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 захищеної інформаційно-комунікаційної мережі медичної клініки "МедЛайф-Плюс"**

Виконав: студент VII курсу, групи КІб-703

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

_____ Михайло ПЕТРИЧКА
(ім'я та прізвище)

Керівник _____ Володимир ШТОКАЛО
(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

Петричці Михайлу Петровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту захищеної інформаційно-комунікаційної мережі медичної клініки "МедЛайф-Плюс"**

керівник роботи Штокало Володимир Ярославович
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 30.04.2026р № 4/9-252.

2. Строк подання студентом роботи: 22 червня 2026 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		
Охорона праці, техніка безпеки та екологічні вимоги	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 _____ Михайло ПЕТРИЧКА
(підпис) (ім'я та прізвище)

Керівник роботи _____ Володимир ШТОКАЛО
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Петричка М.П. Розробка проєкту захищеної інформаційно-комунікаційної мережі медичної клініки "МедЛайф-Плюс": 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 медичної клініки "МедЛайф-Плюс" 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 Tracert.

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

ANNOTATION

Petrichka M.P. Development of a project for a secure information and communication network of the medical clinic "MedLife-Plus": 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 project for a computer network of the medical clinic "MedLife-Plus" 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. Create a virtual network model in Cisco Packet Tracert.

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

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DNS (Domain Name System) – сервер доменних імен.

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

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.

IEEE 802.3u – стандарт Fast Ethernet 100Мбіт/с.

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) – апаратна адреса ПК;

SIP (Session Initiation Protocol) – основний протокол сигналізації в IP-телефонії (VoIP),

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

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

UTP (Unshielded Twisted Pair) - неекранована скручена пара;

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.

ПК – персональний комп’ютер.

ОС – операційна система.

ПК – персональний комп’ютер.

ВСТУП

Сучасна медицина стрімко переходить на цифрові технології, де електронні картки пацієнтів, результати обстежень та внутрішні інформаційні системи формують єдиний простір. Для медичних закладів, таких як клініка «МедЛайф-Плюс», це означає не лише підвищення швидкості обслуговування, а й виникнення серйозної відповідальності за збереження конфіденційної інформації. Персональні дані пацієнтів та результати діагностики потребують особливого рівня захисту, оскільки будь-який витік відомостей може призвести до правових та репутаційних наслідків. Тому побудова безпечного та відмовостійкого мережевого середовища є головним завданням під час автоматизації медичних процесів.

Особливістю функціонування сучасної клініки «МедЛайф-Плюс» є наявність головного корпусу та територіально віддалених діагностичних центрів. Така структура зумовлює необхідність організації захищеної взаємодії між підрозділами через загальнодоступні канали зв'язку. Крім того, всередині самої установи виникає потреба в чіткому розділенні потоків даних, адже складне медичне обладнання та звичайні робочі станції персоналу не повинні перебувати в одному незахищеному просторі. Це вимагає розробки такої архітектури мережі, яка б унеможливлювала несанкціонований доступ до лікарської таємниці як ззовні, так і зсередини організації.

Метою кваліфікаційної роботи є розробка проєкту захищеної та відмовостійкої інформаційно-комунікаційної мережі для клініки «МедЛайф-Плюс», що забезпечує надійний обмін інформацією між філіями та суворе розмежування прав доступу користувачів до мережевих ресурсів.

Практична цінність отриманих результатів полягає в тому, що створений проєкт є готовим технічним рішенням, яке можна адаптувати та впровадити в реальних медичних закладах схожого типу.

.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Найменування розробки: проєкт захищеної інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс».

Результати розробки призначені для впровадження на об'єктах медичної клініки «МедЛайф-Плюс», яка функціонує у місті Тернопіль і включає головну клініку та територіально віддалену філію (діагностичний центр). Проєкт орієнтований на застосування в закладах охорони здоров'я, що обробляють медичну та персональну інформацію пацієнтів і потребують високого рівня інформаційної безпеки, надійності та безперебійності роботи IT-інфраструктури.

Розроблена інформаційно-комунікаційна мережа застосовуватиметься для:

- забезпечення захищеного обміну даними між головною клінікою та діагностичним центром;
- організації роботи медичної інформаційної системи (МІС), електронного документообігу та доступу до електронних карток пацієнтів;
- інтеграції спеціалізованого медичного обладнання (апарати УЗД, МРТ, рентген тощо) в єдину мережеву інфраструктуру з ізоляцією трафіку від загальної офісної мережі;
- організації безпечного доступу до ресурсів мережі для медичного та адміністративного персоналу на основі рольової моделі управління доступом;
- захисту персональних даних пацієнтів (медичної таємниці) відповідно до вимог чинного законодавства України у сфері захисту інформації (ЗУ "Про захист персональних даних") [1].

Проєкт може бути використаний як типове рішення для модернізації або розбудови з нуля мережевої інфраструктури медичних установ подібного

масштабу та структури, що мають підвищені вимоги до конфіденційності, цілісності та доступності інформаційних ресурсів.

.

1.1.2 Призначення розробки

Головним призначенням даного проєкту є створення цілісної, масштабованої, відмовостійкої та безпечної інформаційно-комунікаційної інфраструктури для медичної клініки «МедЛайф-Плюс». Розробка спрямована на об'єднання центрального відділення на 40 робочих місць та віддаленого діагностичного центру на 12 робочих місць у спільний високошвидкісний інформаційний простір для автоматизації лікувально-діагностичних та адміністративних процесів.

Впровадження проєкту покликане забезпечити надійне функціонування медичної інформаційної системи (МІС), систем електронного документообігу та цифрових архівів медичних зображень. Мережа проектується для організації миттєвого доступу лікарів та адміністраторів до електронних карток пацієнтів, результатів аналізів та графіків прийому, що безпосередньо впливає на швидкість та якість надання медичних послуг.

Важливим безпековим призначенням розробки є суворе розмежування внутрішніх мережевих потоків даних за допомогою технології віртуальних локальних мереж (VLAN). Це дозволяє ізолювати критично важливе та дороге медичне обладнання (апарати УЗД, КТ, МРТ та лабораторні аналізатори) від загального офісного трафіку та публічного гостьового Wi-Fi. Така ізоляція захищає медичну техніку від потенційних шкідливих програм та мережевих перевантажень.

Проєкт призначений для повного забезпечення вимог Закону України «Про захист персональних даних» [1] та концепції захисту медичної таємниці. Для цього в архітектуру мережі закладаються механізми суворого контролю доступу (ACL) та міжмережевого екранування (Firewall) на базі обладнання Cisco. Це мінімізує ризики несанкціонованого доступу до серверів з боку зловмисників або неавторизованого персоналу.

Крім того, розробка призначена для створення захищених каналів зв'язку (VPN-тунелів із шифруванням) між головною клінікою та діагностичним центром. Це дозволяє безпечно передавати персональні дані пацієнтів через відкриті канали мережі Інтернет.

На серверному рівні призначенням розробки є підвищення відмовостійкості системи завдяки впровадженню технології RAID для захисту від втрати даних при виході з ладу жорстких дисків, а також розгортання доменного контролера для централізованого керування обліковими записами всіх працівників клініки.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для забезпечення надійної, безпечної та безперебійної роботи інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс», а також для підтримки високої швидкості обробки персональних даних пацієнтів, до технічних і програмних засобів висуваються вимоги, які можна розділити на декілька категорій.

Вимоги до серверного обладнання. Центральний сервер головної клініки повинен мати архітектуру підвищеної відмовостійкості. Обов'язкова наявність сучасного багатокернельного процесора (не менше 8–12 ядер) для ефективної роботи віртуальних машин та обробки запитів до медичної інформаційної системи.

Об'єм оперативної пам'яті повинен становити не менше 32–64 ГБ із підтримкою технології виправлення помилок (ECC RAM). Дискова підсистема має базуватися на швидкісних SSD або NVMe накопичувачах, об'єднаних в апаратний RAID-масив (наприклад, RAID 1 для операційної системи та RAID 10 або RAID 5 для баз даних) для захисту від втрати інформації у разі виходу з ладу одного чи кількох дисків.

Сервер повинен мати щонайменше два гігабітні мережеві інтерфейси для балансування трафіку та резервування каналів, а також дубльоване (резервне) джерело живлення.

Вимоги до робочих станцій персоналу. Комп'ютери офісних працівників, реєстратури та кабінетів лікарів (загалом близько 60–70 ПК для всієї структури) повинні забезпечувати швидку роботу з офісними програмами, браузерами та клієнтською частиною медичної інформаційної системи.

Мінімальні технічні характеристики включають: сучасний процесор із частотою не менше 3.0 ГГц (мінімум 4 ядра), об'єм оперативної пам'яті від 8 ГБ та накопичувач типу SSD об'ємом від 246 ГБ. Монітори повинні мати діагональ не менше 21.5 дюймів та IPS-матрицю для комфортної тривалої роботи медичного персоналу та чіткого відображення медичних документів чи графічних результатів діагностики.

Вимоги до активного мережевого обладнання. Комутатори робочих груп (пріоритетно лінійки Cisco Catalyst або аналогічні керовані комутатори другого та третього рівнів) повинні мати 24 або 48 портів зі швидкістю 1 Гбіт/с.

Обладнання обов'язково має підтримувати технологію віртуальних локальних мереж (VLAN) для логічного сегментування мережі, функції агрегації каналів та стандарти безпеки на рівні портів. Головний маршрутизатор або апаратний міжмережевий екран (Firewall, наприклад, серії Cisco ASA або Firepower) повинен мати високу пропускну здатність для обробки шифрованого трафіку, підтримувати створення захищених VPN-тунелів (IPsec) для підключення віддалених діагностичного центру та мати гнучкий функціонал налаштування списків контролю доступу (ACL) для фільтрації шкідливого трафіку.

Вимоги до пасивної мережевої інфраструктури. Вся кабельна система всередині приміщень головної клініки та філії має бути виконана за допомогою мідного кабелю "вита пара" категорії не нижче Cat 5e або Cat 6, що гарантує швидкість передачі даних до 1 Гбіт/с на відстанях до 100 метрів.

Для організації центральних вузлів комутації необхідно передбачити настінні або підлогові телекомунікаційні шафи (реки) стандартної ширини 19

дюймів, оснащені блоками розеток та патч-панелями для зручного адміністрування та маркування ліній.

Вимоги до серверного програмного забезпечення. Як основну серверу операційну систему необхідно використовувати Windows Server (версії 2019 або 2022) або стабільний корпоративний дистрибутив Linux (наприклад, Ubuntu Server або Rocky Linux).

На сервері мають бути розгорнуті засоби віртуалізації (Hyper-V або Proxmox) для розділення функцій між віртуальними машинами.

Обов'язковим є налаштування служби каталогів Active Directory (для Windows) для централізованого керування обліковими записами користувачів, а також мережевих служб DNS та DHCP.

Вимоги до клієнтського та захисного програмного забезпечення. На всіх робочих станціях має бути встановлена ліцензійна операційна система Windows 10/11 Pro, яка підтримує введення комп'ютера в корпоративний домен.

Кожне робоче місце повинно бути захищене корпоративним антивірусним програмним забезпеченням із централізованим керуванням та регулярним оновленням баз вірусних сигнатур.

Також на ПК інсталюється спеціалізоване клієнтське програмне забезпечення медичної системи для взаємодії із центральною базою клініки.

Вимоги до програмного забезпечення для моделювання. Для етапу проєктування, візуалізації топології, налаштування конфігураційних файлів комутаторів та маршрутизаторів, а також для фінального тестування правил безпеки та перевірки проходження пакетів між сегментами VLAN має використовуватись спеціалізоване середовище імітаційного моделювання Cisco Packet Tracer.

1.1.4 Вимоги до документації

Розробка проєкту захищеної інформаційно-комунікаційної мережі для медичної клініки «МедЛайф-Плюс» повинна супроводжуватися створенням повного комплекту технічної, експлуатаційної та розпорядчої документації. Це

необхідно для подальшого якісного монтажу, ефективного адміністрування мережі, швидкого усунення несправностей, а також для успішного проходження аудитів на відповідність вимогам законодавства України у сфері захисту персональних даних. До складу документації висуваються такі вимоги:

- пояснювальна записка до технічного проєкту. Цей документ має містити розгорнуте теоретичне та технічне обґрунтування всіх архітектурних рішень. У ньому детально описується аналіз об'єкта (головної клініки та двох філії), обґрунтування вибору топології, кабельної системи, активного обладнання Cisco та серверних платформ. Також обов'язковим є детальний опис підсистем безпеки: логіки розподілу віртуальних мереж (VLAN), принципів міжмережевого екранування та технологій шифрування даних при їх передачі;

- графічна документація та схеми мережі. Комплект документів повинен включати детальні графічні схеми, розроблені у середовищі Cisco Packet Tracer або спеціалізованих графічних редакторах. Сюди відносяться: фізична схема розміщення обладнання та прокладання кабельних трас у будівлях; логічна схема мережі із зазначенням меж філії, комутаторів робочих груп, маршрутизаторів та міжмережевих екранів; а також структурна схема взаємодії серверної інфраструктури, медичного обладнання та робочих станцій персоналу.

- документація з мережевої адресації та сегментації. Окремим документом (або розгорнутою таблицею) оформлюється схема розподілу адресного простору клініки. Вона повинна містити чіткі межі IP-адрес для кожної підмережі, номери та призначення всіх створених VLAN (окремо для адміністрації, лікарів, медичного обладнання та гостьової мережі), а також таблиці статичних IP-адрес для критично важливих вузлів: серверів, шлюзів, мережевих принтерів та діагностичних апаратів (УЗД, ЕКГ тощо).

