

– пароль консольного порту – контролює фізичне підключення до пристрою через локальний інтерфейс керування;

– паролі віртуальних ліній (VTY/Telnet/SSH) – фільтрують спроби віддаленого адміністрування мережевого вузла через протоколи SSH або Telnet;

– пароль привілейованого режиму – обмежує доступ до команд високого рівня (enable mode), що дозволяють змінювати системні налаштування;

– глобальне шифрування паролів – спеціальна команда, що перетворює всі відкриті текстові паролі в конфігураційному файлі на зашифрований вигляд, посилюючи захист від перегляду конфігурації сторонніми особами.

Для захисту доступу до режиму розширених прав пріоритетним є використання команди: enable secret <пароль>.

Саме ця команда є стандартом безпеки, оскільки вона автоматично використовує стійкі алгоритми хешування для зберігання пароля, на відміну від застарілої команди enable password.

Процес захисту фізичного порту вимагає переходу до режиму конфігурування ліній. Спочатку обирається інтерфейс консолі, після чого призначається секретна комбінація командою password. Важливим кроком є застосування команди login, яка ініціює запит на перевірку автентичності під час спроби входу.

Детальний приклад синтаксису для налаштування консольного доступу та привілейованого режиму візуалізовано на рисунку 3.3.

```
Sw1(config)# enable secret Bezkorovaynyi
Sw1(config)#line console 0
Sw1(config-line)#password Bezkorovaynyi
Sw1(config-line)#login
Sw1(config-line)#exit
Sw1(config)#
```

Рисунок 3.3 – Встановлення парольного захисту на привілейований режим

Для гарантування безпеки під час віддаленого адміністрування комутатора через мережеві протоколи Telnet або SSH критично важливим є налаштування паролів на віртуальних термінальних лініях – VTY (Virtual Teletype). Ці логічні інтерфейси виступають основним бар'єром проти несанкціонованого зовнішнього входу в систему керування пристроєм [6].

Зазвичай мережеве обладнання підтримує багатоканальний доступ, що реалізується через групу ліній (як правило, у діапазоні від 0 до 15). Така конфігурація забезпечує можливість паралельної роботи кількох адміністра-

торів, дозволяючи їм одночасно здійснювати моніторинг або зміну параметрів пристрою з різних робочих станцій [6].

Повна послідовність команд, які застосовуються для інсталяції парольного захисту на інтерфейси віддаленого доступу, детально проілюстрована на рисунку 3.4.

```
Swl(config)#line vty 0 15
Swl(config-line)#password Bezkorovaynyi
Swl(config-line)#login
Swl(config-line)#transport input ssh
Swl(config-line)#exit
Swl(config)#service password-encryption
Swl(config)#exit
```

Рисунок 3.4 – Налаштування парольного захисту на відділений доступ по SSH

Команда transport input ssh є надзвичайно важливим елементом налаштування безпеки мережевого обладнання (комутаторів та маршрутизаторів). Вона визначає, які саме протоколи дозволені для встановлення віддаленого з'єднання з пристроєм через віртуальні лінії (VTY). Оскільки, з’єднання через Telnet є ненадійним, то даною командою воно буде заборонено, а дозволено лише більш надійне і шифроване SSH-з’єднання.

Окрім цього, для посилення загального захисту системи застосовується глобальна команда service password-encryption. Вона дозволяє автоматично перетворити всі паролі, що зберігаються у файлі конфігурації у відкритому текстовому форматі, на зашифровані хеш-послідовності.

У наведеній інструкції, як приклад, використовується пароль "Bezkorovaynyi". Для реальної роботи в мережевому середовищі цей пароль необхідно замінити на складну та надійну комбінацію символів, яка відповідає корпоративним стандартам безпеки.

Заключним етапом налаштування є створення облікового запису користувача для авторизації через SSH. Відповідний синтаксис та послідовність команд для генерації локальної бази користувачів наведено на рисунку 3.5.

```
Sw1(config)#username root privilege 15 secret Bezkorovaynyi
Sw1(config)#ip domain name udms_te.local
Sw1(config)#crypto key generate rsa
The name for the keys will be: Sw1.udms_te.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 256
% A decimal number between 360 and 4096
How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

Рисунок 3.5 – Додавання користувача для віддаленого доступу по SSH

Наступним етапом конфігурування є розгортання структури VLAN на кожному з наявних комутаторів. Створення VLAN є обов'язковою умовою для розмежування широкомовних доменів та забезпечення ізоляції трафіку між різними групами користувачів у межах однієї фізичної інфраструктури.

Цей процес передбачає створення логічних сегментів мережі згідно з архітектурою проекту. Вичерпний перелік ідентифікаторів (номерів) та відповідних назв для всіх підмереж, що підлягають налаштуванню, деталізовано у таблиці 3.1, а розташування відділів на додатку А.

Таблиця 3.1 – Ідентифікатори, призначення та назви віртуальних підмереж

Розташування підмережі	Назва VLAN	Номер VLAN
IT-відділ. Адміністрування мережі	VLAN10	10
Паспортно-реєстраційний сектор	VLAN20	20
Громадянство та імміграція	VLAN30	30
Фінансово-господарський відділ	VLAN40	40
Загальний документообіг та канцелярія	VLAN50	50
Система відеоспостереження	VLAN60	60
Дирекція. Директор та секретар	VLAN70	70
Серверна інфраструктура (В серверній)	VLAN90	90
З’єднання роутера (міжмережного екрану) із головним комутатором	SWG_Router	80

Процедура ініціалізації VLAN на комутаційному обладнанні розпочинається з активації режиму глобального конфігурування. Безпосереднє створення нового логічного сегмента виконується за допомогою директиви vlan <номер>, де в ролі аргументу виступає унікальний числовий ідентифікатор мережі, представлений в таблиці 3.1.

Для зручності подальшого адміністрування та ідентифікації трафіку кожній новоствореній VLAN призначається текстова мітка (описова назва) через команду name <назва> [3].

Повний синтаксис та послідовність виконання цих операцій на прикладі комутатора Sw1 (див. додаток Б) наведено як приклад на рисунку 3.6.

```
Sw1(config)#vlan 10
Sw1(config-vlan)#name vlan10
Sw1(config-vlan)#vlan 20
Sw1(config-vlan)#name vlan20
Sw1(config-vlan)#vlan 30
Sw1(config-vlan)#name vlan30
Sw1(config-vlan)#vlan 40
Sw1(config-vlan)#name vlan40
Sw1(config-vlan)#vlan 50
Sw1(config-vlan)#name vlan50
Sw1(config-vlan)#vlan 60
Sw1(config-vlan)#name vlan60
Sw1(config-vlan)#vlan 70
Sw1(config-vlan)#name vlan70
Sw1(config-vlan)#vlan 80
Sw1(config-vlan)#name SWG_Router
Sw1(config-vlan)#vlan 90
Sw1(config-vlan)#name vlan90
Sw1(config-vlan)#exit
Sw1(config)#
```

Рисунок 3.6 – Додавання віртуальних мереж у базу даних на комутаторі Sw1

Завершивши формування віртуальних мереж (VLAN), необхідно перейти до визначення функціональних ролей портів комутатора, що є базовою умовою їхньої правильної роботи. У мережевій архітектурі виділяють два ключові типи інтерфейсів [6]:

– Access-порти (порти доступу) – призначені для прямого підключення периферійного обладнання (ПК, принтери тощо);

– Trunk-порти (магістральні порти) – використовуються для організації каналів зв'язку між комутаторами або для з'єднання з маршрутизатором, забезпечуючи передачу трафіку декількох VLAN одночасно.

Спираючись на топологічну схему (див. додаток Б), процедура налаштування інтерфейсів комутатора Sw1 виконується в режимі глобальної конфігурації. Зокрема, uplink-порт пристрою Sw1 має бути переведений у транковий режим, оскільки через нього здійснюється обмін даними з маршрутизатором. Детальний перелік команд, використаних для базового налаштування портів Sw1, наведено на рисунку 3.7.

```
Sw1(config)#interface range gigabitethernet0/1-gigabitethernet3/1
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#interface range gigabitethernet0/1-gigabitethernet1/1
Sw1(config-if-range)#switchport access vlan 10
Sw1(config-if-range)#interface range gigabitethernet2/1-gigabitethernet3/1
Sw1(config-if-range)#switchport access vlan 70
Sw1(config-if)#interface gigabitethernet1/1/1
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk allowed vlan 70,10
Sw1(config-if)#exit
Sw1(config)#
```

Рисунок 3.7 – Налаштування інтерфейсів комутатора Sw1

Додатковий рівень безпеки на рівні доступу (Layer 2) забезпечується за допомогою технології Port Security. Це критично важливий аспект налаштування комутаторів, який дозволяє обмежити доступ до мережі на основі MAC-адрес кінцевих пристроїв.

Замість того, щоб залишати порти відкритими для будь-якого підключення, Port Security дозволяє адміністратору контролювати, хто саме має право передавати трафік через конкретний інтерфейс.

Можна встановити максимальну кількість MAC-адрес (наприклад, тільки одну), які дозволені на порту. Це запобігає підключенню несанкціонованих хабів або комутаторів до робочих місць.

Типи вивчення MAC-адрес:

– Static – адреса прописується вручну адміністратором;

– Dynamic – комутатор запам'ятовує першу адресу, яка з'явилася в мережі, але видаляє її після перезавантаження.

– Sticky (липкі адреси) – комутатор вивчає адресу динамічно і автоматично зберігає її в поточному файлі конфігурації (running-config). Це найзручніший метод для швидкого налаштування безпеки.

Якщо до порту підключиться пристрій з невідомою MAC-адресою або буде перевищено ліміт адрес, комутатор може діяти за одним із трьох сценаріїв:

– Shutdown – порт негайно вимикається (переходить у стан error-disabled), надсилається повідомлення в лог (SNMP), а світлодіод на порту стає помаранчевим. Щоб увімкнути його знову, адміністратор має вручну ввести shutdown / no shutdown;

– Restrict – порт залишається активним, але трафік від порушника відкидається. Комутатор генерує повідомлення про порушення та збільшує лічильник інцидентів;

– Protect – трафік від невідомих адрес просто блокується, але жодних сповіщень чи записів у лог не створюється.

Для активації захисту на порті доступу використовуються команди представлені на рисунку 3.8.