- специфікація обладнання та програмного забезпечення. Документ оформлюється у вигляді таблиці, яка містить вичерпний перелік усіх компонентів мережі. Для апаратного забезпечення вказуються точні моделі комутаторів, маршрутизаторів, Firewall, серверів, ДБЖ, параметри кабелів та патч-панелей із зазначенням необхідної кількості. Для програмного забезпе-

чення вказуються назви операційних систем, ліцензій, антивірусних пакетів та клієнтського ПЗ медичної інформаційної системи;

- інструкції з налаштування та експлуатаційні інструкції. Комплект повинен містити покрокові керівництва для системного адміністратора клініки. Сюди відносяться інструкції зі створення апаратного RAID-масиву на сервері, розгортання операційної системи, конфігурування віртуальних машин, налаштування доменного контролера Active Directory. Також мають бути додані текстові файли конфігурацій (конфіги) для комутаторів та маршрутизаторів Cisco з детальними коментарями до правил списків контролю доступу (ACL) та параметрів VPN-тунелів;

- регламенти безпеки та резервного копіювання. Документація повинна містити правила та графіки створення резервних копій (Backup Policy) баз даних пацієнтів та конфігураційних файлів обладнання. Також розробляється інструкція з моніторингу безпеки, де прописуються дії адміністратора у разі виявлення спроб несанкційного доступу або збоїв у мережі філії;

- інструкції користувачів щодо безпечної роботи. Короткі та зрозумілі пам'ятки для медичного та адміністративного персоналу клініки. Вони повинні регламентувати правила парольної політики (складність та термін дії паролів), правила безпечної роботи з електронними картками пацієнтів у медичній системі, а також сувору заборону підключення робочих комп'ютерів до публічних або сторонніх мереж (наприклад, до гостьового Wi-Fi клініки).

1.1.5 Техніко-економічні показники

Впровадження проєкту захищеної інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс» повинно забезпечити високу технічну ефективність інфраструктури при оптимальних капітальних та експлуатаційних витратах. Основними техніко-економічними показниками та критеріями доцільності розробки є:

- оптимізація капітальних витрат. Економічний ефект досягається за рахунок раціонального підбору комунікаційного обладнання Cisco та серверних платформ, які мають найкраще співвідношення ціни, продуктивності та безпеки. Замість придбання дорогих вузькоспеціалізованих пристроїв для філії, проєкт передбачає централізацію обчислювальних потужностей у головній клініці, що суттєво знижує початкові витрати на закупівлю заліза для діагностичного центру;

- економічна ефективність від впровадження віртуалізації. Використання технологій віртуалізації на базі єдиного потужного фізичного сервера (замість купівлі кількох окремих серверів під кожну задачу – домен, бази даних, медична інформаційна система) дозволяє скоротити витрати на серверне обладнання на 40–50%. Це також призводить до зниження операційних витрат на електроживлення, охолодження серверної кімнати та подальше технічне обслуговування;

- мінімізація фінансових ризиків від витоку даних. Створення захищеного контуру мережі, впровадження Firewall, списків контролю доступу (ACL) та ізоляції сегментів VLAN для медичного обладнання повністю нівелює ризики несанкціонованого доступу до медичної таємниці. У масштабах бізнесу це запобігає потенційним багатотисячним юридичним позовам від пацієнтів, штрафам з боку державних регуляторів за порушення Закону України «Про захист персональних даних» та катастрофічним репутаційним втратам клініки;

- підвищення відмовостійкості та зниження збитків від простою. Завдяки використанню надійного обладнання із високим показником середнього часу між відмовами, апаратному дзеркалюванню дисків (RAID) та налаштуванню резервних маршрутів, коефіцієнт готовності мережі має становити не менше 99.9%. Це мінімізує ризик технічних збоїв, через які лікарі чи реєстратура могли б втратити доступ до медичної інформаційної системи. Кожна година простою клініки такого масштабу (60–70 робочих місць) несе прямі фінансові збитки через неможливість прийому пацієнтів та проведення діагностики;

- оптимізація операційної діяльності та робочого часу персоналу. Побудова високошвидкісної мережі (1 Гбіт/с) та захищених VPN-тунелів із

філією забезпечує миттєвий обмін "важкими" цифровими медичними знімками (УЗД, МРТ, КТ) та даними пацієнтів. Це скорочує час очікування результатів лікарями, пришвидшує обслуговування пацієнтів у реєстратурі та дозволяє персоналу обробляти більшу кількість звернень за робочу зміну, підвищуючи загальну рентабельність клініки;

- масштабованість інфраструктури та захист інвестицій. Проєктні рішення (зокрема розподіл IP-адрес та архітектура комутації) розробляються з урахуванням перспективи розширення клініки на 25–30% без необхідності повної перебудови мережі чи заміни ядра системи. У разі підключення нових комп'ютерів або відкриття другого діагностичного центру, інтеграція відбудеться шляхом простого масштабування у межах створеної моделі, що зберігає інвестиції, вкладені у поточну розробку;

- економічна вигода етапу моделювання. Проектування та фінальне тестування мережі в середовищі Cisco Packet Tracer дозволяє повністю виключити фінансові витрати на закупівлю помилкового або несумісного обладнання на етапі практичного впровадження. Симуляція дозволяє безкоштовно перевірити працездатність конфігурацій, логіку маршрутизації та безпеку ACL-правил до початку реального монтажу.

1.1.6 Стадії та етапи розробки

Проєктування та розробка захищеної інформаційно-комунікаційної мережі для медичної клініки «МедЛайф-Плюс» здійснюється відповідно до стандартних етапів життєвого циклу розробки автоматизованих та мережевих систем. Весь процес виконання кваліфікаційної роботи розподілений на декілька послідовних стадій.

Передпроєктна стадія та формування технічного завдання. На цьому початковому етапі здійснюється збір вихідних даних про архітектуру та географічний розподіл об'єктів клініки, розраховується точна кількість робочих місць (40 ПК у головному офісі та 12 ПК у філії) та аналізуються типи медичного

обладнання. Визначаються ключові загрози безпеці персональних даних пацієнтів та формуються технічні вимоги, які зафіксовані в поточному технічному завданні.

Стадія аналізу об'єкта та обґрунтування технічних рішень. Цей етап присвячений аналізу існуючої інфраструктури клініки та порівняльному аналізу мережевих технологій. Проводиться теоретичне обґрунтування вибору топології майбутньої мережі, вибір типу кабельного середовища (вита пара відповідних категорій), підбір конкретних моделей комутаторів, маршрутизаторів та міжмережевих екранів Cisco, а також вибір серверного програмного забезпечення.

Стадія технічного проєктування та логічної організації мережі. Етап включає розробку архітектури мережі на папері. На цьому кроці розраховується і розподіляється адресний простір (IPv4) для всієї клініки та її діагностичного центру. Створюється схема логічного розділення мережі за допомогою технології VLAN, визначаються правила розмежування доступу офісного персоналу, гостьових пристроїв та медичної техніки, а також проектуються схеми захищених VPN-тунелів для зв'язку з філією.

Стадія розробки робочої документації та інструкцій. На цьому етапі створюється прикладне інженерне наповнення проєкту. Пишуться детальні технічні інструкції з налаштування серверного обладнання (створення відмовостійкого RAID-масиву, розгортання віртуальних машин, конфігурування контролера домену Active Directory, DNS та DHCP сервісів).

Також формуються покрокові інструкції та текстові конфігурації для налаштування активного обладнання Cisco, включаючи правила списків контролю доступу (ACL) та міжмережевого екранування.

Стадія імітаційного моделювання та тестування. Проводиться практична перевірка та верифікація всіх запроєктованих рішень у спеціалізованому програмному середовищі Cisco Packet Tracer.

На цьому етапі збирається віртуальна модель мережі «МедЛайф-Плюс», застосовуються створені конфігураційні файли, тестується правильність

маршрутизації даних та надійність блокування шкідливого чи несанкціонованого трафіку між сегментами VLAN за допомогою ACL.

Стадія техніко-економічного та організаційного обґрунтування. Етап присвячений фінансовому розрахунку доцільності проєкту. Проводиться калькуляція капітальних витрат на закупівлю заліза, кабелів та софту, оцінюються терміни окупності системи та ризики фінансових втрат від потенційних простоїв клініки чи витоку даних. Окремо розробляються заходи з охорони праці та техніки безпеки при монтажі та експлуатації створеної мережі.

Підсумкова стадія та підготовка до захисту. На заключному етапі здійснюється фінальне зведення всіх розділів у єдину пояснювальну записку кваліфікаційної роботи, перевірка документації на відповідність чинним стандартам (ДСТУ) та вимогам випускової кафедри, а також підготовка графічного матеріалу (презентації та плакатів) для захисту перед екзаменаційною комісією.

1.1.7 Порядок контролю та прийому

Порядок контролю та прийому визначає послідовність перевірок, види випробувань та критерії, за якими готова інформаційно-комунікаційна мережа медичної клініки «МедЛайф-Плюс» приймається в промислову експлуатацію. Процес контролю та прийому системи розподіляється на такі загальні етапи:

- вхідний контроль матеріалів та обладнання. Проводиться до початку монтажних робіт. Перевірці підлягає вся специфікація закупленого активного обладнання, серверів, кабельної продукції та пасивних компонентів. Контролюється цілісність пакування, відповідність серійних номерів, наявність гарантійних талонів, сертифікатів відповідності та ліцензій на програмне забезпечення;

- поточний контроль монтажних робіт. Здійснюється безпосередньо під час розгортання інфраструктури в головній клініці та діагностичного центру. Контролюється якість прокладання кабельних трас, правильність монтажу теле-

комунікаційних шаф, надійність заземлення обладнання, а також відповідність маркування кабельних ліній та розеток робочих місць проектній документації;

- попередні випробування. Етап контролю, який виконується розробником на ізольованому стенді або в середовищі імітаційного моделювання перед запуском мережі в реальну роботу. Перевіряється базова працездатність конфігураційних файлів комутаторів та маршрутизаторів, логіка розподілу IP-адрес, коректність підняття віртуальних мереж (VLAN) та працездатність шифрованих VPN-тунелів із філією;

- приймальні випробування підсистеми безпеки. Обов'язкова комплексна перевірка засобів захисту інформації на відповідність вимогам ТЗ щодо захисту персональних даних пацієнтів. Спеціальна комісія перевіряє ефективність міжмережевого екранування (Firewall) та списків контролю доступу (ACL). Критерієм успішності є повна ізоляція мережевого трафіку медичного обладнання та гостьового Wi-Fi від внутрішньої офісної мережі клініки;

- дослідна експлуатація системи. Мережа запускається в тестовому режимі на обмежений термін (наприклад, 1–2 тижні) для перевірки її роботи під реальним навантаженням. На цьому етапі контролюється відмовостійкість серверів (робота RAID-масиву), швидкість доступу працівників реєстратури та лікарів до медичної інформаційної системи (МІС), а також виявляються та усуваються приховані помилки в маршрутизації чи розподілі адрес через DHCP;

- прийом експлуатаційної документації: Замовник перевіряє наявність та повноту повного пакету супровідних документів. Сюди відносяться точні фізичні та логічні схеми мережі, таблиці адресації, тексти конфігураційних файлів обладнання, інструкції з адміністрування серверних ОС та контролера домену, а також регламенти резервного копіювання баз даних;

- остаточна здача-прийом мережі в експлуатацію. Заключний етап, який оформлюється двостороннім Актом здачі-прийому виконаних робіт. Комісія замовника підписує документ за умови успішного проходження всіх попередніх етапів тестування, відсутності зауважень до швидкодії та безпеки мережі, а

також після проведення інструктажу для штатного системного адміністратора клініки щодо правил обслуговування нової інфраструктури.

1.2 Аналіз структури медичної клініки "МедЛайф-Плюс"

Детальний аналіз організаційно-штатної структури, внутрішньої топології та інформаційних потоків медичної клініки «МедЛайф-Плюс» є основою для формування архітектури майбутньої захищеної мережі.

Специфіка сучасного медичного закладу полягає в одночасному функціонуванні класичних бізнес-підрозділів та високотехнологічних лікувально-діагностичних зон. Розуміння точного розташування мережевих вузлів, їх кількісних характеристик та характеру взаємодії дозволяє створити мережу, яка не лише забезпечить високу швидкість обміну даними, але й гарантуватиме виконання вимог законодавства України щодо захисту персональних даних та збереження медичної таємниці.

Об'єкт автоматизації має чітко виражену розподілену структуру, що складається з головної клініки та двох віддаленого діагностичного центру, кожен з яких характеризується набором мережевих вузлів та функціональних обов'язків.

Головна клініка є центральним вузлом усієї інфраструктури, де зосереджено адміністративний апарат та основні лікувальні кабінети з загальною кількістю у 40 пристрої: персональних комп'ютерів, периферійного та інфраструктурного обладнання.

Адміністративний блок та відділ кадрів налічують 6 ПК та 2 мережеві багатофункціональні пристрої (БФП), які опрацьовують переважно внутрішню документацію, трудові договори та загальні розпорядження.

Бухгалтерія та фінансовий відділ містять 4 ПК та 1 мережевий принтер. Цей сегмент взаємодіє з державними податковими сервісами та системами клієнт-банку.

Відділ реєстратури та рецепції, що забезпечує першу лінію взаємодії з пацієнтами, містить 6 ПК, 1 спеціалізовані принтери для друку чеків та талонів.

Клінічний блок, що складається з кабінетів профільних лікарів (терапевтів, хірургів, кардіологів), є найбільш чисельним і налічує 16 ПК, призначених для ведення електронних медичних карток у загальній медичній інформаційній системі (МІС).

Денний стаціонар та пости медсестер укомплектовані 4 ПК для оперативного контролю стану пацієнтів та обліку медикаментів.

В таблиці 1.1 наведено узагальнені дані про розподіл мережевих вузлів по окремих підрозділах головної клініки.

Таблиця 1.1 – Комплексний розподіл пристроїв у Головній клініці

Функціональний підрозділ	Тип мережевого пристрою	Кількість	Призначення вузла в інфраструктурі
Адміністрація та відділ кадрів	Персональний комп'ютер	6	Документообіг та кадровий облік
Бухгалтерія та фінанси	Персональний комп'ютер	4	Робота з фінансовою звітністю та банкінгом
Реєстратура та рецепція	Персональний комп'ютер	6	Оформлення пацієнтів та робота з МІС
Кабінети профільних лікарів	Персональний комп'ютер	16	Ведення електронних медичних карток
Денний стаціонар та медсестри	Персональний комп'ютер	4	Оперативний облік та контроль лікування
Загальна мережева периферія	Мережеві БФП та IP-телефони	4	Централізований друк та зв'язок
Разом		40	

Окремим важливим об'єктом головної клініки повинна стати серверна кімната, де розташовується центральний фізичний сервер відмовостійкої архітектури, головний маршрутизатор та міжмережевий екран. Одне із завдань розробки є оптимальний обґрунтований вбір приміщення для серверної кімнати.

Територіально віддалену філію клініки орієнтовані на первинний збір діагностичної інформації та мають меншу щільність стандартних комп'ютерних робочих місць, але вищий рівень насиченості спеціалізованим обладнанням.

Діагностичний центр укомплектований рівно 12 мережевими пристроями. У зоні реєстрації цієї філії встановлено 2 персональні комп'ютери для координації пацієнтів.

Кабінети ультразвукової діагностики та електрокардіографії містять 3 персональні комп'ютери лікарів, які інтегровані з 2 цифровими медичними апаратами, що мають власні мережеві інтерфейси для передачі даних за протоколом DICOM. Клініко-діагностична лабораторія цієї філії налічує 3 персональні комп'ютери, до яких підключено 2 автоматизовані лабораторні аналізатори, що виступають як самостійні мережеві вузли з фіксованими IP-адресами..

В таблиці 1.2 наведено узагальнені дані про розподіл мережевих вузлів по окремих підрозділах першого діагностичного центру.

Таблиця 1.2 – Розподіл пристроїв у діагностичному центрі

Функціональний підрозділ (кабінет)	Тип мережевого пристрою	Кількість	Призначення вузла в інфраструктурі
Рецепція та реєстрація філії	Персональний комп'ютер	2	Первинний запис та координація пацієнтів
Кабінети УЗД та ЕКГ діагностики	Персональний комп'ютер	3	Робочі місця лікарів-діагностів
УЗД та ЕКГ апаратура	Цифровий медичний апарат	2	Збір та передача за протоколом DICOM
Клініко-діагностична лабораторія	Персональний комп'ютер	3	Обробка та верифікація результатів аналізів
Лабораторне обладнання	Автоматизований аналізатор	2	Вимірювальні цифрові комплекси з IP-виходом
Разом		12	

Аналіз інформаційних потоків всередині підприємства «МедЛайф-Плюс» дозволяє розділити весь трафік на кілька взаємопов'язаних, але принципово різних за призначенням та рівнем критичності рівнів.

Вертикальні потоки даних відображають взаємодію між робочими станціями філії та центральним сервером головної клініки. Лікарі та реєстратори з віддалених центрів постійно здійснюють запити до бази даних медичної інформаційної системи для перегляду розкладу, внесення записів про пацієнтів та отримання протоколів лікування.

Окремий потужний потік складає передача графічних файлів високої чіткості (знімки КТ, МРТ, рентгенівські знімки) з діагностичного центру до центрального сховища.

Горизонтальні потоки даних відбуваються безпосередньо всередині підрозділів, наприклад, при передачі результатів аналізів від лабораторного аналізатора на комп'ютер лаборанта, або при відправці документів на друк до мережевих БФП.

Окрему категорію становить зовнішній трафік: фінансовий потік бухгалтерського обліку, що виходить у глобальну мережу до банківських серверів, та публічний гостьовий трафік пацієнтів, які підключаються до бездротової мережі Wi-Fi під час очікування прийому в холах клініки.

Необхідність суворого розмежування доступу між підрозділами обумовлена як вимогами безпеки, так і оптимізацією мережевої продуктивності.

Відсутність ізоляції між сегментами створює загрозу, за якої зловмисник або шкідливе програмне забезпечення, що потрапило на комп'ютер гостя через публічний Wi-Fi або на ПК реєстратора через фішинговий електронний лист, може отримати безперешкодний доступ до бази даних пацієнтів чи конфігурації медичних апаратів.

Співробітники бухгалтерії чи відділу кадрів не повинні мати технічної можливості переглядати медичні карти чи результати обстежень пацієнтів, оскільки це порушує право на медичну таємницю. У свою чергу, лікарі не повинні мати доступу до фінансових документів та баз даних бухгалтерського обліку.

Найбільш критичним є захист дорогого медичного обладнання (КТ, МРТ, лабораторні аналізатори). Ці пристрої функціонують під управлінням вбудованих операційних систем, які рідко оновлюються виробниками, тому будь-яка вірусна активність у загальній мережі може вивести їх з ладу, що призведе до зупинки роботи діагностичного центру та фінансових збитків.

Таким чином, результати аналізу структури клініки чітко вказують на необхідність впровадження технології віртуальних локальних мереж (VLAN) для логічної ізоляції адміністративного, бухгалтерського, медичного та гостьового сегментів, використання міжмережевого екрана для контролю зовнішнього периметра, налаштування списків контролю доступу (ACL) для фільтрації внутрішнього трафіку та організації шифрованих VPN-тунелів для безпечного об'єднання Головної клініки з віддаленим діагностичним центром.

.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Аналіз та обґрунтування вибору топології та технології мережі

Процес проєктування архітектури захищеної інформаційно-комунікаційної мережі для медичної клініки «МедЛайф-Плюс» вимагає системного підходу до вибору базової топології та технологічних стандартів, оскільки саме ці параметри визначають подальшу стійкість системи до відмов та можливість впровадження багаторівневих засобів захисту інформації. Враховуючи специфіку об’єкта, що складається з головного корпусу та окремого діагностичного центру, вибір конфігурації мережі повинен базуватися на принципах високої доступності, керованості та логічної ізоляції критичних сегментів.

Аналіз класичних фізичних топологій показує, що для сучасної медичної установи використання шинної або кільцевої структур є недоцільним через їхню низьку відмовостійкість та складність у діагностиці несправностей. Зокрема, у шинній топології розрив центрального кабелю призводить до зупинки всієї мережі, що є неприпустимим для роботи медичних інформаційних систем та передачі даних з діагностичного обладнання в реальному часі. Кільцева топологія, хоч і забезпечує певну передбачуваність часу затримки, залишається вразливою до виходу з ладу окремих вузлів, якщо не використовувати дорогі технології резервування.

Оптимальним базовим рішенням для побудови локальних обчислювальних мереж традиційно вважається фізична топологія типу «зірка». У такій структурі всі кінцеві пристрої, такі як робочі станції лікарів, термінали реєстратури чи медичне обладнання, підключаються безпосередньо до єдиного центрального комутаційного вузла [4].

Цей підхід забезпечує високий рівень надійності: пошкодження кабелю до окремого пристрою впливає лише на цей конкретний вузол і не порушує працездатність усієї системи. Крім того, централізація потоків даних значно спрощує адміністрування мережі, локалізацію несправностей та впровадження

політик інформаційної безпеки безпосередньо на портах комутатора. Проте класична топологія «зірка» має суттєві фізичні та логічні обмеження при її застосуванні у масштабах цілої медичної установи.

Враховуючи, що лише в головному корпусі клініки передбачається розгортання близько сорока різнотипних мережевих пристроїв, об’єднати їх усі за допомогою єдиного центрального комутатора технічно складно та економічно неефективно. Це вимагало б прокладання величезної кількості довгих кабельних трас до однієї серверної кімнати, що часто порушує стандарти щодо максимальної довжини мідного кабелю та перетворює центральний комутатор на єдину критичну точку відмови для всієї життєдіяльності клініки.

Зважаючи на зазначені просторові та технічні обмеження, для розбудови інформаційної інфраструктури клініки обґрунтовано доцільним є перехід від базової концепції до топології «розширена зірка», яка також відома як ієрархічна або деревоподібна структура.

Ця архітектурна модель передбачає наявність центрального комутатора ядра мережі (див. рис. 2.1), до якого підключаються комутатори рівня доступу, розташовані у різних відділеннях (наприклад, у зоні реєстратури, кабінетах профільних лікарів чи адміністрації), а вже до них безпосередньо приєднуються робочі станції та периферія [4].

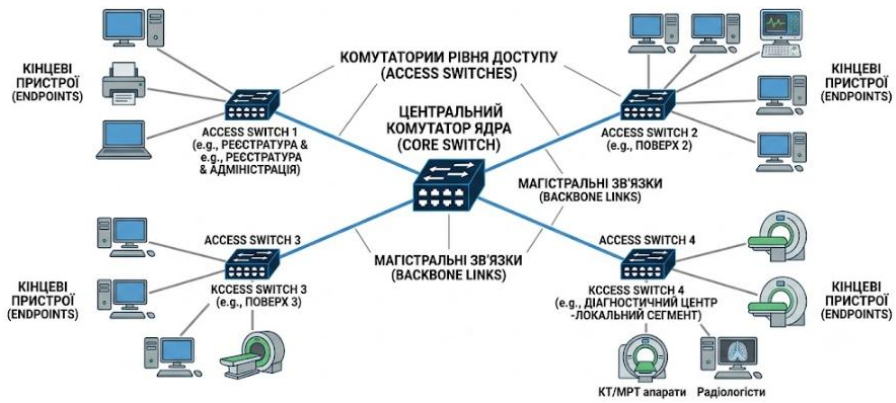


Рисунок 2.1 – Ієрархічна модель мережі клініки

Такий ієрархічний підхід ідеально відповідає фізичній та організаційній структурі закладу. Він дозволяє локалізувати внутрішній трафік окремих

підрозділів на рівні відповідних комутаторів доступу, розвантажуючи магістральні канали зв'язку. До того ж топологія «розширена зірка» забезпечує надзвичайно високу гнучкість: при створенні нових робочих місць або встановленні додаткового медичного обладнання достатньо підключити їх до найближчого периферійного комутатора, не порушуючи роботу центрального ядра мережі.

Особливої уваги потребує організація зв’язку між головним корпусом та віддаленим діагностичним центром. Оскільки будівлі територіально рознесені і прокладання прямих власних ліній зв’язку є неможливим, взаємодія здійснюється через відкриту мережу Інтернет.

Для забезпечення конфіденційності медичних даних та цілісності інформації при передачі через публічне середовище єдино правильним рішенням є побудова захищених VPN-тунелів (Virtual Private Network). Використання технологій криптографічного захисту на шлюзах обох локацій дозволяє створити єдиний захищений інформаційний простір клініки, де трафік між корпусами надійно зашифрований і захищений від перехоплення чи модифікації сторонніми особами.

Щодо технологічного базису, стандартом для побудови такої мережі виступає родина технологій Ethernet. Для підключення кінцевих вузлів на рівні доступу передбачається використання стандарту Gigabit Ethernet по витій парі, що гарантує швидкий доступ персоналу до електронної системи охорони здоров'я. Для магістральних з’єднань між комутаторами застосовуються оптичні стандарти вищих швидкостей. Окремо слід передбачити впровадження технології живлення по локальній мережі (PoE), що дасть змогу забезпечити енергопостачання мережевих принтерів безпровідних точок доступу для гостьового сегменту, безпосередньо через інформаційні кабелі, мінімізуючи кількість силових ліній.

Основним інструментом забезпечення безпеки на канальному рівні у цій розгалуженій структурі є технологія віртуальних локальних мереж (VLAN). Її інтеграція дозволяє логічно розділити фізичну інфраструктуру «розширеної зірки» на декілька цілком ізольованих широкомовних доменів: адміністративний, медичний, фінансовий, гостьовий та виділений сегмент для діагностичного об-

ладнання. Цей логічний поділ є важливим заходом для запобігання несанкціонованому перехопленню медичної таємниці та захисту персональних даних пацієнтів. Крім того, жорстка ізоляція сегмента з апаратами МРТ та КТ від мережі загального користування унеможливлює вплив стороннього трафіку чи шкідливого програмного забезпечення на стабільність роботи цих життєво важливих пристроїв.

Для розбудови горизонтальної підсистеми від комутаторів до робочих місць застосовується неекранована вита пара (UTP) категорії 6 або вище, що створює необхідний резерв пропускної здатності на майбутнє.

У приміщеннях діагностичного центру, де існує висока ймовірність впливу потужного електромагнітного випромінювання від медичної апаратури, необхідно застосовувати екрановану виту пару (FTP) для захисту інформаційних потоків від спотворень.

У підсумку, продумана синергія топології «розширена зірка», сучасних технологій передачі даних та глибокої логічної сегментації формує високопродуктивний, відмовостійкий і масштабований фундамент інфраструктури клініки «МедЛайф-Плюс», повністю готовий до розгортання наступних рівнів криптографічного та програмно-апаратного захисту інформації.