```
Sw1(config)#interface range gigabitethernet0/1-gigabitethernet3/1
Sw1(config-if-range)#switchport port-security
Sw1(config-if-range)#witchport port-security maximum 1
Sw1(config-if-range)#switchport port-security mac-address sticky
Sw1(config-if-range)#switchport port-security violation shutdown
Sw1(config-if-range)#exit
Sw1(config)#
```

Рисунок 3.8 – Налаштування захисту портів

Аналогічні операції з конфігурування слід виконати для пристроїв Sw2 – Sw6 та SwG. При цьому необхідно враховувати специфіку кожного вузла, вказуючи відповідні ідентифікатори інтерфейсів та номери VLAN згідно з даними, наведеними в таблиці 3.2.

Таблиця 3.2 – Налаштування інтерфейсів комутаторів рівня доступу

Назва	Інтерфейси комутатора	Типи портів	Команда визначення інтерфейсу	Port Security
Sw1	GigabitEthernet0/1 – GigabitEthernet1/1	access	switchport access vlan 10	Gig0/1 – Gig3/1
	GigabitEthernet2/1 – GigabitEthernet3/1	access	switchport access vlan 70	
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 10,70	
Sw2	GigabitEthernet0/1 – GigabitEthernet18/1	access	switchport access vlan 20	Gig0/1 – Gig18/1
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 20	
Sw3	GigabitEthernet0/1 – GigabitEthernet8/1	access	switchport access vlan 30	Gig0/1 – Gig8/1
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 30	
Sw4	GigabitEthernet0/1 – GigabitEthernet4/1	access	switchport access vlan 40	Gig0/1 – Gig4/1
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 40	
Sw5	GigabitEthernet0/1 – GigabitEthernet4/1	access	switchport access vlan 50	Gig0/1 – Gig4/1
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 50	
Sw6	GigabitEthernet0/1 – GigabitEthernet9/1	access	switchport access vlan 60	Gig0/1 – Gig9/1
	GigabitEthernet1/1/1	trunk	switchport trunk allowed vlan 60	
SwG	GigabitEthernet1/1/1	access	switchport access vlan 80	Gig1/1/1, Gig1/0/1, – Gig1/0/1
	GigabitEthernet1/0/1, GigabitEthernet1/0/2	access	switchport access vlan 90	
	GigabitEthernet1/0/3	trunk	switchport trunk allowed vlan 10,70	
	GigabitEthernet1/0/4	trunk	switchport trunk allowed vlan 20	
	GigabitEthernet1/0/5	trunk	switchport trunk allowed vlan 30	
	GigabitEthernet1/0/6	trunk	switchport trunk allowed vlan 40	
	GigabitEthernet1/0/7	trunk	switchport trunk allowed vlan 50	
	GigabitEthernet1/0/8	trunk	switchport trunk allowed vlan 60	

Для того, щоб усі поточні налаштування комутаторів залишилися активними після планового або аварійного перезавантаження пристрою, необхідно перенести їх із оперативної пам'яті в енергонезалежну. Це реалізується за допомогою директиви “copy running-config startup-config” [6].

Виконання цієї команди гарантує стабільність роботи мережі, запобігаючи скиданню параметрів до заводських налаштувань або попередніх станів. Альтернативним варіантом для швидкого збереження є команда write memory або скорочено wr [6].

3.2.2 Інструкції з налаштування головного комутатора

Налаштування комутатора 3-го рівня (L3 Switch) для маршрутизації між VLAN (Inter-VLAN routing) – це важливий етап, який дозволяє пристрою не лише комутувати трафік всередині мережі, а й виступати шлюзом для передачі даних між різними підмережами.

На початковому етапі потрібно налаштувати назву пристрою, парольний захист та типи портів для комутації та захист портів рівня доступу. Інструкція даного етапу налаштування комутатора описано в рорділі 3.1.

Наступний етап – налаштування на головному комутаторі маршрутизації між VLAN.

За замовчуванням більшість комутаторів L3 працюють як звичайні пристрої 2-го рівня. Щоб увімкнути логіку маршрутизатора, необхідно ввести команду: ip routing.

Без цієї команди пристрій не буде пересилати пакети між різними інтерфейсами, навіть якщо вони налаштовані правильно.

Для того, щоб комутатор став шлюзом за замовчуванням (Default Gateway) для пристроїв у кожній VLAN, необхідно створити віртуальні інтерфейси та призначити їм IP-адреси. При цьому IP-адреси віртуальних портів повинні відповідати адресам шлюзів із відповідних віртуальних підмереж, представлені в таблиці 2.3. Для цього необхідно ввести команди представлені на рисунку 3.9.

```
Switch(config)#ip routing
Switch(config)#interface Vlan10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

Switch(config-if)#description IT
Switch(config-if)#ip address 192.168.0.86 255.255.255.248
Switch(config-if)#interface Vlan20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#description Passport_reestr
Switch(config-if)#ip address 192.168.0.30 255.255.255.224
Switch(config-if)#interface Vlan30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#description Gromad_reecstracia
Switch(config-if)#ip address 192.168.0.62 255.255.255.240
Switch(config-if)#interface Vlan40
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

Switch(config-if)#description Finanace
Switch(config-if)#ip address 192.168.0.70 255.255.255.248
Switch(config-if)#interface Vlan50
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

Switch(config-if)#description Documentoobig
Switch(config-if)#ip address 192.168.0.78 255.255.255.248
Switch(config-if)#interface Vlan60
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

Switch(config-if)#description Videonaglyad
Switch(config-if)#ip address 192.168.0.46 255.255.255.240
Switch(config-if)#interface Vlan70
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan70, changed state to up

Switch(config-if)#description Directore
Switch(config-if)#ip address 192.168.0.94 255.255.255.248
Switch(config-if)#interface Vlan80
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan80, changed state to up

Switch(config-if)#description SwitchG Router
Switch(config-if)#ip address 192.168.0.106 255.255.255.252
Switch(config-if)#interface Vlan90
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan90, changed state to up

Switch(config-if)#description Server
Switch(config-if)#ip address 192.168.0.102 255.255.255.248
Switch(config-if)#exit
Switch(config)#
```

Рисунок 3.9 – Ввімкнення маршрутизації та налаштування віртуальних портів на головному комутаторі

Оскільки, вихід із локальної мережі до провайдера здійснюється через міжмережевий екран (маршрутизатор), який є шлюзом, головний комутатор повинен знати, що весь невідомий трафік (наприклад, запити в інтернет) потрібно відправляти на IP-адресу фаєрвола у VLAN 80. Для цього слід ввести команду маршруту за замовчуванням представлену на рисунку 3.10.

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.105
Switch(config)#
```

Рисунок 3.10 – Встановлення маршруту за замовчуванням на головному комутаторі

3.3 Інструкції з налаштування маршрутизатора та VPN-тунелів

Налаштування маршрутизатора є фінальним етапом розгортання мережі. Цей пристрій забезпечує вихід у глобальну мережу Інтернет та організовує захищені VPN-тунелі для зв'язку з територіальними підрозділами ДМС у Тернопільській області..

Першочерговим завданням перед конфігуруванням мережевих інтерфейсів є присвоєння маршрутизатору унікальної назви (hostname). Для цього застосовується той самий набір команд, що й під час налаштування комутаторів робочих груп (детальніше див. рис. 3.2.1).

Крім цього, дуже важливо забезпечити безпеку пристрою, впровадивши систему парольного захисту. Також необхідно створити персональний обліковий запис адміністратора для організації захищеного дистанційного керування через протокол SSH. Відповідні синтаксичні конструкції та приклади виконання цих операцій задокументовані на рисунках 3.3 – 3.5.

Після базового захисту слід перейти до налаштування портів згідно з схемою представленою в додатку Г. Маршрутизатор/фаєрвол FortiGate FG-100F під’єднання до двох провайдерів та ще один інтерфейс до головного комутатора:

–

– основний провайдер (ISP1) – підключений через GigabitEthernet1/0 (адреса 100.100.100.2/30);

– резервний провайдер (ISP2) – підключений через GigabitEthernet2/0 (адреса 200.200.200.2/30);

– внутрішня мережа (LAN) – інтерфейс GigabitEthernet0/0 з'єднує маршрутизатор із головним комутатором SwG (адреса 192.168.0.105/30);.

Для того, щоб пристрої з внутрішніх VLAN (див. таблицю 2.3) могли виходити в інтернет, необхідно активувати механізм NAT (Network Address Translation). При цьому необхідно спочатку визначити типи портів на маршрутизаторі як внутрішні та зовнішні.

Внутрішній порт (інтерфйс GigabitEthernet0/0) під'єднаний до головного комутатора для нього слід задати команду "ip nat inside'.

Зовнішні інтерфейси під'єднують маршрутизатор до основного та резервного провайдерів Інтернет. Для них слід задати команду "ip nat outside'.

Для налаштування інтерфейсів маршрутизатора/файєрвола слід ввести команди представлені на рисунку 3.11.

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)#description trunk to SWG
R1(config-if)#ip address 192.168.0.105 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ip nat inside
R1(config-if)#interface GigabitEthernet1/0
R1(config-if)#description PRIMARY_ISP
R1(config-if)#ip address 100.100.100.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ip nat outside
R1(config-if)#interface GigabitEthernet2/0
R1(config-if)#description BACKUP_ISP
R1(config-if)#ip address 200.200.200.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
```

Рисунок 3.11 – Встановлення налаштувань інтерфейсів міжмережевого екрану

Оскільки головний комутатор виконує маршрутизацію між внутрішніми підмережами і в розділі 3.1.2 налаштуоано маршру за замовчуванням для виходу в Інтрнет, фаєрвол повинен знати, як повернути пакет назад у підмережі.

На маршрутизаторі-фаєрволі необхідно прописати статичні маршрути до всіх внутрішніх мереж, відповідно до даних таблиця 2.3, через IP-адресу комутатора (див. рис. 3.12).

```
R1(config)#ip route 192.168.0.0 255.255.255.224 192.168.0.106
R1(config)#ip route 192.168.0.32 255.255.255.240 192.168.0.106
R1(config)#ip route 192.168.0.48 255.255.255.240 192.168.0.106
R1(config)#ip route 192.168.0.64 255.255.255.248 192.168.0.106
R1(config)#ip route 192.168.0.72 255.255.255.248 192.168.0.106
R1(config)#ip route 192.168.0.80 255.255.255.248 192.168.0.106
R1(config)#ip route 192.168.0.88 255.255.255.248 192.168.0.106
R1(config)#ip route 192.168.0.96 255.255.255.248 192.168.0.106
R1(config)#
```

Рисунок 3.12 – Налаштування статичної маршрутизації на файєрволі

Наступним етапом побудови відмовостійкої мережі є конфігурування системи NAT. Ця технологія забезпечує безпечний вихід користувачів внутрішніх сегментів у глобальну мережу, дозволяючи багатьом вузлам локальної інфраструктури спільно використовувати обмежену кількість публічних IP-адрес. Окрім економії адресного простору, NAT виконує захисну функцію, маскуючи топологію приватної мережі від зовнішніх загроз.

При визначені інтерфейсів вже вказано які із портів будуть внутршіні та зовнішні, тому наступним етапом буде створення списків доступу (ACL), щоб NAT "розумів", які саме пристрої випускати в інтернет. Для цього використовується команда access-list.

Насамперед необхідно ідентифікувати внутрішні мережі, для цього слід створити список, який включає всі ваші VLAN (від 10 до 90). Зручно використати один запис, що охоплює весь діапазон адрес 192.168.0.0/24.

Після цього слід створити правила трансляції для обох провайдерів, використавши ключове слово overload (також відоме як PAT), щоб дозволити багатьом внутрішнім пристроям виходити через одну зовнішню IP-адресу.

Повний перелік команд для налаштування NAT представлена на рисунку 3.13.

```
R1(config)#access-list 100 permit ip 192.168.0.0 0.0.0.255 any
R1(config)#ip nat inside source list 100 interface GigabitEthernet1/0 overload
R1(config)#ip nat inside source list 100 interface GigabitEthernet2/0 overload
R1(config)#
```

Рисунок 3.13 – Налаштування NAT

Обидва NAT будуть працювати, але маршрутизатор буде використовувати той канал до провайдера, для якого активний маршрут за замовчуванням. Тому далі необхідно задати маршрут за замовчуванням для основного провайдера, вказавши параметр track 1. Для резервного провайдера слід вказати пріоритет 10.

Для забезпечення автоматичного перемикання на резервний канал, коли основний провайдер (ISP1) фізично працює (порт «Up»), але фактично не надає доступ до Інтернету, використовується механізм IP SLA (Service Level Agreement) у поєднанні з Object Tracking.

Механізм IP SLA дозволяє маршрутизатору генерувати тестовий трафік (наприклад, ICMP-запити до надійних вузлів у мережі, таких як Google DNS — 8.8.8.8) для перевірки реальної якості та доступності каналу. Якщо відгук не надходить протягом визначеного часу, маршрутизатор вважає канал непрацездатним. Повний перелік команд налаштавання маршрутів за замовчуванням та IP SLA представлено на рисунку 3.14.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 100.100.100.1 1
R1(config)#ip route 0.0.0.0 0.0.0.0 200.200.200.1 10
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 8.8.8.8 source-interface GigabitEthernet1/0
R1(config-ip-sla-echo)# exit
R1(config)#ip sla schedule 1 life forever start-time now
R1(config)#track 1 ip sla 1 reachability
```

Рисунок 3.14 – Налаштування моніторингу каналу зв’язку із провайдером

Команда “ip sla schedule” активує створену операцію (1) негайно (start-time now) і на необмежений термін (life forever).

Наступна команда “track 1 ip sla 1 reachability” стежить за результатом операції SLA. Якщо reachability (доступність) зникає, статус об'єкта track 1

змінюється на Down. Щоб ця система реально перемикала Інтернет, необхідно прив'язати об'єкт track до основного маршруту за замовчуванням.

Для забезпечення конфіденційного обміну даними між девєятьма територіально віддаленими офісами та центральним вузлом через публічну мережу Інтернет реалізується побудова віртуальних приватних мереж (VPN). Дані тунелі дозволяють логічно об'єднати віддалені філії в єдину захищену інфраструктуру.

Для функціонування VPN-каналів виділено наступні адресні простори з маскою /30: 192.168.0.108, 192.168.0.112, 192.168.0.116, 192.168.0.120, 192.168.0.124, 192.168.0.128, 192.168.0.132, 192.168.0.136.

Процес налаштування розпочинається з ініціалізації віртуального інтерфейсу Tunnel 1 на центральному маршрутизаторі R1. Згідно з проектними розрахунками, даному інтерфейсу призначається IP-адреса 192.168.0.109 (див. рис. 3.15).

```
R1(config)#interface tunnel 1

R1(config-if)#
%LINK-5-CHANGED: Interface Tunnel1, changed state to up

R1(config-if)#ip address 192.168.0.193 255.255.255.252
R1(config-if)#tunnel source gigabitethernet0/0/0
R1(config-if)#tunnel destination 178.99.18.20
R1(config-if)#exit
R1(config)#
```

Рисунок 3. 15 – Налаштування віртуального тунелю на маршрутизаторі R1

Згідно з наведеною схемою (рис. 3.16), публічна IP-адреса 178.99.18.20 закріплена за зовнішнім інтерфейсом маршрутизатора, який розташований у віддаленому офісі.

Далі слід перейти на маршрутизатор віддаленого офісу і ввести налаштування аналогічні до представлених на рисунку 3.16 але в якості адреси другого інтерфейсу в тунелі вказати адресу зовнішнього інтерфейсу головного маршрутизатора (100.100.100.2).

Подібним чином необхідно налаштувати тунелі для інших віддалених офісів. Повний перелік IP-адрес представлено в таблиці 3.3.

Таблиця 3.3 – Адреси фізичних та віртуальних інтерфейсів у VPN-тунелях

Нгомер тунелю	Віддалений офіс	Фізичні IP-адреси на маршрутизаторах		IP-адреси VPN	
		клієнт	сервер	клієнт	сервер
1	1	178.99.10.20	100.100.100.2	192.168.0.110	192.168.0.109
2	2	178.119.12.21	100.100.100.2	192.168.0.114	192.168.0.113
3	3	145.131.14.118	100.100.100.2	192.168.0.118	192.168.0.117
4	4	105.103.11.18	100.100.100.2	192.168.0.118	192.168.0.117
5	5	195.132.114.11	100.100.100.2	192.168.0.122	192.168.0.121
6	6	134.122.14.11	100.100.100.2	192.168.0.126	192.168.0.125
7	7	155.132.14.110	100.100.100.2	192.168.0.130	192.168.0.129
8	8	141.131.14.2	100.100.100.2	192.168.0.134	192.168.0.133
9	9	199.11.114.2	100.100.100.2	192.168.0.138	192.168.0.137

Керуючись розрахунками з таблиці 3.3 здійснюється конфігурування віртуальних інтерфейсів VPN-тунелів на периферійних маршрутизаторах R2, R3, R2, R4, R5, R6, R7, R8, R9 та R10. Це забезпечує кінцеву точку зв'язку з боку територіальних підрозділів.

Після формування базової тунельної інфраструктури (GRE), необхідно забезпечити належний рівень конфіденційності даних. Оскільки стандартні тунелі не мають вбудованих механізмів шифрування, поверх них розгортається протокол IPSec. У даному проекті обрано транспортний режим функціонування IPSec, який дозволяє інкапсулювати корисне навантаження вище мережевого рівня моделі OSI, зберігаючи оригінальний IP-заголовок без змін.

Процес впровадження IPSec реалізується у два послідовні етапи на обох вузлах зв'язку.

Перший етап – налаштування політик ISAKMP: на даному етапі в режимі глобальної конфігурації визначаються параметри безпеки та створюється відповідна політика. Детальний перелік команд для цього етапу наведено на рисунку (див. рис. 3.16).

```
RG(config)#crypto isakmp policy 1
RG(config-isakmp)#encryption 3des
RG(config-isakmp)#hash md5
RG(config-isakmp)#authentication pre-share
RG(config-isakmp)#group 2
RG(config-isakmp)#lifetime 86400
RG(config-isakmp)#exit
RG(config)#crypto isakmp key chudoostriv address 178.98.17.101
RG(config)#
```

Рисунок 3.16 – Налаштування політики ISAKMP

Згідно з конфігурацією, наведеною на рисунку 3.17, для забезпечення конфіденційності обрано алгоритм симетричного блочного шифрування 3DES, а цілісність даних гарантується використанням хеш-функції MD5. Процедура автентифікації базується на застосуванні попередньо узгодженого спільного ключа (pre-shared key).

Для генерації секретних ключів активовано другу групу алгоритму Діффі-Геллмана, а параметр lifetime регламентує часовий інтервал дії сеансового ключа. У процесі налаштування встановлено ідентифікатор ключа «chudoostriv», який прив'язано до публічної IP-адреси віддаленого шлюзу (згідно з табл. 3.3). Критично важливою умовою є ідентичність цього ключа на обох сегментах VPN-тунелю.

Переходячи до другої фази налаштування IPsec, формується набір перетворень (Transform Set), що отримав назву «TS». Даний набір визначає конкретні методи захисту корисного навантаження (див. рис. 3.17). Ще одним етапом є переведення IPsec у транспортний режим, що оптимізує роботу тунелю.

```
RG(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
RG(cfg-crypto-trans)# mode transport
RG(cfg-crypto-trans)# exit
```

Рисунок 3.17 – Налаштування траснпортного режиму роботи IPSec

Заключним етапом конфігурування захищеного каналу є інтеграція IPsec із GRE-тунелем за допомогою механізму Crypto Map. У даному проекті створюється криптографічна карта з ідентифікатором MY_CRYPTO_MAP та

індексом пріоритетності 10. Використання порядкових номерів дозволяє маршрутизатору послідовно обробляти декілька записів у межах однієї карти.