Повна топологія мережі представлена у додатку Б.

2.2 Вибір кабельного середовища та розташування вузлів мережі

Переведення логічної структури мережі клініки «МедЛайф-Плюс» у площину фізичної реалізації вимагає прийняття ряду критичних проєктних рішень щодо вибору середовища передачі даних та стратегічного розміщення комутаційного обладнання. Базуючись на аналізі геометричних параметрів будівель, функціонального призначення приміщень та щільності розміщення кінцевих вузлів, визначеної у таблиці обладнання, процес проєктування структурованої кабельної системи (СКС) здійснюється диференційовано для

кожного корпусу з метою забезпечення максимальної продуктивності та надійності.

Першочерговим етапом проєктування є вибір кабельного середовища для горизонтальної підсистеми. Враховуючи необхідність підтримки гігабітних швидкостей (1000BASE-T) для переважної більшості кінцевих пристроїв, таких як робочі станції адміністрації та лікарів, та мережеві принтери, базовим рішенням для обох корпусів доцільно обрати кабель на основі витої пари UTP категорії 6. Використання неекранованого кабелю Cat 6 є економічно обґрунтованим для більшості приміщень, оскільки забезпечує необхідний запас пропускної здатності на відстані до 100 метрів та підтримує технологію Power over Ethernet (PoE) для бездротових точок доступу [2].

Водночас, аналіз планів приміщень (див. додаток А) та таблиці обладнання виявляє зони з високим рівнем електромагнітних завад (EMI). До таких зон належать приміщення, де розміщено потужне медичне обладнання (КТ, МРТ), а також суміжні з ними лабораторії.

Для забезпечення цілісності критично важливих діагностичних даних та стабільної роботи мережі, при проєктуванні горизонтальних трас, що обслуговують ці специфічні зони, вирішено застосувати екрановану виту пару категорії 6а типу F/UTP або SF/UTP. Використання екрану у поєднанні з обов'язковим заземленням комутаційних шаф гарантуватиме захист інформаційних сигналів від зовнішніх наведень.

Ключовим рішенням щодо топології та розміщення вузлів у головному корпусі стає організація центрального комутаційного вузла. Аналіз плану приміщень (додаток А) дозволяє визначити оптимальне місце для його розташування – виділене приміщення "СЕРВЕРНА".

Це приміщення розташоване географічно ближче до геометричного центру будівлі, що мінімізує довжину кабельних трас та забезпечує можливість підключення всіх кінцевих вузлів на цьому поверсі з дотриманням стандарту 100 метрів. У цій серверній кімнаті планується встановлення підлогової комутаційної шафи

(RACK) відповідної ємності, яка виконуватиме роль головного кросу (MC) будівлі та центру ядра мережі.

До цієї серверної шафи в головному корпусі буде підведено зовнішній канал від інтернет-провайдера. Відповідно, у ній буде розміщено оптичний крос (FODF), ONT або медіаконвертер, а також ключове активне обладнання: комутатор ядра, сервери медичної системи та межовий маршрутизатор із функцією VPN-шлюзу. Саме цей маршрутизатор у точці входу інтернету забезпечуватиме криптографічний захист усього трафіку, що спрямовується через відкриту мережу до віддаленого діагностичного центру, створюючи захищений тунель між двома локаціями. Від шафи в серверній розходитимуться горизонтальні кабельні траси (UTP та F/UTP Cat 6/6a) до патч-панелей, що обслуговують кінцеві пристрої на поверсі.

Проєктне розташування кінцевих точок підключення (Wall Port, WP) та кількість вузлів у головному корпусі базується на функціональному зонуванні та даних таблиці 1.2:

- у зоні реєстратури передбачається максимальна щільність підключень: для обслуговування ПК реєстратури, принтерів та IP-телефонів заплановано встановлення групи з 5 розеток (Wall Port №1 - Wall Port №5) біля стійки. Таке рішення дозволяє забезпечити повноцінну роботу 3 робочих місць реєстраторів та периферійного обладнання;

- у адміністративних приміщеннях (кабінетах адміністрації та лікарів) вирішено встановити подвійні розетки на кожному робочому місці (наприклад, Wall Port №9, Wall Port №12-WP№14), що забезпечить підключення ПК та для 14 робочих місць;

- у специфічних приміщеннях, таких як лабораторія та зони МРТ та КТ, які ідентифіковані на плані, необхідно спроєктувати екрановані Wall Port (WP), підключені кабелем F/UTP Cat 6a. Це стосується щонайменше 2 медичних апаратів та супутніх робочих станцій, що знаходяться у безпосередній близькості до джерел випромінювання;

- для забезпечення бездротового покриття у холах та коридорах, біля кабінетів лікарів, заплановано місця для стельових точок доступу, які підключатимуться до комутаторів з підтримкою PoE.

Для віддаленого діагностичного центру, який територіально рознесений та об’єднується з головним корпусом через VPN, необхідно спроєктувати локальний комутаційний вузол. Враховуючи меншу кількість користувачів, але високу критичність обладнання, для розміщення локальної 19-дюймової комутаційної шафи доцільно виділити технічне приміщення або захищену нішу.

У цій локальній шафі буде розміщено комутатор доступу (Access Switch Diagnosis Center), патч-панелі (PP), та локальний VPN-маршрутизатор, який підключатиметься до власного інтернет-каналу. Ця точка стане кінцевим пунктом VPN-тунелю, що надійно зашифрує трафік між корпусами.

Від локальної шафи діагностичного центру розходитимуться кабельні траси UTP Cat 6 для робочих станцій радіологів (кількість вузлів згідно таблиці 1.2) та екрановані траси F/UTP Cat 6a для безпосереднього підключення апаратів комп'ютерної та магнітно-резонансної томографії. Мережеві рохетки у діагностичному центрі також будуть розміщені безпосередньо біля відповідних медичних апаратів та робочих столів радіологів. Таким чином, продуманий вибір кабелів, стратегічне розташування серверної кімнати в головному корпусі та локальної шафи в діагностичному центрі, а також точне планування точок підключення Wall Port та WAP формують надійний, відмовостійкий і завадостійкий фізичний фундамент для розгортання захищеної мережі клініки.

2.3 Обґрунтування вибору комунікаційного обладнання

Проєктування цілісної інформаційної системи клініки «МедЛайф-Плюс» вимагає комплексного підходу до вибору комунікаційного обладнання, яке поділяється на пасивну та активну складові. Пасивне обладнання формує фізичну основу (тракт передачі даних), тоді як активне забезпечує інтелектуальне керування потоками інформації та безпеку. Надійність мережі прямо

залежить від якості середовища передачі, тому першочерговим завданням є вибір кабельної продукції, комутаційних вузлів та засобів монтажу.

Основою кабельної системи клініки обрано мідну виту пару, оскільки цей тип середовища забезпечує оптимальний баланс між вартістю та продуктивністю для локальних мереж. Для більшості адміністративних та лікувальних приміщень головного корпусу доцільно використовувати неекрановану виту пару (UTP) категорії 6.

Для побудови лінійних трактів горизонтальної підсистеми СКС в адміністративних зонах, реєстратурі та кабінетах консультаційного прийому обрано мідний кабель типу «вита пара» українського виробництва ПАТ «Одескабель» марки Одескабель КПВ-ВП (250) 4х2х0,57 (UTP-cat.6). Даний кабель має мідні жили діаметром 0,57 мм (23 AWG), ізольовані поліолефіном, та захисну оболонку з ПВХ-пластикату. Він повністю забезпечує роботу стандартів Gigabit Ethernet на частотах до 250 МГц та гарантує стабільну передачу даних без згасання сигналу на відстані до 100 метрів [12].

Для прокладання ліній у зонах з підвищеним рівнем електромагнітного випромінювання (кабінети УЗД, ЕКГ, рентген-діагностики та зони поблизу КТ/МРТ апаратів), з метою захисту медичного трафіку від наведень, обрано фольгований кабель цього ж виробника – Одескабель КПВЭ-ВП (500) 4х2х0,57 (F/UTP-cat.6A). Цей кабель оснащений загальним екраном з алюмополімерної стрічки (фольги) з дренажним провідником і оболонкою з матеріалу, що не підтримує горіння (LSOH), що підвищує пожежну безпеку медичної установи [12].

Термінація кабельних ліній на робочих місцях здійснюється за допомогою модульних розеток на базі модулів Keystone Jack Одескабель OK-KJ6-U для стандартних вузлів та екранованих модулів OK-KJ6A-S для діагностичного обладнання.

З’єднання кінцевого обладнання з розетками та активного обладнання в шафі здійснюється за допомогою заводських патч-кордів для гарантування мінімальних перехресних наведень. Обрано моделі Одескабель PC-UTP-Cat6-

1.5m-GY для стандартних ліній та Одескабель PC-FTP-Cat6A-2m-BL для екранованих сегментів діагностики.

Розрахунок параметрів комутаційної шафи для головного корпусу базується на сумарній висоті всіх активних та пасивних компонентів, що вимірюється в монтажних одиницях (юнітах).

У шафу головного корпусу планується встановити:

- дві патч-панелі Одескабель OK-PP-24-U6 (2U загалом);
- два кабельні організатори для впорядкування патч-кордів (2U);
- керований комутатор Cisco Catalyst 9200L (1U);
- межовий маршрутизатор Cisco ISR 1111 (1U);
- мережевий сервер (Rack-unit) 2U;
- блок розеткових розподільників живлення (1U)
- полицю з джерелом безперебійного живлення (2U).

Сумарне завантаження становить 9U. З урахуванням необхідності 30% технологічного резерву для вентиляції та майбутнього розширення, обрано настінну 19-дюймову шафу Одескабель CH-12U-06-06-П-С з габаритами 637х600х600 мм (ВхШхГ), зовнішній вигляд якої представлено на рисунку 2.2.

Рисунок 2.2 – Зовнішній вигляд комутаційної шафи Одескабель CH-12U-06-06-П-С

Для діагностичного центру, де кількість ліній значно менша, достатньо встановлення шафи Одескабель CH-6U-06-04-П-С (368х600х450 мм), яка вміщує одну патч-панель, маршрутизатор та блок живлення (загалом 4U з резервом у 2U).

Для діагностичного центру, де кількість ліній значно менша, достатньо встановлення шафи Одескабель СН-6U-06-04-П-С (368х600х450 мм), зовнішній вигляд якої представлено на рисунку 2.3, Дана шафа вміщує одну патч-панель, маршрутизатор та блок живлення (загалом 4U з резервом у 2U)

Рисунок 2.3 – Зовнішній вигляд комутаційної шафи Одескабель 6U-06-04-П-С

Центральним елементом комутації в шафах обох корпусів є патч-панелі, які забезпечують перехід від лінійних кабелів, прокладених від кабінетів, до гнучких патч-кордів, що підключаються до активного обладнання Cisco. Враховуючи обраний стандарт категорій 6 та 6А, а також використання продукції ПАТ «Одескабель», для проєкту обрано для головного корпусу, де зафіксовано 40 робочих місць (згідно з таблицею 1.1), необхідно забезпечити відповідну кількість портів із резервом. Обрано дві патч-панелі Одескабель OK-PP-24-U6 (див. рис. 2.4).

Рисунок 2.4 – Зовнішній вигляд патч-панелі Одескабель OK-PP-24-U6

Це стандартні 19-дюймові неекрановані панелі висотою 1U на 24 порти RJ-45 кожна. Сумарна ємність двох панелей складає 48 портів, що дозволяє підключити всі 40 ліній корпусу та залишити 8 портів (20%) для майбутнього розширення мережі. Панелі мають цифрову маркіровку портів та майданчики для додаткових підписів, що спрощує адміністрування.

Для діагностичного центру, де використовуються екрановані лінії від апаратів КТ та МРТ (згідно з таблицею 1.2), обрано екрановану патч-панель Одескабель ОК-РР-24-F6A (24 порти, Cat.6A FTP). Металевий корпус панелі та наявність загальної шини заземлення дозволяють замкнути екрануючий контур, що йде від діагностичного обладнання, захищаючи мережу від перешкод. 24 порти панелі повністю охоплюють 12 вузлів філії з двократним запасом ємності.

Для з'єднання патч-панелей із комутатором Cisco та сервера з мережею обрано патч-корди Одескабель PC-UTP-Cat6-0.5m-GY (довжина 0,5 м ідеальна для комутації всередині шафи, щоб уникнути хаосу дротів). Для підключення кінцевих ПК у кабінетах до розетки обрано патч-корди довжиною 1,5 м та 3 м залежно від віддаленості системного блока.

Наступним етапом розробки є вибір активного мережевого обладнання. Логічна структура мережі закладу безпосередньо відображає його фізичне розміщення та функціональний розподіл підрозділів. Головний корпус клініки має двоповерхову структуру (див. додаток А), на кожному з поверхів якої розгорнуто окремі комутаційні вузли доступу. Загальна кількість робочих місць у головному корпусі становить сорок вузлів, які розподілені між поверхами нерівномірно, відповідно до специфіки роботи медичного й адміністративного персоналу.

На першому поверсі головного корпусу зосереджені підрозділи з високою інтенсивністю взаємодії з пацієнтами. До першого комутатора доступу підключаються шість персональних комп'ютерів реєстратури та рецепції, чотири комп'ютери денного стаціонару та медсестринських постів, а також шість кабінетів профільних лікарів первинного прийому. Крім того, на першому поверсі розміщено два пристрої загальної мережевої периферії, що включають мережеві багатофункціональні пристрої.