Процес налаштування, деталізований на рисунку 3.18, передбачає перехід у режим специфічної конфігурації Crypto Map. На цьому етапі визначається IP-адреса віддаленого вузла (peer) – 178.98.17.101, яка згідно з таблицею 3.3 є публічною адресою шлюзу на протилежному боці VPN-тунелю. Фінальним кроком є асоціація раніше створеного набору перетворень (Transform Set) із даною криптографічною картою.

```
RG(config)#crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RG(config-crypto-map)#set peer 178.98.17.101
RG(config-crypto-map)#set transform-set MY_TRANS_SET
```

Рисунок 3.18 – Налаштування Crypto Map

Для коректного функціонування схеми GRE over IPsec необхідно забезпечити криптографічний захист саме того GRE-трафіку, що передається між публічними інтерфейсами маршрутизаторів. З цією метою створюється спеціалізований список контролю доступу (ACL), який ідентифікує пакети протоколу GRE (номер протоколу 47), що курсують між адресами, вказаними у таблиці 2.6.

Після визначення трафіку в ACL, виконується фінальне налаштування об'єкта Crypto Map: створений список доступу прив'язується до криптографічної карти, яка, у свою чергу, активується на фізичному зовнішньому інтерфейсі маршрутизатора.

Після завершення конфігурування першого вузла, аналогічні налаштування впроваджуються на другому маршрутизаторі тунелю. При цьому забезпечується дзеркальність параметрів безпеки: у команді crypto isakmp key як цільова адреса вказується публічний інтерфейс головного офісу – 100.100.100.2. Такий підхід гарантує успішну автентифікацію та встановлення захищеного з’єднання між обома точками VPN-каналу.

Аналогічний алгоритм розгортання шифрування та захисту даних застосовується для всіх інших віртуальних тунелів у мережі.

Після встановлення захищених VPN-каналів, для забезпечення повноцінного обміну даними між центральним офісом та всіма внутрішніми сегментами (VLAN) віддалених підрозділів, необхідно реалізувати схему статичної маршрутизації. Це дозволить маршрутизаторам коректно визначати шлях до цільових підмереж через створені логічні інтерфейси..

3.4 Інструкції по налаштуванню засобів захисту мережі

Захист активного мережевого обладнання є важливим фундаментом на кожному етапі життєвого циклу комп'ютерної мережі – від проєктування до щоденної експлуатації. Ігнорування безпекових протоколів створює вразливості, що можуть призвести до перехоплення трафіку, несанкціонованого керування пристроями та компрометації конфіденційних даних.

Відповідно до фахових рекомендацій [3], комплексна система захисту базується на таких механізмах:

– впровадження суворої політики ідентифікації та розмежування прав доступу (AAA);

– мінімізація «поверхні атаки» шляхом деактивації невикористовуваних сервісів та протоколів;

– превентивна активація інтегрованих модулів безпеки;

– встановлення жорстких лімітів на тривалість активних сесій адміністрування;

– налаштування системного логування та миттєвих сповіщень про критичні події.

У мережевій структурі УДМС в Тернопільській області реалізовано ешелоновану систему доступу до комутаторів та маршрутизаторів:

– консольний захист – унеможливлює несанкціонований вхід при фізичному підключенні до пристрою;

– захищений віддалений доступ (SSH). На відміну від протоколу Telnet, використання SSH забезпечує криптографічний захист сесій керування;

– пароль на привілейований режим створює додатковий бар'єр для доступу до конфігураційних налаштувань ядра мережі (параметри налаштування наведені в підрозділі 3.2.1).

Окрім базового захисту обладнання, для УДМС в Тернопільській області впроваджено розширений стек безпекових рішень:

– централізоване управління (Active Directory): реалізація принципу мінімальних привілеїв та впровадження вимог до складності паролів (12–14 символів) із регулярною ротацією;

– використання ліцензійного антивірусного ПЗ, активація локальних брандмауерів та контроль використання знімних носіїв;

– логічна ізоляція (VLAN та ACL). Сегментація мережі на рівні віртуальних локальних мереж та впровадження списків контролю доступу за принципом «явна заборона всього, що не дозволено»;

– стратегія 3-2-1): створення трьох копій даних на двох різних типах носіїв, одна з яких зберігається поза межами офісу;

– збір системних журналів (Syslog) для виявлення аномальної активності на ранніх стадіях;

– проведення регулярних тренінгів для персоналу щодо протидії фішингу та розробка протоколів реагування на інциденти.

Реалізація зазначеного комплексу заходів дозволяє створити в УДМС в Тернопільській області стійку до загроз, багаторівневу цифрову інфраструктуру, що гарантує цілісність даних та безперебійність державних сервісів.

3.5 Моделювання мережі

Практичне впровадження спроєктованої мережевої моделі здійснюється за допомогою інструментарію симулятора Cisco Packet Tracer. Алгоритм розгортання топології складається з наступних етапів.

Спочатку, використовуючи панель компонентів середовища, необхідно розмістити на робочій області всі передбачені специфікацією пристрої. Обрання відповідних типів кабелів (прямих чи перехресних) проводиться на панелі елементів. Для встановлення зв'язку виконується вибір конкретних фізичних портів на обох вузлах мережі. Комутація обладнання здійснюється з суворим дотриманням логічної схеми з'єднань, наведеної у додатку Б.

На другому етапі для кожної робочої станції необхідно викликати вікно налаштування пристрою і у меню Desktop застосунку IP Configuration впроваджуються параметри мережевого рівня. Зокрема, встановлюються статичні значення IPv4-адреси, маски підмережі та основного шлюзу згідно з розрахунковою таблицею 2.3. Для забезпечення коректної роботи доменних імен вказується адреса DNS-сервера – 192.168.0.97. Приклад налаштування вузла WS_1 (IT-відділ) візуалізовано на рисунку 3.19.

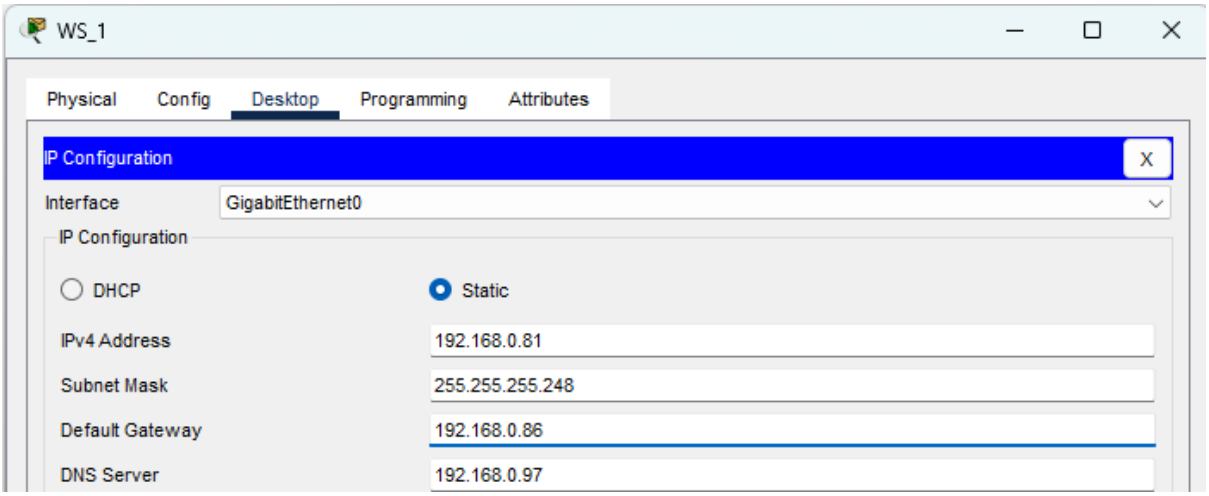


Рисунок 3.19 – Приклад налаштування IPv4 адреси робочій станції

Наступним етапом є конфігурування засобів візуального моніторингу. Для камер відеоспостереження встановлюються мережеві параметри, що відповідають виділеній віртуальній підмережі VLAN60 (згідно з даними таблиці 2.3). Щоб встановити налаштування необхіно відкрити вікно властивостей, вибрати вкладку Config, у лівій панелі розділ із інтерфейсом GigabitEthernet0 і вказати аресу та маску. Процес призначення статичних IP-адрес для камер безпеки ілюструється на рисунку 3.20.

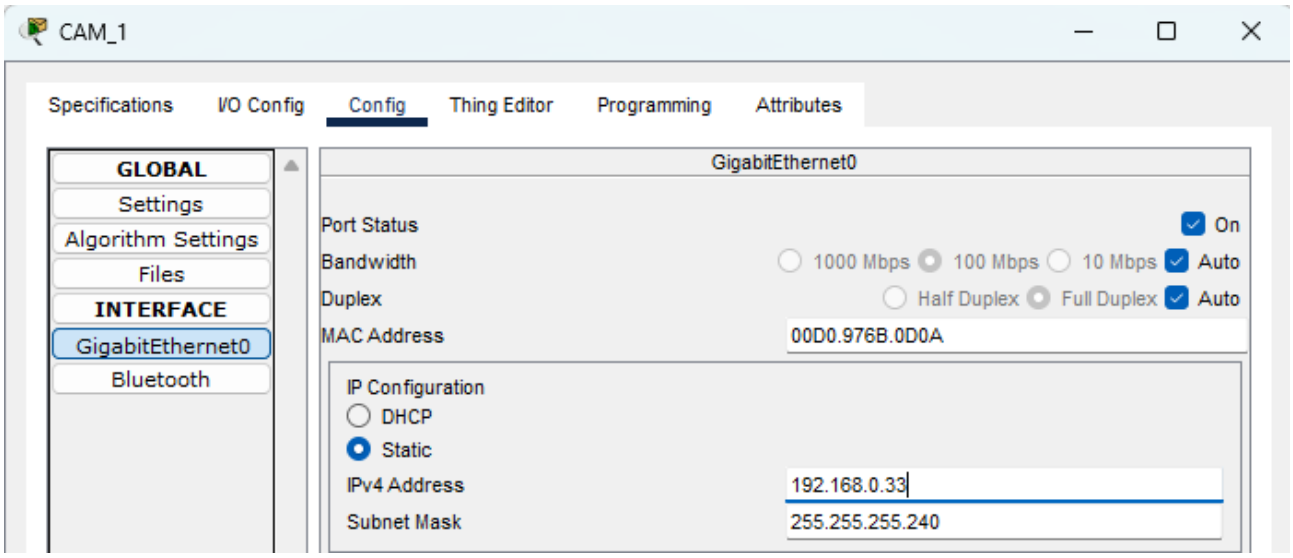


Рисунок 3.20 – Приклад налаштування IPv4 адреси камері відеоспостереження

Адресу шлюзу (для підмережі камер відеоспостереження 192.168.0.46), потрібно вказати в розділі Settings цієї ж вкладки Config.