Таким чином, до комутатора першого поверху сумарно підключається вісімнадцять активних робочих вузлів, що при використанні двадцятичотирьохпортового комутатора забезпечує оптимальний технологічний резерв у розмірі двадцяти п'яти відсотків для майбутнього розширення клініки.

На другому поверсі головного корпусу розташовані адміністративні та фінансові служби, а також кабінети вузьких спеціалістів. Комутатор доступу другого поверху об'єднує шість робочих місць адміністрації та відділу кадрів, чотири комп'ютери бухгалтерії та фінансового відділу, а також десять кабінетів профільних лікарів. До цього ж пристрою підключаються два периферійні пристрої адміністративного крила корпусу. Сумарне навантаження на комутатор другого поверху становить двадцять два активні вузли. Встановлення на другому поверсі комутатора на двадцять чотири порти є повністю виправданим, оскільки воно покриває поточні потреби та залишає вільні порти для короткострокового підключення діагностичного чи презентаційного обладнання.

Окремим незалежним сегментом мережі є віддалений діагностичний центр, логічна топологія якого передбачає підключення дванадцяти пристроїв, серед яких цифрова медична апаратура, лабораторні аналізатори та автоматизовані робочі місця лікарів-радіологів. Для забезпечення комутації в діагностичному центрі також проектується двадцятичотирьохпортовий комутатор, що гарантує стовідсотковий запас ємності та високу завадостійкість ліній передачі даних. Таким чином, загальна комутаційна структура доступу клініки складається з трьох однотипних вузлів на двадцять чотири порти кожен, що суттєво полегшує процес уніфікації мережі.

Першочерговим завданням безпеки та зв'язку є вибір центрального пристрою периметра мережі, який суміщатиме функції маршрутизації, захисту та прямого підключення до волоконно-оптичних ліній зв'язку інтернет-провайдерів.

Наявність інтегрованих оптичних портів SFP на межовому пристрої є обов'язковою інженерною вимогою, оскільки це забезпечує гальванічну ізоляцію внутрішньої мережі клініки від зовнішніх наведень, гарантує високу пропускну здатність каналу та унеможливлює використання додаткових медіаконвертерів, які створюють додаткові точки відмови.

Оскільки мережа оперує медичною таємницею, центральний шлюз повинен належати до класу міжмережевих екранів нового покоління (NGFW) та

мати апаратне прискорення для створення шифрованих VPN-тунелів із діагностичним центром. Для порівняльного аналізу в межах проекту було обрано три актуальні моделі з вбудованими оптичними інтерфейсами, а саме Cisco Firepower 1120, Fortinet FortiGate 70F та MikroTik RB5009UG+S+IN..

Порівняльний аналіз технічних характеристик та інтегрованих сервісів безпеки межових захисних пристроїв наведено в таблиці 2.1.

Таблиця 2.1 – Порівняльний аналіз захищених маршрутизаторів периметра мережі

Критерій порівняння	Cisco Firepower 1120	Fortinet FortiGate 70F	MikroTik RB5009UG+S+IN
Клас мережевого пристрою	Міжмережевий екран NGFW	Міжмережевий екран NGFW	Маршрутизатор з Firewall
Оптичні інтерфейси (SFP)	4 x 1GE SFP	2 x 1GE SFP	1 x 10G SFP+
Мідні інтерфейси (RJ-45)	4 x 1GE RJ-45	10 x 1GE RJ-45	7 x 1GE, 1 x 2.5GE
Пропускна здатність Firewall	2.3 Гбіт/с	10 Гбіт/с	10 Гбіт/с (L3 routing)
Пропускна здатність IPS / NGFW	2.6 Гбіт/с / 2.3 Гбіт/с	1.4 Гбіт/с / 1 Гбіт/с	Відсутній повноцінний DPI
Пропускна здатність IPsec VPN	1.2 Гбіт/с	6.5 Гбіт/с	430 Мбіт/с
Інтегровані сервіси безпеки	Cisco Talos, IPS, AMP	FortiGuard Labs, IPS	Базовий Firewall (L4)
Базова операційна система	Cisco Firepower Threat Defense	FortiOS	RouterOS v7

Аналіз результатів порівняння показує, що для проекту захищеної мережі медичної клініки «МедЛайф-Плюс» з прямим виходом в оптичний інтернет

остаточний вибір зупинено на міжмережевому екрані Cisco Firepower 1120, зовнішній вигляд якого представлено на рисунку 2.5.

Рисунок 2.5 – Зовнішній вигляд міжмережевого екрана Cisco Firepower 1120

Ця модель повністю задовольняє вимоги гнучкості завдяки наявності чотирьох незалежних оптичних портів SFP, що дозволяє не лише підключити основний високошвидкісний канал від провайдера по оптиці, але й організувати резервний оптичний канал або виділений фізичний лінк на внутрішню магістраль.

Головною перевагою є висока продуктивність інспекції трафіку та інтеграція з глобальною аналітикою кіберзагроз Cisco Talos, яка блокує цілеспрямовані атаки на медичні установи в режимі реального часу. Пропускна здатність IPsec VPN на рівні 1.2 Гбіт/с забезпечує колосальний запас для обміну важкими графічними даними з філією.

Наступним кроком проектування є вибір комутаційного обладнання для побудови внутрішньої мережі доступу на основі розрахованої кількості вузлів. З огляду на необхідність уніфікації активного обладнання та спрощення обслуговування мережі, для всіх трьох комутаційних вузлів (перший поверх, другий поверх та діагностичний центр) доцільно обрати однакові моделі двадцятичотирьохпортових керованих комутаторів з підтримкою технології PoE+.

Це дозволить забезпечити стабільне живлення, мережевих камер та бездротових точок доступу. Для порівняльного аналізу комутаторів робочих груп було обрано три моделі корпоративного класу, до яких увійшли Cisco Catalyst 9200L-24P-4G-E, HPE Aruba CX 6000 24G PoE та Huawei CloudEngine S5735-L24P4X-A.

Технічні параметри та вбудовані механізми безпеки комутаторів доступу на двадцять чотири порти відображено в таблиці 2.2.

Таблиця 2.2 – Порівняльний аналіз комутаторів доступу

Критерій порівняння	Cisco Catalyst 9200L-24P-4G-E	HPE Aruba CX 6000 24G	Huawei CloudEngine S5735-L24P4X-A
Інтерфейси доступу	24 x 10/100/1000 Base-T	24 x 10/100/1000 Base-T	24 x 10/100/1000 Base-T
Магістральні порти (Uplink)	4 x 1G SFP	4 x 1G SFP	4 x 10G SFP+
Загальний бюджет потужності PoE	370 Вт	370 Вт	370 Вт
Підтримка технології стекування	Наявна (StackWise-80)	Відсутня	Наявна (iStack)
Апаратні функції безпеки	MACsec-128, TrustSec, ACL	802.1X, DHCP Snooping	802.1X, DoS-defense
Механізми якості обслуговування	Розширений QoS (8 черг)	Базовий QoS (Strict)	Базовий QoS (SP/WRR)
Платформа управління	Cisco IOS XE	ArubaOS-CX	VRP

За результатами проведеного аналізу для встановлення на обох поверхах головного корпусу та в діагностичному центрі обрано комутатори Cisco Catalyst 9200L-24P-4G-E, щовнішній вигляд якого представлено на рисунку 2.6.

Вибір ідентичних пристроїв на базі операційної системи Cisco IOS XE спрощує централізоване адміністрування та дозволяє реалізувати наскрізні політики безпеки [14].

Для головного корпусу наявність технології StackWise-80 дозволяє у майбутньому об'єднати комутатори першого та другого поверхів у єдиний

логічний стек із загальною пропускною здатністю до 80 Гбіт/с, що значно підвищить швидкість обробки внутрішнього трафіку та спростить керування інфраструктурою будівлі. Бюджет PoE у 370 Вт повністю задовольняє потребам кожної робочої групи.

Рисунок 2.6 – Зовнішній вигляд комутатора Cisco Catalyst 9200L-24P-4G-E

Особливу роль у виборі Cisco Catalyst відіграє посилений комплекс вбудованих апаратних функцій захисту [14]. Технологія Port Security дозволяє жорстко закріпити фізичні порти комутатора за унікальними MAC-адресами комп'ютерів лікарів чи діагностичних апаратів, унеможливлюючи несанкціоноване підключення сторонніх пристроїв у кабінетах. Підтримка технологій DHCP Snooping, Dynamic ARP Inspection та IP Source Guard надійно захищає внутрішній простір клініки від поширених мережевих атак, пов'язаних із підміною адрес та перехопленням медичних даних пацієнтів. Розширені механізми якості обслуговування (QoS) гарантують найвищий пріоритет для важких графічних файлів знімків КТ та МРТ, що виключає затримки та втрати пакетів під час їх передачі на сервери медичної інформаційної системи.

Завершальним етапом формування активного контуру є вибір бездротового обладнання для розгортання мережі Wi-Fi корпоративного класу. Для медичного закладу критично важливо використовувати точки доступу сучасного стандарту Wi-Fi 6 (802.11ax), який забезпечує стабільну роботу великої кількості бездротових клієнтів в умовах щільної забудови та мінімізує взаємні завади від медичного обладнання.

Бездротова інфраструктура повинна підтримувати технологію мультиплексування OFDMA, шифрування WPA3-Enterprise для надійної автентифікації персоналу, а також можливість створення кількох ізольованих віртуальних бездротових мереж (Multi-SSID) з прив'язкою до відповідних VLAN.

Для порівняльного аналізу в проекті розглядаються три моделі корпоративних точок доступу внутрішнього виконання, які підтримують централізоване керування та отримують живлення за технологією PoE від обраних комутаторів доступу, а саме Cisco Catalyst 9115AXI-E, Aruba AP-505 та Ubiquiti UniFi U6 Pro.

Порівняльні технічні характеристики та функціонал безпеки бездротових точок доступу наведено в таблиці 2.3.

Таблиця 2.3 – Порівняльний аналіз бездротових точок доступу Wi-Fi 6

Критерій порівняння	Cisco Catalyst 9115AXI-E	Aruba AP-505	Ubiquiti UniFi U6 Pro
Стандарт бездротового зв'язку	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Конфігурація антен (MIMO)	4x4 (5 ГГц), 2x2 (2.4 ГГц)	2x2 (5 ГГц), 2x2 (2.4 ГГц)	4x4 (5 ГГц), 2x2 (2.4 ГГц)
Макс. швидкість	До 5.38 Гбіт/с	До 1.77 Гбіт/с	До 5.3 Гбіт/с
Інтерфейс підключення (Uplink)	1 x 2.5 Gbps Ethernet	1 x 1 Gbps Ethernet	1 x 1 Gbps Ethernet
Стандарти живлення	PoE (802.3af)	PoE (802.3af)	PoE (802.3af)
Підтримка безпеки WPA3	Enterprise / Personal	Enterprise / Personal	Enterprise / Personal
Архітектура керування	Embedded Wireless Controller	Aruba Central / Virtual Controller	UniFi Network Application

Аналіз характеристик демонструє значну перевагу моделі Cisco Catalyst 9115AXI-E (див. рис. 2.7), яка і стає остаточним вибором для реалізації бездрото-

вого сегмента мережі клініки. Наявність повноцінної антенної конфігурації 4x4 MU-MIMO на частоті 5 ГГц дозволяє точці доступу одночасно обслуговувати кілька важких потоків даних, що є критичним при передачі медичних знімків високої роздільної здатності на мобільні термінали лікарів.

Рисунок 2.7 – Зовнішній вигляд комутатора Cisco Catalyst 9115AXI-E

Наявність швидкісного інтерфейсу підключення 2.5 Gbps Ethernet усуває ефект «вузького горла» на рівні дротового лінка до комутатора. Завдяки технології Cisco Embedded Wireless Controller керування всіма точками доступу здійснюється централізовано безпосередньо з однієї з точок, що виключає необхідність купівлі окремого апаратного контролера та спрощує адміністрування.

Точки доступу інтегруються в загальну систему моніторингу Cisco, підтримують виявлення сторонніх точок (Rogue AP) та забезпечують безшовний роумінг при переміщенні персоналу між поверхами та будівлями. Для повного покриття об'єктів клініки проектується встановлення шести таких пристроїв, розподілених порівну по два блоки на кожен комутаційний вузол доступу.

У підсумку, побудова активного контуру мережі медичної клініки «МедЛайф-Плюс» на базі сумісного обладнання від компанії Cisco дозволяє створити монолітну, легко керовану та відмовостійку інфраструктуру з можливістю прямої термінації оптичних ліній зв'язку. Усі обрані пристрої ідеально взаємодіють між собою на протокольному рівні, підтримують розгортання наскрізних віртуальних локальних мереж для ізоляції різних підрозділів клініки та забезпечують багаторівневий технічний захист інформації, що повністю відповідає розробленій логічній топології мережі закладу.

2.4 Особливості монтажу мережі

Фізичний монтаж інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс» є дуже важливим важливим етапом, від якості виконання якого безпосередньо залежить надійність, довговічність та пропускна здатність усієї інфраструктури.

Основу горизонтальної кабельної підсистеми головного корпусу складає мідний кабель «вита пара» категорії 6 від вітчизняного виробника ПАТ «Одескабель». Використання кабелю шостої категорії є необхідною умовою для забезпечення стабільної роботи мережі за технологією GigabitEthernet на всіх сорока робочих місцях клініки.

Відповідно до розроблених монтажних схем першого та другого поверхів (див. додаток В), прокладання кабельних трас здійснюється комбінованим способом. Основні магістральні пучки кабелів проходять у прихованих металевих перфорованих лотках за підвісною стелею коридорів, що забезпечує їх надійний захист, належну вентиляцію та зберігає естетичний вигляд медичних приміщень.