Конфігурування активних компонентів інфраструктури, зокрема маршрутизаторів та комутаторів, реалізовано через консольний інтерфейс. Процес передбачає фізичне з'єднання термінального пристрою (ПК або ноутбука) з обладнанням за допомогою спеціалізованого кабелю Console (секція Connections у симуляторі). Детальний перелік команд та параметрів налаштування, що застосовувалися для підготовки обладнання до роботи, наведено у розділах 3.2 та 3.3. Загальна архітектура та фінальний вигляд спроєктованої мережі представлені у додатку Г.

3.5 Тестування роботи побудованої моделі мережі

Верифікація працездатності спроєктованої мережевої інфраструктури здійснювалася шляхом аналізу зв'язності між вузлами різних віртуальних сегментів (VLAN). Для первинної діагностики використано утиліту ping з робочої станції WS_1 (підмережа VLAN10). Детальний аналіз шляхів передавання трафіку проведено за допомогою команди tracert, що дозволило підтвердити коректне функціонування VPN-тунелів при взаємодії між віддаленими та центральним офісом.

Візуалізація динамічних процесів у середовищі Cisco Packet Tracer реалізована через режим Simulation. Результати проілюстровано на рисунку 3.21.

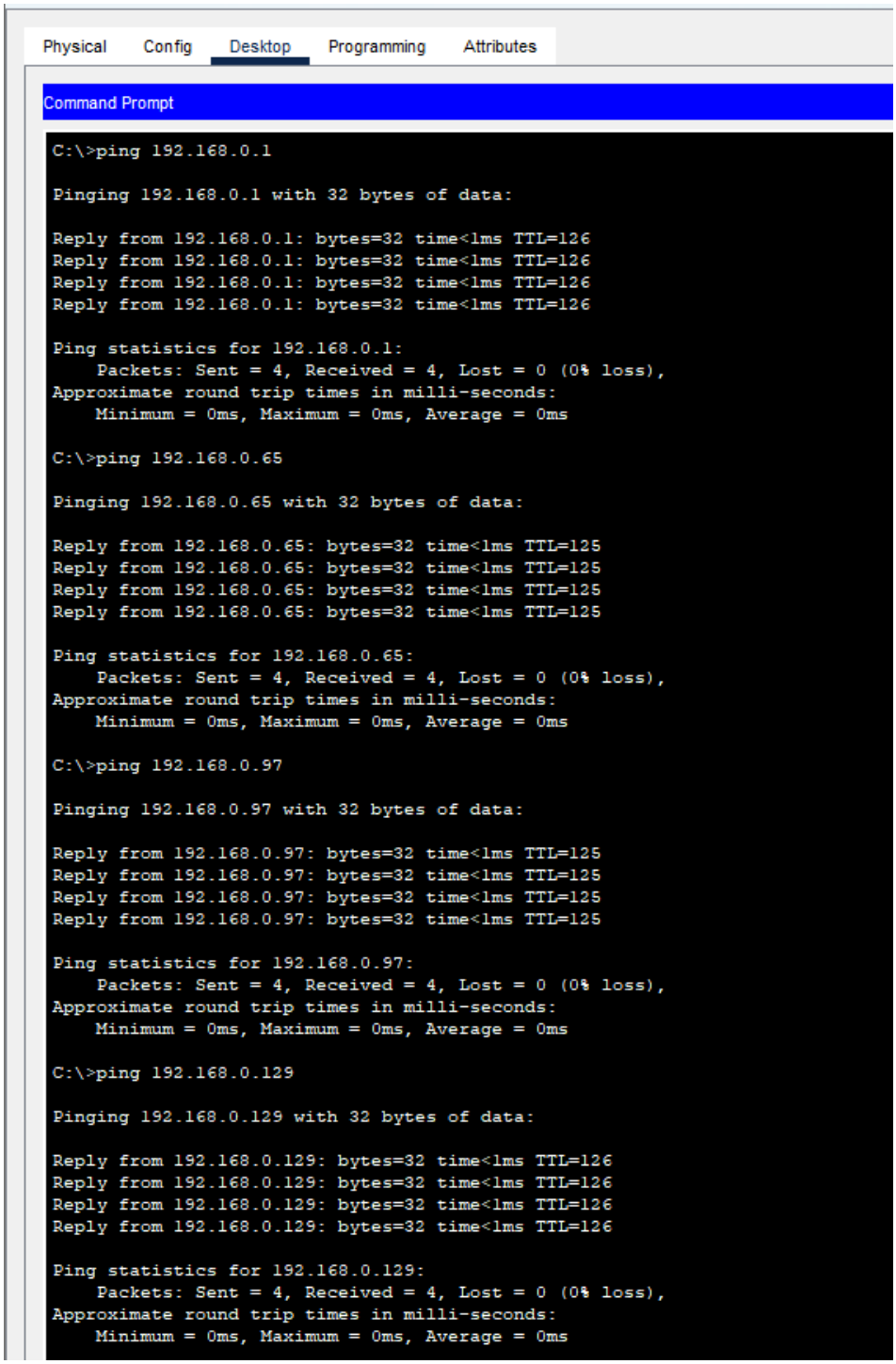


Рисунок 3.21 – Перевірка роботи мережі командою ping

Для проведення глибокого моніторингу траєкторії руху пакетів та ідентифікації часових затримок на кожному транзитному вузлі мережі застосовується утиліта tracert.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Розрахунок загального часового ресурсу, необхідного для реалізації науково-дослідної роботи (НДР), базується на детальному аналізі тривалості кожної стадії технологічного циклу. Відповідні відомості, що включають перелік етапів та їхню середню тривалість, систематизовано у таблиці 4.1. Процес моніторингу та верифікації часових витрат покладено на профільну робочу групу у складі керівника проєкту, провідного інженера та техніка.

Таблиця 4.1 – Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Постановка задачі, формування технічного завдання на проект локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проекту	15
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі УДМС в Тернопільській області. Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури УДМС для сегментування локальної мережі на підмережі.	Інженер	25

Продовження таблиці 4.1

1	2	3	4
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Технік	35
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	30
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
		Разом	110

Сумарний час виконання операцій технологічного процесу проектування мережі становить 110 години, з них 15 годин – робота керівника проекту, 60 години – інженера, 35 години – техніка.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці трактується як грошовий еквівалент вартості та ціни специфічного товару – робочої сили. Вона реалізується у вигляді винагороди, що виплачується роботодавцем персоналу за фактично виконаний обсяг робіт. Рівень індивідуального заробітку корелює з підсумковими показниками ефективності діяльності суб'єкта господарювання, підлягає державному оподаткуванню та не має встановленої верхньої межі.

Основна заробітна плата розраховується за формулою:

$$З_{осн} = Т_с \cdot К_г, \quad (4.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Виходячи з рекомендованих тарифних ставок встановимо таку ставку для керівник проекту – 270 грн, інженера – 200 грн./год. а для техніка – 150 грн./год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 15 \cdot 270 = 4050$ грн.
- інженера – $З_{осн2} = 60 \cdot 200 = 12000$ грн.
- техніка – $З_{осн3} = 35 \cdot 150 = 5250$ грн.

Сумарна основна заробітна плата становить

$$З_{осн}=4050 +12000 + 5250 =21300 \text{ грн.}$$

Додаткова заробітна плата становить 10 –15 % від суми основної заробітної плати.

$$З_{дод} = З_{осн} \cdot К_{допл}, \quad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам, 0,1– 0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника $З_{дод1}=4050 \cdot 0,12= 486$ грн.
- інженера $З_{дод1}=12000 \cdot 0,12= 1440$ грн.
- техніка $З_{дод3}=5250 \cdot 0,12= 630$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=414 + 1332 + 630 = 2556 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п} = З_{осн} + З_{дод} \quad (4.3)$$

Отже, загальні витрати на оплату праці становлять:

$$В_{о.п.}= 21300 + 2556 = 23856 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи. Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = ФОП \cdot 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з}= 23856 \cdot 0,22= 5248,32 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/	Категорія працівників	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн
		Тарифна ставка, грн.	К-сть відпрац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	270	15	4050	486	-	-
2	Інженер	200	60	12000	1440	-	-
3	Технік	150	35	5250	630	-	-
			Разом	21300	2556	5248,32	29104,32

Отже, загальні витрати на оплату праці становлять 29104,32 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{BI} = q_i \bullet P_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} \sum M_{B_i} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
2	Комутаційна шафа Hypernet WMNC-18U-FLAT	шт.	1	6580	6580
3	Комутаційна шафа Hypernet WMNC-3U-FLAT	шт.	5	2400	12000
4	Патчпанель 24 порти, кат. 6	шт.	6	1200	7200
5	Розетка RJ-45 (категорія 6)	шт.	41	120	4920
6	Роз’єм 8P8C (100 шт)	шт.	1	590	590
7	Короб (середня ціна)	м.	124	115	14260
8	Кабель UTP (кат. 6) (бухта)	шт.	2	5353	10706
9	Патчкорди (кат. 6)	шт.	41	56	2296
10	Патчкорди (оптоволокно)	шт.	3	85	255
11	Кабель опотоволоконний	м.	72	35	2520
12	Конектор SC	шт.	8	38	304
13	Гофрована трубка	м.	8	45	360
14	Міжмережевий екран FortiGate FG-100F	шт.	1	112 325	112325
15	Головний комутатор Cisco Catalyst C9300-24S	шт.	1	228120	228120
16	Комутатор робочих груп Cisco Catalyst C9200L-24P-4X	шт.	6	57313	343878
17	Сервер Dell PowerEdge R760	шт.	2	121710	243420
18	Камера Hikvision DS-2CD2143G2-	шт.	10	3990	39900
18	ДБЖ APC Back-UPS Pro 1500VA	шт.	2	4680	9360
Р а з о м			-	-	1038994

Отже, загальна сума матеріальних витрат на розробку мережі становить 1038994 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 10 годин, споживана потужність – 0,5 кВт/год, вартість 1 кВт електроенергії – 9 грн. Тому витрати на електроенергію будуть становити::

$$З_е = 0,5 \cdot 10 \cdot 9 = 45 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8–10% від загальної суми матеріальних затрат.

$$Т_в = З_{м.в} \cdot 0,08..0,1, \quad (4.8)$$

де $Т_В$ – транспортні витрати.