Спуски інформаційних кабелів безпосередньо до робочих місць медичного та адміністративного персоналу реалізуються за допомогою настінних пластикових кабель-каналів із суворим дотриманням допустимого радіуса вигину. Для мінімізації електромагнітних наведень на лінії передачі даних, слабкострумові траси прокладаються на відстані не менше тридцяти сантиметрів від силових електричних ліній.

Центральним вузлом комутації кожного поверху є дев'ятнадцятидюймова телекомунікаційна шафа. На першому поверсі, де зосереджена рецепція площею 7,5 на 4,5 метри та кабінети лікарів первинного прийому, комутаційна шафа встановлюється у спеціально відведеному технічному приміщенні з обмеженим доступом.

Аналогічна настінна шафа монтується на другому поверсі для обслуговування адміністративного крила, бухгалтерії та додаткових медичних

кабінетів. Усередині кожної шафи виконується жорстка фіксація активного мережевого обладнання, зокрема міжмережевого екрану Cisco Firepower 1120 та керованих комутаторів доступу Cisco Catalyst 9200L.

Розшивка інформаційних кабелів категорії 6 здійснюється на двадцятичотирьохпортові неекрановані патч-панелі за міжнародним стандартом T568B. Для організації акуратного та впорядкованого вигляду кабельного господарства всередині шаф обов'язковим є встановлення горизонтальних кабельних організаторів висотою 1U, що розміщуються між активними комутаторами та пасивними патч-панелями.

Підключення кінцевих пристроїв на робочих місцях реалізується через встановлення зовнішніх інформаційних розеток із модулями стандарту RJ-45 відповідної шостої категорії. У медичних кабінетах розетки монтуються на висоті, що унеможливлює їх випадкове механічне пошкодження під час переміщення габаритного медичного обладнання або проведення регулярного вологого санітарного прибирання.

Особлива увага під час монтажних робіт приділяється розташуванню корпоративних бездротових точок доступу Cisco Catalyst 9115AXI-E. Згідно з планами поверхів, вони кріпляться безпосередньо до напрямних профілів підвісної стелі у шаховому порядку для забезпечення рівномірного покриття радіосигналом Wi-Fi усієї площі клініки без утворення "мертвих зон".

Підведення живлення до точок доступу здійснюється по тих самих мідних інформаційних кабелях за стандартом PoE+, що повністю виключає необхідність прокладання додаткових електричних ліній 220В до місць їх встановлення на стелі.

Зв'язок із єдиним віддаленим діагностичним центром клініки забезпечується через підключення до волоконно-оптичної магістралі інтернет-провайдера. Оптичний кабель заводиться в серверну шафу першого поверху та термінується в оптичному кросі (ODF), який захищає крихкі місця зварювання оптичних волокон. Від кросу оптичний патч-корд підключається безпосередньо у відповідний SFP-модуль міжмережевого екрану периметра.

На завершальному етапі монтажних робіт проводиться обов'язкове інструментальне тестування всіх мідних ліній кабельним аналізатором на відповідність вимогам категорії 6, а також здійснюється суворе фізичне маркування.

Кожен прокладений кабель, кожна інформаційна розетка та кожен порт на патч-панелі позначається унікальним ідентифікатором за допомогою промислового принтера етикеток. Це маркування заноситься до кабельного журналу проекту, що гарантує швидку ідентифікацію будь-якого вузла та суттєво спрощує подальшу експлуатацію і технічне обслуговування локальної мережі медичного закладу.

2.5 Обґрунтування вибору програмного забезпечення

Для повноцінного функціонування спроєктованої захищеної інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс» фундаментальним етапом після затвердження апаратної бази є технічне обґрунтування вибору системного та прикладного програмного забезпечення. Першочерговим завданням є вибір базової серверної операційної системи, яка слугуватиме ядром усієї IT-інфраструктури закладу.

Серверна платформа повинна забезпечувати надійне функціонування медичної інформаційної системи (МІС), збереження баз даних електронних медичних карток, а також підтримку служб централізованого управління правами доступу користувачів. З огляду на специфіку медичного закладу, де циркулює конфіденційна інформація, операційна система повинна відповідати найвищим стандартам інформаційної безпеки та підтримувати інтеграцію з мережевим обладнанням Cisco для реалізації автентифікації на рівні портів.

Для порівняльного аналізу було обрано три передові серверні платформи корпоративного рівня: комерційну систему Microsoft Windows Server 2025, відкриту платформу Ubuntu Server 26.04 LTS та спеціалізовану комерційну систему Red Hat Enterprise Linux 9. Детальні порівняльні характеристики розглянутих серверних операційних систем наведено в таблиці 2.4.

Таблиця 2.4 – Порівняльний аналіз серверних операційних систем

Критерій порівняння	Microsoft Windows Server 2022	Ubuntu Server 26.04 LTS	Red Hat Enterprise Linux 9
Модель ліцензування	Комерційна (за ядрами та CAL-ліцензіями)	Відкритий вихідний код (безкоштовна)	Комерційна підписка (Enterprise Support)
Служба каталогів	Нативна служба Active Directory (AD DS)	Сторонні пакети (Samba4, FreeIPA)	Інтегрована система Red Hat Identity Management
Інтеграція з мережею (802.1X)	Вбудований сервер Network Policy Server (RADIUS)	Потребує налаштування FreeRADIUS	Потребує налаштування FreeRADIUS
Сумісність із медичним ПЗ	Максимальна (сервери PACS, DICOM-шлюзи, МІС)	Висока (для веб-орієнтованих МІС та баз даних)	Висока (сертифікована для медичних баз даних)
Централізоване управління	Групові політики (GPO), Windows Admin Center	Засоби автоматизації Ansible, Puppet	Платформа Red Hat Satellite
Технічна підтримка	Глобальна комерційна підтримка Microsoft	Підтримка спільноти (опціонально від Canonical)	Преміальна цілодобова підтримка рівня Enterprise

За результатами проведеного порівняльного аналізу для розгортання ядра мережі клініки «МедЛайф-Плюс» обрано серверну операційну систему Microsoft Windows Server 2022.

Вирішальним аргументом на користь цієї платформи є наявність неперевершеної екосистеми Active Directory, яка дозволяє створити єдиний корпоративний домен для головного корпусу та діагностичного центру.

За допомогою механізмів групових політик (GPO) системний адміністратор зможе централізовано та жорстко регламентувати права доступу

лікарів і персоналу до медичних файлів, блокувати використання зовнішніх USB-накопичувачів та примусово застосовувати політики складності паролів [7].

Крім того, наявність вбудованої ролі Network Policy Server (NPS) дозволяє легко розгорнути RADIUS-сервер для протоколу 802.1X, що ідеально інтегрується з обраними комутаторами Cisco Catalyst для автентифікації кожного пристрою при підключенні до розетки.

Переважна більшість пропрієтарного медичного програмного забезпечення, зокрема сервери обробки знімків PACS/DICOM, має офіційну сертифікацію саме під середовище Windows Server.

Після визначення базової серверної інфраструктури виникає потреба у забезпеченні цілодобового моніторингу стану активного мережевого обладнання та завантаженості каналів зв'язку. Система моніторингу повинна підтримувати протоколи SNMPv3, Syslog та NetFlow, надійно взаємодіяти з апаратним забезпеченням Cisco та надавати інтуїтивно зрозумілий графічний інтерфейс.

Для порівняння було обрано три популярні системи мережевого моніторингу, що охоплюють різні сегменти ринку: платформу з відкритим вихідним кодом Zabbix, комерційну систему Paessler PRTG Network Monitor та спеціалізований корпоративний комплекс Cisco DNA Center.

Для впровадження мережевого моніторингу в клініці «МедЛайф-Плюс» обрано систему Paessler PRTG Network Monitor. Хоча рішення Cisco DNA Center пропонує найглибшу інтеграцію з обраною апаратною базою, вартість його впровадження та апаратні вимоги є надлишковими для мережі такого масштабу.

З іншого боку, безкоштовна система Zabbix вимагає значних витрат часу на тонке налаштування серверів у середовищі Linux. PRTG Network Monitor є оптимальним балансом, оскільки система встановлюється безпосередньо на обрану раніше операційну систему Windows Server 2022, пропонує готові заводські шаблони для обладнання Cisco та підтримує безпечний протокол SNMPv3.

Порівняльні характеристики систем мережевого моніторингу зведено у таблицю 2.5.

Таблиця 2.5 – Порівняльний аналіз систем мережевого моніторингу

Критерій порівняння	Zabbix	Paessler PRTG Network Monitor	Cisco DNA Center
Тип ліцензування	Open Source (Безкоштовна)	Комерційна (залежить від кількості сенсорів)	Комерційна (корпоративна підписка)
Архітектура системи	Сервер-агент (або опитування по SNMP)	Централізована служба (на базі Windows Server)	Апаратно-програмний комплекс (Appliance)
Підтримка обладнання	Мультивендорна	Мультивендорна	Оптимізована під обладнання компанії Cisco
Механізми автовиявлення	Наявні, потребують ручного налаштування	Наявні, високий ступінь автоматизації процесів	Глибока автоматизація (AI Network Analytics)
Підтримка NetFlow/sFlow	Підтримується через додаткові сторонні модулі	Вбудована підтримка аналізу трафіку	Вбудована розширена підтримка

Ліцензійна політика PRTG дозволяє використовувати до ста сенсорів абсолютно безкоштовно, що повністю покриває поточні потреби клініки.

Завершальним, але критично важливим компонентом програмної інфраструктури є система захисту робочих станцій кінцевих користувачів. Оскільки персональні комп'ютери медичного персоналу активно взаємодіють з медичною інформаційною системою та обробляють чутливі персональні дані пацієнтів, стандартних засобів захисту операційної системи є недостатньо. Виникає потреба в антивірусному рішенні корпоративного класу з централізованою консоллю управління та проактивним захистом від вірусів-

вимагачів. Для порівняння розглядалися три передові системи кіберзахисту: ESET PROTECT Advanced, Bitdefender GravityZone Business Security та Cisco Secure Endpoint. Параметри цих програмних продуктів безпеки наведено у таблиці 2.6.

Таблиця 2.6 – Порівняльний аналіз програмних комплексів захисту кінцевих точок

Критерій порівняння	ESET PROTECT Advanced	Bitdefender GravityZone	Cisco Secure Endpoint
Клас програмного рішення	Антивірус та розширений захист (EPP+EDR)	Платформа EPP з базовими функціями EDR	Повноцінна система виявлення та реагування (EDR)
Консоль управління	Локальна (у домені AD) або хмарна версія	Хмарна інфраструктура	Хмарна інфраструктура
Захист від вірусів-вимагачів	Високий (вбудований Ransomware Shield)	Високий (модуль Advanced Anti-Exploit)	Максимальний (на базі аналітики Cisco Talos)
Інтеграція з межею мережі	Обмежена (працює автономно на ПК)	Обмежена (автономна робота агентів)	Повна нативна інтеграція з екраном Cisco Firepower
Захист файлових серверів	Повністю підтримується Windows Server	Повністю підтримується Windows Server	Повністю підтримується Windows Server

Для захисту автоматизованих робочих місць персоналу та центрального сервера клініки обрано програмний комплекс Cisco Secure Endpoint. Вирішальним фактором на користь цього продукту є його нативна апаратна інтеграція з міжмережевим екраном периметра Cisco Firepower 1120.

Це дозволяє створити єдину екосистему безпеки, де центральний шлюз та кінцеві точки в режимі реального часу обмінюються інформацією про загрози. У випадку виявлення інфікованого файлу на одному з комп'ютерів, система миттєво ізолює скомпрометований вузол від решти пристроїв, а міжмережевий екран автоматично блокує шкідливий трафік на межі мережі, що гарантує безперервну роботу клініки та повне збереження медичної таємниці.

2.6 Визначення функцій серверів та серверного обладнання

Для забезпечення надійного функціонування спроєктованої інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс» важливим завданням є визначення логічних функцій серверного ядра та підбір відповідного високопродуктивного апаратного забезпечення. Оскільки в попередньому розділі базовою платформою було обрано операційну систему Microsoft Windows Server 2022, логічна архітектура серверного сегмента будуватиметься на основі технології апаратної віртуалізації Hyper-V.

Це дозволяє на базі одного фізичного вузла розгорнути декілька ізольованих віртуальних серверів, кожен з яких виконуватиме чітко визначену роль. Головною логічною функцією є підтримка служби каталогів Active Directory Domain Services (AD DS) у зв'язці з інтегрованими сервісами доменних імен (DNS) та динамічного розподілу адрес (DHCP).

Наступною важливою роллю є функціонування сервера мережевих політик (Network Policy Server), який взаємодіє з комутаторами Cisco Catalyst за протоколом 802.1X для апаратної перевірки кожного пристрою при підключенні до локальної мережі.

Окремі високопродуктивні віртуальні машини виділяються для розгортання бази даних медичної інформаційної системи (МІС), системи мережевого моніторингу Paessler PRTG та спеціалізованого PACS-сервера, який відповідає за накопичення, архівацію та швидку видачу важких графічних знімків у форматі DICOM, що надходять від апаратів КТ та МРТ з діагностичного центру.

З огляду на життєво важливий характер медичних даних та необхідність цілодобового доступу до електронних карток пацієнтів, фізичне серверне обладнання повинно відповідати найвищим корпоративним стандартам відмовостійкості та продуктивності.

Фізичний сервер повинен мати потужну дискову підсистему з підтримкою апаратних RAID-контролерів для захисту інформації від руйнування у разі виходу з ладу окремих накопичувачів, підтримувати оперативну пам'ять із функцією корекції помилок (ECC) та бути оснащеним резервними блоками живлення.

Для обслуговування загалом понад п'ятдесяти активних робочих місць клініки та одночасної обробки великих масивів графічних даних необхідна двопроцесорна платформа стоєчного виконання. Для порівняльного аналізу в межах даного проєкту було відібрано три сучасні моделі серверів корпоративного класу від провідних світових виробників: Dell PowerEdge R750, HPE ProLiant DL380 Gen10 Plus та Cisco UCS C240 M6.

Порівняльні технічні характеристики та можливості масштабування обраного серверного обладнання наведено в таблиці 2.7.

Таблиця 2.7 – Порівняльний аналіз фізичного серверного обладнання

Критерій порівняння	Dell PowerEdge R750	HPE ProLiant DL380 Gen10 Plus	Cisco UCS C240 M6
1	2	3	4
Форм-фактор шасі	2U (Монтаж у стійку)	2U (Монтаж у стійку)	2U (Монтаж у стійку)
Процесорна архітектура	До 2-х Intel Xeon Scalable 3-го покоління	До 2-х Intel Xeon Scalable 3-го покоління	До 2-х Intel Xeon Scalable 3-го покоління
Максимальний обсяг RAM	8 ТБ (32 слоти DIMM)	8 ТБ (32 слоти DIMM)	8 ТБ (32 слоти DIMM)
Дисковий простір та накопичувачі	До 24 x 2.5" SAS/SATA/NVMe	До 24 x 2.5" SAS/SATA/NVMe	До 28 x 2.5" SAS/SATA/NVMe

Продовження таблиці 2.7

1	2	3	4
Можливості апаратного RAID-контролера	PERC H755N (підтримка NVMe RAID)	Smart Array P408i-a	Cisco RAID Controller (підтримка NVMe/SAS)
Технології віддаленого управління	iDRAC9 Enterprise	iLO 5 Advanced	Cisco Integrated Management Controller (CIMC) / Intersight
Резервування живлення	2 блоки живлення (Hot-Plug)	2 блоки живлення (Hot-Plug)	2 блоки живлення (Hot-Plug)

За результатами технічного аналізу оптимальним рішенням для побудови серверного ядра клініки «МедЛайф-Плюс» визначено сервер Cisco UCS C240 M6, зображений на рисунку 2.8.

Рисунок 2.8 – Зовнішній вигляд сервера Cisco UCS C240 M6

Головним аргументом на користь цієї апаратної платформи є її абсолютна сумісність та ідеальна інтеграція в раніше спроєктовану монолітну мережеву інфраструктуру, яка повністю побудована на базі рішень компанії Cisco. Використання єдиної хмарної платформи управління Cisco Intersight дозволяє системному адміністратору з однієї консолі здійснювати глибокий моніторинг стану серверного обладнання, міжмережевого екрана периметра та комутаторів доступу, що значно знижує операційні витрати на обслуговування IT-

інфраструктури. Сервер Cisco UCS C240 M6 має кращі показники масштабованості дискової підсистеми, підтримуючи до двадцяти восьми накопичувачів, що є критично важливим для медичного закладу.

Апаратні потужності обраного сервера дозволяють реалізувати гібридну дискову архітектуру для потреб різних віртуальних машин. Операційна система та високонавантажена транзакційна база даних медичної інформаційної системи розміщуються на швидкісних твердотільних накопичувачах стандарту NVMe, об'єднаних у масив RAID 10, що гарантує миттєвий відгук системи під час одночасної роботи кількох десятків лікарів.

Водночас для потреб PACS-сервера формується об'ємний масив RAID 6 з використанням класичних жорстких дисків інтерфейсу SAS, який забезпечує надійне довгострокове збереження важких знімків комп'ютерної та магнітно-резонансної томографії з діагностичного центру навіть у випадку одночасного виходу з ладу двох накопичувачів.

2.7 Розподіл адресного простору мережевих вузлів

Для забезпечення безпеки, логічної ізоляції трафіку та оптимізації пропускної здатності захищеної інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс» застосовується технологія віртуальних локальних мереж (VLAN).

Розподіл фізичної інфраструктури на незалежні широкомовні домени дозволяє відокремити медичне обладнання від загального офісного трафіку та публічних мереж, що є надзвичайно важливим для захисту медичної таємниці.

Процес логічної сегментації розпочинається з визначення необхідної кількості віртуальних мереж та присвоєння їм унікальних ідентифікаторів (VLAN ID). Згідно з організаційною структурою клініки та філії, створюється ряд спеціалізованих віртуальних мереж.

Для обслуговування відвідувачів у головному корпусі виділяється мережа Guests з ідентифікатором 10, а для пацієнтів філії передбачено аналогічну

мережу Guests_Diag з ідентифікатором п'ятнадцять. Ці мережі будуть поширюватись через безпровідні точки доступу.

Робочі станції медичного персоналу головного корпусу об'єднуються у віртуальну мережу Likar з ідентифікатором 20, тоді як специфічне діагностичне обладнання та комп'ютери лабораторії відносяться до мережі Diagn з ідентифікатором 25.

Для адміністративного апарату формується мережа Admin під номером тридцять. Вузол реєстратури головного корпусу працюватиме у мережі Recep з ідентифікатором сорок, а фінансовий відділ ізолюється у мережі Bugh під номером 50.

Для потреб денного стаціонару створюється мережа Stac з ідентифікатором шістдесят, а реєстратура діагностичного центру виділяється у мережу Recep_Diag з ідентифікатором 45.

Окремі віртуальні мережі створюються для керування бездротовими точками доступу: AP_Clinic під номером сімдесят для головного офісу та AP_Diag під номером 75 для філії.

Серверна інфраструктура ізолюється у високопріоритетній мережі Serv з ідентифікатором вісімдесят. Для організації маршрутизації між корпусами передбачено окремий транзитний канал VPN_Link, який функціонує на третьому рівні моделі OSI та не потребує окремого ідентифікатора віртуальної мережі.

Наступним етапом є розподіл єдиного адресного простору протоколу IPv4 для всіх визначених сегментів з використанням технології масок змінної довжини (VLSM). За базову адресу корпоративної мережі обрано приватний діапазон 192.168.10.0 з префіксом “/24”. Розподіл здійснюється за принципом від найбільших підмереж до найменших для уникнення фрагментації простору.

Мережі Guests та Guests_Diag розраховані на 50 вузлів кожна, що вимагає маски /26, яка надає 62 корисні адреси. Для мережі Likar, яка включає 28 пристроїв, обрано маску /27 з 30 корисними адресами. Мережі Diagn, Admin та Recep, кожна з яких містить від 10 до 12 вузлів, використовують маску /28, що надає 14 адрес. Мережі Bugh, Stac, Recep_Diag та AP_Clinic розраховані на 6

вузлів, тому для них застосовано маску /29 на 6 адрес. Для точок доступу філії AP_Diag, сервера Serv та магістрального каналу VPN_Link зарезервовано маску /30, що забезпечує рівно 2 адреси. Такий підхід, що базується на методі VLSM, дозволяє уникнути надмірної фрагментації адресного простору 192.168.10.0/24 та забезпечити раціональне використання ресурсів.

Широкомовна адреса для кожної підмережі визначається як її остання доступна IP-адреса, що використовується для передачі службових даних у межах одного сегмента, тоді як перша адреса стабільно закріплюється за шлюзом.

Таке математичне планування забезпечує високу ефективність використання адресного простору 192.168.10.0/24 без утворення конфліктів. Підсумкові результати проєктування представлені у таблиці 2.8.

Таблиця 2.8 – План розподілу IP-адрес та шлюзів для мережевих сегментів

Назва підмер.	Номер VLAN (ID)	Адреса мережі	Адреса шлюзу	Діапазон корисних адрес	Широкомовна адреса
1	2	3	4	5	6
Guests	10	192.168.10.0/26	192.168.10.1	192.168.10.2 – 192.168.10.62	192.168.10.63
Guests_Diag	15	192.168.10.64/26	192.168.10.65	192.168.10.66 – 192.168.10.126	192.168.10.127
Likar	20	192.168.10.128/27	192.168.10.129	192.168.10.130 – 192.168.10.158	192.168.10.159
Diagn	25	192.168.10.160/28	192.168.10.161	192.168.10.162 – 192.168.10.174	192.168.10.175
Admin	30	192.168.10.176/28	192.168.10.177	192.168.10.178 – 192.168.10.190	192.168.10.191
Recep	40	192.168.10.192/28	192.168.10.193	192.168.10.194 – 192.168.10.206	192.168.10.207
Bugh	50	192.168.10.208/29	192.168.10.209	192.168.10.210 – 192.168.10.214	192.168.10.215

Продовження таблиці 2.8

1	2	3	4	5	6
Stac	60	192.168.10.216/29	192.168.10.217	192.168.10.218 – 192.168.10.222	192.168.10.223
Recep_Diag	45	192.168.10.224/29	192.168.10.225	192.168.10.226 – 192.168.10.230	192.168.10.231
AP_Clinic	70	192.168.10.232/29	192.168.10.233	192.168.10.234 – 192.168.10.238	192.168.10.239
AP_Diag	75	192.168.10.240/30	192.168.10.241	192.168.10.242	192.168.10.243
Serv	80	192.168.10.244/30	192.168.10.245	192.168.10.246	192.168.10.247
VPN_Link	–	192.168.10.248/30	—	192.168.10.249 – 192.168.10.250	192.168.10.251

2.8 Тестування та налагодження мережі

Завершальним етапом реалізації проєкту захищеної інформаційно-комунікаційної мережі медичної клініки «МедЛайф-Плюс» є комплексне тестування та налагодження програмно-апаратних засобів, спрямоване на верифікацію коректності налаштувань, забезпечення стабільності каналів зв'язку та відповідності мережі заданим параметрам безпеки.

Процес тестування розпочинається з фізичної перевірки кабельної системи, де за допомогою спеціалізованих тестерів проводиться оцінка цілісності прокладених ліній категорії 6 та 6A, перевірка якості обтискання конекторів RJ-45 та відсутність замикань або перехресних перешкод у екранованих сегментах, що підключають діагностичне обладнання.

Після фізичного рівня проводиться верифікація конфігурації комутаційного обладнання Cisco, де послідовно перевіряється правильність розподілу портів за віртуальними мережами згідно з розробленим планом VLAN,

наявність активних з'єднань між ними та коректність роботи протоколів керування.

Особлива увага під час налагодження приділяється тестуванню функціональності міжмережевого екрана Cisco Firepower та правильності налаштування шлюзів за замовчуванням для кожної підмережі. На цьому етапі перевіряється здатність мережі до маршрутизації пакетів між ізольованими сегментами з дотриманням політик безпеки, що регламентують доступ медичного персоналу до електронних карток пацієнтів та серверного сегмента.

Налагодження безпеки кінцевих точок виконується шляхом інсталяції та перевірки робочого стану агентів Cisco Secure Endpoint на всіх автоматизованих робочих місцях клініки. Проводиться тестова атака з використанням безпечних сигнатур шкідливого коду для перевірки здатності системи виявляти загрози, ізолювати інфікований вузол та автоматично надсилати повідомлення про інцидент до консолі адміністратора.

Додатково здійснюється верифікація налаштувань протоколу автентифікації 802.1X, що передбачає тестування доступу до мережевих розеток за допомогою облікових даних користувачів Active Directory. У разі виявлення розбіжностей між проєктними даними та фактичними показниками проводиться повторне калібрування параметрів маршрутизації, корекція списків доступу (ACL) та налаштування пріоритезації трафіку (QoS) для гарантування безперервної передачі даних медичної інформаційної системи. Результати всіх етапів тестування фіксуються у протоколі пусконалагоджувальних робіт, що засвідчує повну готовність IT-інфраструктури до введення в промислову експлуатацію.

.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування сервера мережі

3.1.1 Інструкції із створення та налаштування RAID-масиву

Для забезпечення максимального рівня відмовостійкості та продуктивності серверного ядра клініки «МедЛайф-Плюс» на базі обраного сервера Cisco UCS C240 M6 першочерговим етапом налаштування є створення апаратних масивів незалежних дисків.

Згідно з обґрунтованою у попередньому розділі архітектурою, серверна дискова підсистема матиме гібридну структуру, що включає масив рівня RAID 10 для операційної системи та транзакційних баз даних, а також масив рівня RAID 6 для зберігання об'ємних медичних зображень PACS-сервера.

Процес конфігурування розпочинається з фізичного підключення сервера до мережі електроживлення та підключення інформаційного кабелю до виділеного порту управління інтегрованого контролера Cisco Integrated Management Controller (CIMC).

Після подачі живлення системний адміністратор повинен відкрити веббраузер на підключеній робочій станції та ввести IP-адресу інтерфейсу управління, яка за замовчуванням отримується по протоколу DHCP або налаштовується статично через базову систему введення-виведення при першому запуску сервера. На сторінці веб-авторизації необхідно ввести стандартизовані або попередньо змінені облікові дані локального адміністратора для доступу до головної графічної консолі управління сервером.

Після успішної авторизації в інтерфейсі Cisco Integrated Management Controller необхідно перейти до навігаційного меню, обрати розділ керування сховищем даних та знайти встановлений апаратний контролер Cisco RAID Controller. Для створення першого високошвидкісного масиву рівня RAID 10, призначеного для операційної системи Windows Server 2022 та медичної

інформаційної системи, адміністратор ініціює вбудований майстер створення віртуального диска з невикористаних фізичних накопичувачів.