Отже,

$$Т_В = 1038994 \cdot 0,08 = 83119,52 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

В процесі використання основних фондів виконуються заходи що до їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації. Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення. Комп’ютери та

оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_в \cdot Н_А}{100\%} \cdot T \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн.;

$Б_в$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 26000 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{26000 \cdot 0{,}04}{150} \cdot 10 = 104 \text{ грн}$$

4.7 Обчислення накладних витрат

Накладні витрати – це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6,, \quad (4.10)$$

де $H_В$ – накладні витрати.

$$H_В = 23856 \cdot 0{,}4 = 9542{,}40 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4, де зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	23856	2,05
Відрахування на соціальні заходи	5248,32	0,45
Матеріальні витрати	1038994	89,5
Витрати на електроенергію	45	0,01
Транспортні витрати	83119,52	7,16
Амортизаційні відрахування	104	0,01
Накладні витрати	9542,40	0,82
Собівартість	1160909,24	100

В таблиці 4.4 зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати, тобто собівартість (Св) НДР розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.п.} + З_{м.в.} + З_е + Т_в + А + Н_в \quad (4.11)$$

Отже, собівартість дорівнює $С_В$=1160909,24 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = C_в \cdot \left(1 + P_{рен}\right) \cdot (1 + ПДВ) \quad (4.12)$$

де $P_{рен.}$ – рівень рентабельності;

ПДВ – ставка податку на додану вартість, (20 %).

Отже, ціна НДР становить:

$$Ц = 1160909{,}24 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 1811018{,}414 \text{ грн}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

де *П* – прибуток;

C_B – собівартість;

$$П = 1811018{,}414 - 1160909{,}24 = 650109{,}17 \text{ грн}$$

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою:

$$E_p = \frac{П}{С_в} = \frac{650109{,}17}{1160909{,}24} = 0{,}56 \quad (4.14)$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень $Т_р$:

$$T_p = \frac{1}{E_р} \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку:

$$T_р = \frac{1}{0,56} = 1,8$$

Всі дані внесемо в зведену таблицю 4.5 економічних показників.

Таблиця 4.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	1160909,24 грн.
2.	Плановий прибуток, грн.	650109,17 грн.
3.	Ціна, грн.	1811018,414 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп'ютерної мережі для УДМС в Тернопільській області становить 1811018,414 грн. Зважаючи на високі показники економічної ефективності – 0,56, кошти, вкладені в проведення проектних робіт окупляться за 1,8 року.

.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

5.1 Способи і засоби пожежогасіння в центральному офісі УДМС у Тернопільській області

Забезпечення пожежної безпеки в приміщеннях центрального офісу УДМС у Тернопільській області є важливим компонентом щодо охорони праці, оскільки функціонування сучасної комп'ютерної мережі та серверного обладнання безпосередньо пов'язане з ризиками виникнення загорянь через можливі перевантаження електромережі, короткі замикання або несправності апаратури.

Особливістю офісних приміщень, де розгорнуто мережеву інфраструктуру, є наявність значної кількості електроустановок, кабельних ліній та обчислювальної техніки, що класифікує можливі пожежі переважно за класом Е, тобто загоряння електроустановок під напругою. Відповідно до чинних нормативних документів України, зокрема ДБН В.2.5-56:2014 «Системи протипожежного захисту» [1], всі приміщення об'єкта мають бути забезпечені ефективними способами та засобами виявлення, локалізації та ліквідації пожеж на ранніх стадіях їх виникнення.

Основним способом протипожежного захисту в центральному офісі є інтеграція автоматичних систем виявлення загорянь та належна комплектація приміщень первинними засобами пожежогасіння. Оскільки застосування води або хімічної піни в місцях розташування обчислювальної техніки та серверних стійок є недопустимим через загрозу ураження електричним струмом персоналу та ризик повного знищення апаратного забезпечення, для ліквідації локальних осередків вогню передбачено використання вуглекислотних та порошкових вогнегасників [4].

Вуглекислотні вогнегасники типу ВВ-2 або ВВ-5 є найбільш ефективними для серверних кімнат і робочих місць спеціалістів, оскільки діюча речовина не пошкоджує електронні плати, не залишає забруднень після випаровування та дозволяє безпечно гасити електромережі під напругою до 1000 В. Порошкові

вогнегасники універсального призначення раціонально розраховані для захисту коридорів, адміністративних кабінетів та допоміжних приміщень установи.

Важливим складником загальної системи протипожежного захисту є чітка організація евакуації персоналу та відвідувачів установи у разі виникнення надзвичайної ситуації. Для забезпечення швидкого, впорядкованого та безпечного залишення будівлі розроблено детальний план евакуації на випадок пожежі, а також схему оптимального розміщення первинних засобів пожежогасіння в офісі, які детально відображені у додатку Д.

На цьому плані графічно позначено основні та запасні евакуаційні шляхи, напрямки руху людей до виходів, місця розташування внутрішніх пожежних кранів, вогнегасників різних типів та кнопок ручного увімкнення сигналу тривоги. Кожен співробітник центрального офісу зобов'язаний ознайомитися з цією схемою під час проходження первинного та повторних інструктажів з охорони праці, що дозволяє мінімізувати паніку та забезпечити злагодженість дій колективу в умовах реальної загрози.

Система пожежної сигналізації офісу безпосередньо інтегрована із загальною системою оповіщення та керування евакуацією. При спрацьовуванні оптико-електронних димових сповіщувачів, які встановлені на стелі в усіх робочих кабінетах та серверній кімнаті, сигнал негайно передається на приймально-контрольний прилад, після чого вмикається звукове та світлове оповіщення, а також автоматично знімається блокування з електромагнітних замків на евакуаційних виходах.

Для підвищення надійності захисту серверного приміщення, де концентрація мережевого обладнання є найвищою, у проєкті передбачено використання технологій локального газового пожежогасіння, яке здатне ліквідувати загоряння всередині серверної шафи без залучення людини та без шкоди для функціонування комп'ютерної мережі УДМС.

Усі первинні засоби пожежогасіння, вказані на схемі у додатку Д, розміщуються у легкодоступних і помітних місцях, переважно поблизу виходів з приміщень та на шляхах евакуації, на висоті не більше ніж півтора метра від

рівня підлоги. Технічне обслуговування, перезарядка та перевірка справності вогнегасників здійснюються регулярно у встановлені терміни із внесенням відповідних записів до журналу обліку.

Дотримання зазначених вимог, постійний контроль за станом електромереж, якістю ізоляції кабелів шостої категорії та підтримання шляхів евакуації у вільному стані гарантують високий рівень пожежної безпеки під час експлуатації розробленої комп'ютерної мережі установи.

5.2 Електробезпека при експлуатації серверного та активного мережевого обладнання в умовах офісу УДМС

Забезпечення електробезпеки під час розгортання та експлуатації апаратних засобів комп'ютерної мережі в центральному офісі УДМС у Тернопільській області є базовою умовою збереження життя і здоров'я персоналу, а також гарантією безперебійного функціонування мережевої інфраструктури.

Сучасне активне мережеве обладнання, що включає серверні платформи, комутатори та системи безперебійного живлення, є потужним споживачем електричної енергії, що створює потенційну загрозу ураження електричним струмом або виникнення аварійних ситуацій. За ступенем небезпеки ураження людей електричним струмом більшість службових кабінетів установи відносяться до приміщень без підвищеної небезпеки, оскільки в них відсутні умови, що чинять деструктивний вплив на ізоляцію.

Водночас серверна кімната, де сконцентровано основне комутаційне обладнання, потребує підвищеної уваги через високу щільність розміщення апаратури, наявність розгалужених кабельних трас та безперервний цілодобовий режим роботи електроустановок.

Основним небезпечним чинником під час роботи з мережевим обладнанням є ризик появи електричної напруги на металевих конструктивних частинах пристроїв, які в нормальному стані не перебувають під напругою, що

зазвичай трапляється внаслідок пошкодження або пробою ізоляції струмоведучих жил [6].

Для захисту обслуговуючого персоналу та системних адміністраторів від випадкового дотику до таких елементів у проєкті передбачено обов'язкове влаштування захисного заземлення відповідно до вимог Правил улаштування електроустановок.

Усі металеві корпуси серверних шаф, комутаційних стійок, а також металеві оболонки активного обладнання надійно приєднуються до внутрішнього контуру заземлення офісу за допомогою гнучких мідних провідників належного перерізу. Це дозволяє в разі замикання фази на корпус миттєво знизити потенціал пошкодженої установки до безпечного для людини рівня та спровокувати спрацьовування апаратів захисту.

Для попередження виникнення аварійних режимів роботи, спричинених перевантаженням ліній живлення або короткими замиканнями в колах комп'ютерної техніки, групові щити живлення офісу комплектуються сучасними автоматичними вимикачами та пристроями захисного відключення, або диференційними автоматами. Ці пристрої здійснюють безперервний моніторинг параметрів електромережі та забезпечують практично миттєве знеструмлення пошкодженої ділянки у разі виявлення струмів витоку на землю або критичного зростання сили струму.

Особливу увагу приділено лініям живлення робочих місць користувачів та серверного вузла, де прокладено кабелі шостої категорії, які захищені від механічних пошкоджень та прокладаються в ізоляційних пластикових коробах, що додатково знижує ймовірність пошкодження фазних провідників.

Додатковим аспектом електробезпеки є експлуатація джерел безперебійного живлення, які застосовуються для підтримки працездатності чотирьох комутаторів та серверів під час аварійних вимкнень зовнішньої електромережі. Джерела безперебійного живлення акумулюють значну кількість енергії та містять у собі блоки акумуляторних батарей, які навіть за умови повного відключення офісу від зовнішньої мережі залишаються під небезпечною

внутрішньою напругою. Тому обслуговування, заміна елементів живлення та проведення регламентних робіт з цими пристроями дозволяється лише із дотриманням чіткої послідовності дій, виключно після повного зняття залишкового заряду з конденсаторів та із застосуванням спеціалізованого інструменту з ізолювальними ручками [6].

Організаційні заходи забезпечення електробезпеки в установі базуються на суворому дотриманні вимог ДСТУ EN 50110-1:2014 «Експлуатація електроустановок» [2], що регламентує порядок допуску до роботи, проведення інструктажів та періодичність перевірки знань персоналу.

До обслуговування активного мережевого обладнання та серверів допускаються лише особи, які пройшли відповідне навчання, мають належну групу з електробезпеки та детально ознайомлені з інструкціями з охорони праці.

В офісі запроваджується графік планово-попереджувальних ремонтів та періодичних вимірювань опору ізоляції силових кабелів і опору заземлювальних пристроїв, що дозволяє своєчасно виявляти приховані дефекти та гарантувати повну безпеку працівників під час повсякденної експлуатації комп'ютерної мережі УДМС.

.

.

ВИСНОВКИ

Результатом кваліфікаційної роботи є розроблений проект корпоративної мережі головного офісу Управління Державної митної служби в Тернопільській області. Основні технічні характеристики розробленого проекту мережі:

- фізична топологія всередині приміщення – «ієрархічна розширена зірка»;
- топологія WAN – VPN over Internet;
- технології використані для розробки мережі - IEEE 802.3ab, IEEE 802.1Q;
- міжмережний екран та маршрутизатор-шлюз – FortiGate FG-100F;
- головний комутатор рівня ядра, що поєднує в собі функції рівня розподілу корпоративної мережі – Cisco Catalyst C9300-24S;
- комутатори рівня доступу – Cisco Catalyst C9200L-24P-4X;
- кластер із двох фізичних серверів – Dell PowerEdge R760 (2U Rack);
- стек протоколів локальної мережі – TCP/IP версії 4.

У ході виконання кваліфікаційної роботи проведено комплексне проектування логічної та фізичної архітектури мережевої інфраструктури. На основі аналізу технічних вимог здійснено обґрунтований підбір апаратного комплексу та програмного забезпечення. При виборі активного обладнання ключовий акцент було зроблено на забезпеченні високої пропускної здатності та можливості подальшого масштабування мережі без необхідності зміни її топології.

Детально описано процедуру налаштування комутаційної інфраструктури, що забезпечує стабільну передачу трафіку між сегментами мережі. Для захисту конфіденційних даних застосовано технологію шифрування на базі стеку протоколів IPsec, що гарантує цілісність та автентичність переданої інформації.

Логічна та фізична топології локальної мережі подано в графічній частині.

В економічній частині зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі. Отримана вартість мережі є в межах запропонованої замовником.

Останній розділ роботи описує питання охорони праці, та техніки безпеки, які є важливими для безпечної праці користувачів комп’ютерної техніки.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДБН В.2.5-56:2014 "Системи протипожежного захисту". URL: https://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_56_2014_sistemi_protipozhezhnogo_zakhistu/1-1-0-1204. (Дата звернення: 7.06.2026)

2. ДСТУ EN 50110-1:2014. Експлуатація електроустановок. Частина 1: Загальні вимоги. URL: https://standards.ua/50110-1. (Дата звернення: 31.05.2026)

3. Буров Є., Митник М. Комп'ютерні мережі.(у 2-х томах) Львів, Магнолія, 2018.

4. Грибан В. Г., Фоменко А. Є., Казначеєв Д. Г. Безпека життєдіяльності та охорона праці : підруч. / В. Г. Грибан, А. Є. Фоменко, Д. Г. Казначеєв. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2022. – 388 с.

5. Єфіменко А. А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. – Житомир : Житомирська політехніка, 2021. – 116 с.

6. Курепін В. М. Основи охорони праці: навчальний посібник для студентів закладів вищої освіти аграрної галузі. Миколаїв : МНАУ, 2022. – 347 с.

7. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2016 р.) – 500 с.

8. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.

9. Базові поняття мережевих технологій. URL: http://um.co.ua/8/8-17/8-1748.html. (Дата звернення: 6.06.2026).

10. App.Diagrams сайт для створення схем URL: https://app.diagrams.net. (Дата звернення: 9.06.2026).

11. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 2.06.2026)

12. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 1.06.2026)

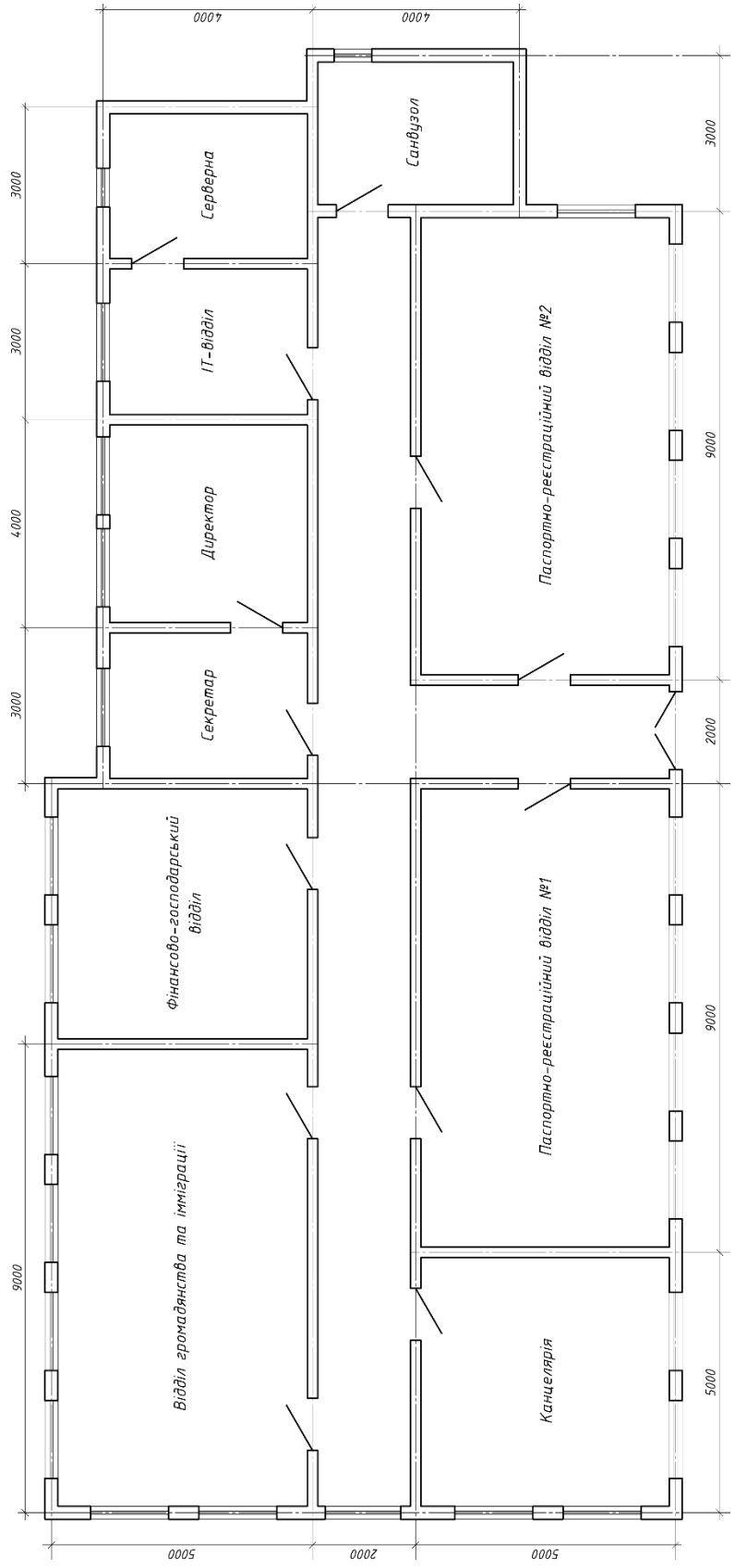
13. Комутатор Cisco Catalyst C9300-24S URL: https://stack-systems.com.ua/kommutator-cisco-ws-c9300-24s (Дата звернення: 2.06.2026)

14. Комутатор Cisco Catalyst C9200L-24P-4X URL: https://stack-systems.com.ua/kommutator-cisco-ws-c9200-24p-4x (Дата звернення: 2.06.2026)

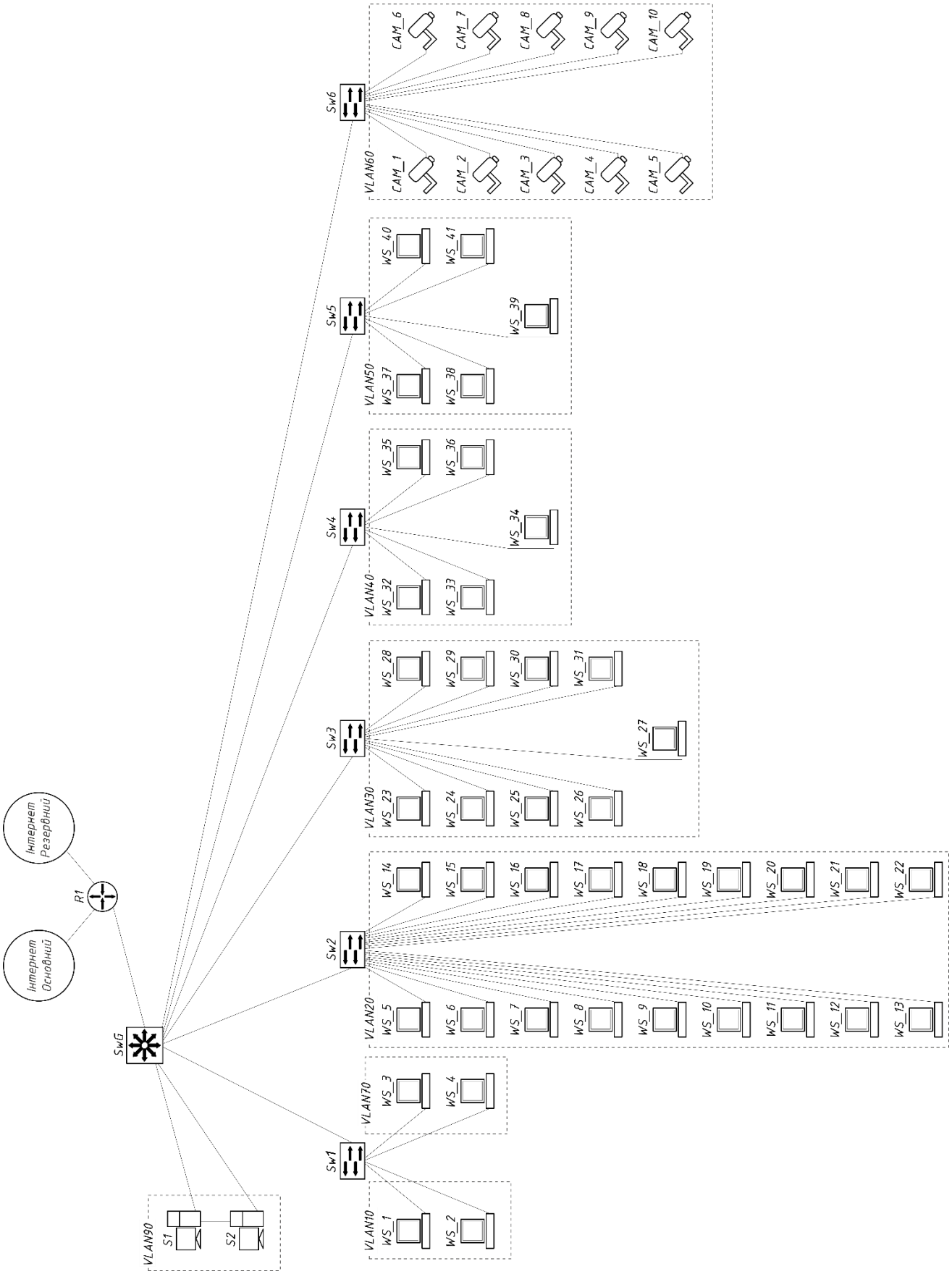
15. PowerEdge R760 Rack Server URL: https://www.dell.com/en-us/shop/cty/pdp/spd/poweredge-r760/pe_r760_tm_vi_vp_sb (Дата звернення: 3.06.2026)

ДОДАТКИ

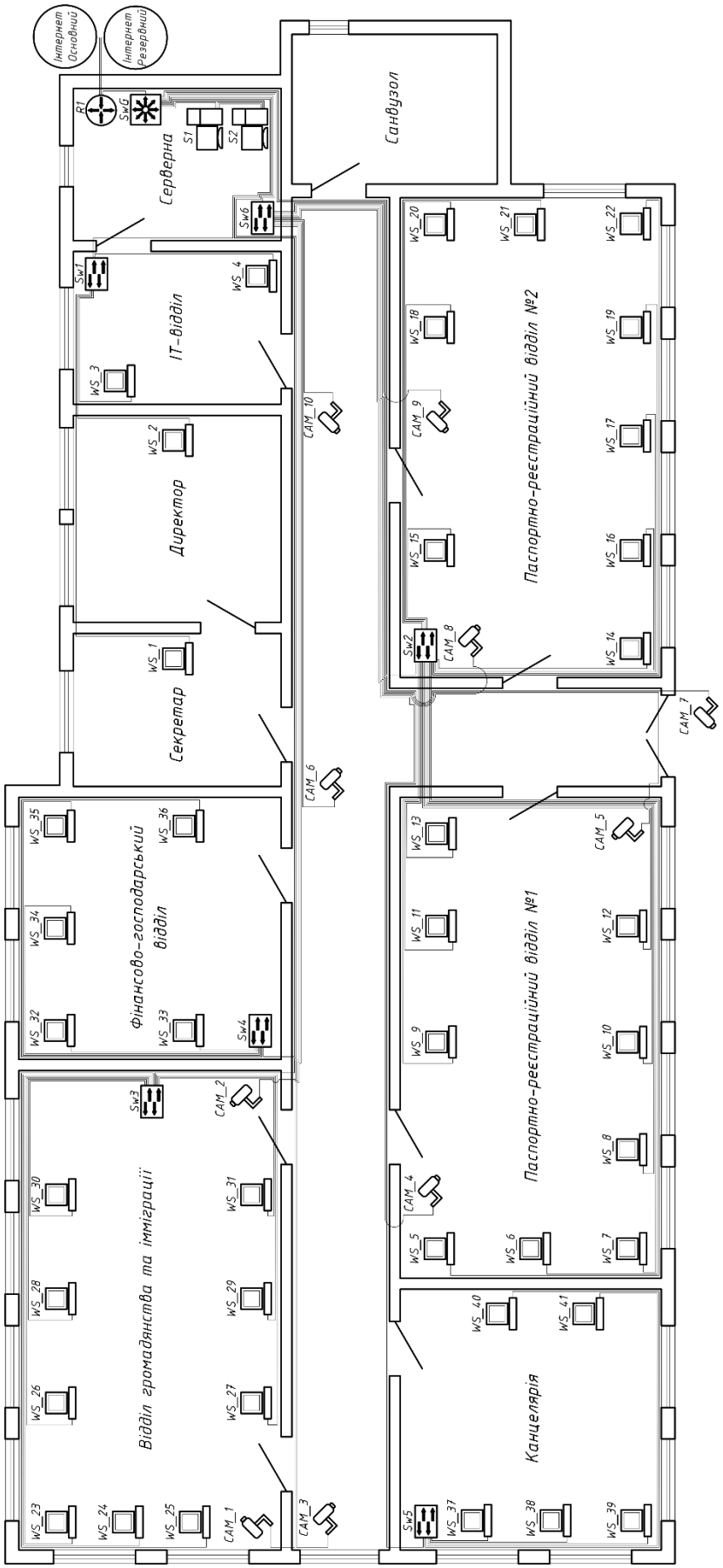
Додаток А. План приміщення будівлі головного офісу УДМС в Тернопільській області



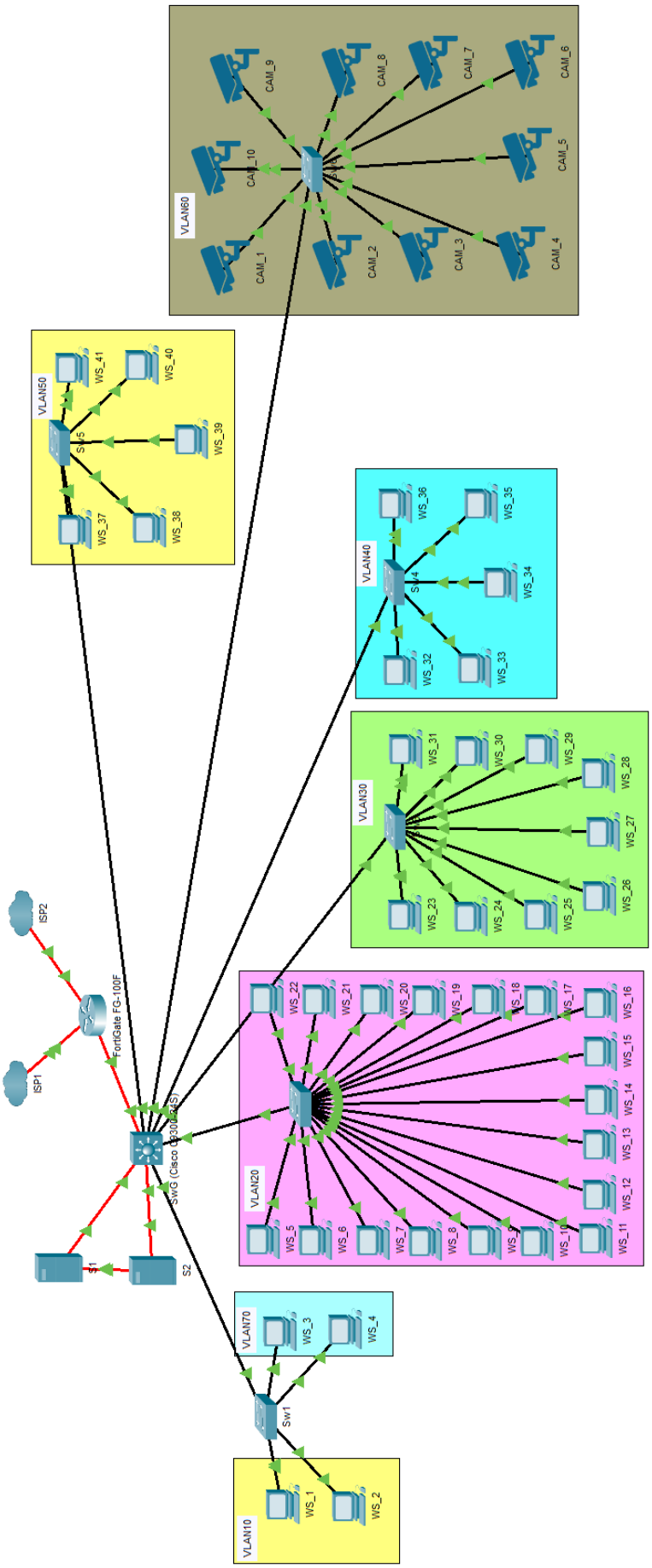
Додаток Б. Логічна топологія мережі УДМС в Тернопільській області



Додаток В. Схема прокладання мережевих кабелів в будівлі головного офісу УДМС в Тернопільській області



Додаток Г. Модель мережі в Cisco Packet Tracer



Додаток Д. План евакуації на випадок пожежі