У вікні налаштувань майстра з випадаючого списку обирається рівень масиву RAID 10, після чого в графічній панелі виділяються щонайменше чотири високошвидкісні твердотільні накопичувачі стандарту NVMe або SAS SSD однакового об'єму. Важливим етапом є тонка конфігурація параметрів віртуального диска, де розмір блоку даних (Strip Size) встановлюється на рівні 64 кілобайтів для оптимізації фрагментованої роботи транзакційної бази даних медичної інформаційної системи.

Політика запису налаштовується у режим відкладеного запису за умови справності батареї контролера (Write Back Good BBU) для максимізації продуктивності, а політика читання переводиться у режим випереджального читання. Після перевірки всіх параметрів процес створення завершується командою швидкої ініціалізації нового віртуального диска.

Наступним кроком є конфігурування другого дискового масиву рівня RAID 6, який забезпечуватиме надійне зберігання важких графічних знімків комп'ютерної та магнітно-резонансної томографії навіть у випадку одночасного виходу з ладу двох накопичувачів.

Використовуючи той самий інтерфейс керування контролером, адміністратор знову запускає майстер створення віртуального диска, обирає рівень RAID 6 та виділяє необхідну групу класичних магнітних жорстких дисків великої ємності з інтерфейсом SAS.

Зважаючи на потребу зберігання великих медіафайлів формату DICOM, розмір блоку даних (Strip Size) для цього масиву доцільно збільшити до двохсот п'ятдесяти шести кілобайтів, що суттєво підвищить швидкість потокового послідовного читання та запису.

Після застосування відповідних політик кешування та запуску повної ініціалізації масиву, адміністратору необхідно повернутися до головної вкладки віртуальних дисків у панелі управління сховищем та перевірити їхній поточний стан. Обидва новостворені масиви повинні набути статусу оптимального

функціонування, що свідчить про успішне завершення процесу апаратного налаштування дискової підсистеми сервера Cisco UCS C240 M6.

Лише після повного підтвердження справності обох RAID-масивів системний адміністратор може переходити до наступного етапу, який передбачає монтування образу операційної системи Windows Server через віртуальний KVM-консоль та її безпосереднє розгортання.

3.1.2 Інструкції із інсталяції сервера та створення віртуальних машин

Після успішного створення та ініціалізації апаратних дискових масивів наступним кроком є розгортання базової операційної системи Microsoft Windows Server 2022 на сервері Cisco UCS C240 M6. Процес інсталяції здійснюється віддалено за допомогою інтегрованого модуля управління Cisco Integrated Management Controller.

Системний адміністратор відкриває віртуальну KVM-консоль (Keyboard, Video, Mouse) через вебінтерфейс управління та використовує функцію віртуальних носіїв (Virtual Media) для монтування інсталяційного ISO-образу серверної операційної системи.

Після перезавантаження сервера та вибору віртуального пристрою як пріоритетного носія для завантаження запускається стандартний майстер встановлення. Під час конфігурації адміністратор обирає версію операційної системи з графічним інтерфейсом користувача (Desktop Experience) для спрощення подальшого адміністрування та вказує раніше створений масив рівня RAID 10 як цільовий розділ для інсталяції системних файлів. Після копіювання файлів та автоматичного перезавантаження системи необхідно задати надійний пароль для локального облікового запису адміністратора, який відповідає корпоративним вимогам безпеки щодо складності та довжини.

Завершивши базове встановлення, адміністратор виконує первинне налаштування мережевих параметрів та ідентифікації сервера. Властивостям мережевого адаптера, підключеного до комутатора ядра в сегменті серверної

інфраструктури, призначається статична IP-адреса з діапазону виділеної віртуальної мережі Serv (VLAN 80). Згідно із даними таблиці 2.8, це арреса 192.168.10.246 із маскою 255.255.255.252. та адресою шлюзу – 192.168.10.245.

Серверу присвоюється унікальне мережеве ім'я (Hostname), що відображає його центральну роль у топології клініки, після чого здійснюється обов'язкове перезавантаження для застосування змін.

Оскільки архітектура серверного ядра клініки «МедЛайф-Плюс» базується на технології апаратної віртуалізації, наступним критичним кроком є встановлення ролі Hyper-V. Через консоль диспетчера серверів (Server Manager) ініціюється майстер додавання ролей та компонентів, де обирається відповідна служба віртуалізації. У процесі встановлення майстер пропонує створити зовнішній віртуальний комутатор (External Virtual Switch), який необхідно жорстко прив'язати до фізичного мережевого інтерфейсу сервера для забезпечення доступу майбутніх віртуальних машин до локальної мережі клініки та маршрутизатора.

Після розгортання середовища віртуалізації системний адміністратор переходить до безпосереднього створення ізольованих віртуальних машин за допомогою консолі диспетчера Hyper-V Manager.

Для кожної запланованої логічної ролі, зокрема контролера домену Active Directory, сервера баз даних медичної інформаційної системи та сервера моніторингу PRTG, створюється окрема віртуальна машина другого покоління (Generation 2), що забезпечує підтримку сучасних технологій безпеки, таких як безпечне завантаження (Secure Boot) за стандартом UEFI.

Під час конфігурації кожній машині виділяється необхідний обсяг оперативної пам'яті з увімкненою функцією динамічного розподілу (Dynamic Memory) для оптимізації використання апаратних ресурсів фізичного сервера. Для зберігання гостьових операційних систем та даних створюються віртуальні жорсткі диски формату VHDX, які розміщуються на швидкісному масиві RAID 10.

Окремого підходу вимагає створення віртуальної машини для спеціалізованого PACS-сервера, який відповідає за обробку медичних зображень. Для цієї машини, окрім базового системного диска, створюється та підключається додатковий віртуальний том великої ємності, який фізично розміщується на резервному дисковому масиві рівня RAID 6, що гарантує максимальну надійність довгострокового зберігання важких графічних знімків комп'ютерної та магнітно-резонансної томографії.

Завершальним етапом є монтування інсталяційних образів до віртуальних приводів кожної створеної машини та їх початковий запуск для подальшого встановлення гостьових операційних систем та розгортання необхідного прикладного медичного програмного забезпечення.

3.2 Інструкції з налаштування комутаторів та маршрутизації між VLAN

3.2.1 Інструкції з налаштування комутаторів робочих груп

Процес базового налаштування комутатора робочої групи передбачає безпосередню взаємодію з інтерфейсом командного рядка (CLI) операційної системи Cisco IOS через консольне підключення.

Налаштування розпочинається з переходу до привілейованого режиму та режиму глобальної конфігурації для ідентифікації пристрою в мережі та встановлення криптографічного захисту доступу. Як приклад розглядається конфігурація комутатора Sw1, який згідно з логічною топологією забезпечує підключення автоматизованих робочих місць відділу реєстратури та кабінетів лікарів. Щоб задати назву комутатору потрібно ввести наступні команди [3]:

Switch> enable Switch

configure terminal

Switch(config)# hostname Sw1

Sw1(config)# enable secret CiscoMed123!

Команда hostname Sw1 змінює стандартне ім'я комутатора на унікальний ідентифікатор згідно з проєктною схемою, що полегшує його розпізнавання під час віддаленого адміністрування. Завершується цей етап застосуванням команди enable secret із вказанням складного пароля, яка активує криптографічне хешування та надійно захищає доступ до привілейованого режиму від несанкціонованого втручання.

Наступний блок команд відповідає за формування логічної бази даних віртуальних мереж безпосередньо в пам'яті комутатора. Введення команди vlan із зазначенням числового ідентифікатора, наприклад, 10, ініціює створення відповідного широкомовного домену та переводить інтерфейс у підрежим конфігурації цієї мережі.

У цьому підрежимі команда name застосовується для присвоєння віртуальній мережі зрозумілої текстової назви, такої як Guests для гостьового сегмента. Після цього використовується команда exit для повернення на рівень глобальної конфігурації. Цей алгоритм циклічно повторюється для створення інших мереж VLAN:

```
Sw1(config)# vlan 10
Sw1(config-vlan)# name Guests
Sw1(config-vlan)# exit
Sw1(config)# vlan 15
Sw1(config-vlan)# name Guests_Diag
Sw1(config-vlan)# exit
Sw1(config)# vlan 20
Sw1(config-vlan)# name Likar
Sw1(config-vlan)# exit
Sw1(config)# vlan 25
Sw1(config-vlan)# name Diagn
Sw1(config-vlan)# exit
Sw1(config)# vlan 30
Sw1(config-vlan)# name Admin
```

```
Sw1(config-vlan)# exit
Sw1(config)# vlan 40
Sw1(config-vlan)# name Recep
Sw1(config-vlan)# exit
Sw1(config)# vlan 45
Sw1(config-vlan)# name Recep_Diag
Sw1(config-vlan)# exit
Sw1(config)# vlan 50
Sw1(config-vlan)# name Bugh
Sw1(config-vlan)# exit
Sw1(config)# vlan 60
Sw1(config-vlan)# name Stac
Sw1(config-vlan)# exit
Sw1(config)# vlan 70
Sw1(config-vlan)# name AP_Clinic
Sw1(config-vlan)# exit
Sw1(config)# vlan 75
Sw1(config-vlan)# name AP_Diag
Sw1(config-vlan)# exit
Sw1(config)# vlan 80
Sw1(config-vlan)# name Serv
Sw1(config-vlan)# exit
Sw1(config)# end
Sw1# copy running-config startup-config
```

Наступним етапом налаштування комутатора Sw1 є конфігурація абонентських портів (інтерфейсів доступу), до яких безпосередньо підключаються кінцеві пристрої користувачів. Для ефективного керування великою кількістю інтерфейсів адміністратор використовує команду interface range, яка дозволяє групувати порти та застосовувати до них ідентичні параметри одночасно, суттєво мінімізуючи часові витрати та ймовірність конфігураційних помилок. Нижче наведено лістинг команд для налаштування сегментів реєстратури (VLAN 40) та робочих місць лікарів (VLAN 20):

```
Sw1(config)# interface range GigabitEthernet 1/0/1 - 6
Sw1(config-if-range)# switchport mode access
Sw1(config-if-range)# switchport access vlan 40
Sw1(config-if-range)# spanning-tree portfast
Sw1(config-if-range)# spanning-tree bpduguard enable
Sw1(config-if-range)# exit
Sw1(config)# interface range GigabitEthernet 1/0/7 - 21
Sw1(config-if-range)# switchport mode access
Sw1(config-if-range)# switchport access vlan 20
Sw1(config-if-range)# spanning-tree portfast
Sw1(config-if-range)# spanning-tree bpduguard enable
Sw1(config-if-range)# exit
```

Даний блок конфігурації виконує чітку логічну сегментацію мережі. Команда switchport mode access примусово переводить обрані порти в режим доступу, що виключає можливість їх роботи в режимі транку та забезпечує передачу даних лише у межах однієї визначеної віртуальної мережі. Наступна команда switchport access vlan призначає порти до конкретного ідентифікатора VLAN, що відповідає структурі розробленої логічної топології.

Особливу увагу під час налаштування приділено механізмам стабільності та безпеки. Активація технології spanning-tree portfast є критично важливою для клієнтських підключень, оскільки вона дозволяє інтерфейсу миттєво переходити в робочий стан «forwarding», оминаючи тривалі етапи перевірки топології протоколом Spanning Tree Protocol (STP), що критично для швидкого доступу користувачів до мережевих ресурсів при ввімкненні персонального комп'ютера. У свою чергу, використання команди spanning-tree bpduguard enable реалізує функцію захисту краю мережі: якщо до порту, на якому увімкнено цей механізм, буде підключено сторонній комутатор, що надішле BPDU-пакет, інтерфейс буде негайно переведений у стан err-disable. Це запобігає виникненню небажаних мережевих петель та підвищує загальну безпеку інфраструктури клініки, унеможливлюючи несанкціоноване розширення мережі без відома системного

адміністратора. Після успішного застосування параметрів команда exit повертає сесію до режиму глобальної конфігурації для подальшого виконання завдань.

Завершальним етапом логічної конфігурації комутатора робочої групи є налаштування магістрального порту (Uplink), який забезпечує передачу трафіку всіх віртуальних мереж між рівнем доступу та маршрутизатором або ядром мережі. Для цієї мети обрано інтерфейс GigabitEthernet 1/0/24, конфігурація якого наведена нижче [3]:

```
Sw1(config)# interface GigabitEthernet 1/0/24
Sw1(config-if)# switchport trunk encapsulation dot1q
Sw1(config-if)# switchport mode trunk
Sw1(config-if)# switchport trunk allowed vlan 10,15,20,25,30,40,45,50,60,70,75,80
Sw1(config-if)# end
Sw1# copy running-config startup-config
```

Використана у наведеному блоці команда switchport trunk encapsulation dot1q активує протокол IEEE 802.1Q, який є галузевим стандартом для маркування кадрів (tagging). Це дозволяє пристрою додавати до кожного кадру службовий тег з ідентифікатором VLAN, забезпечуючи коректну ідентифікацію приналежності трафіку до відповідної віртуальної мережі під час його передачі через спільний фізичний канал.

Команда switchport mode trunk примусово переводить інтерфейс у магістральний режим роботи, що є обов'язковим для зв'язку між комутаторами або між комутатором та маршрутизатором, що реалізує міжмережеву маршрутизацію (Inter-VLAN Routing).

З метою підвищення безпеки та оптимізації смуги пропускання застосовано команду switchport trunk allowed vlan, яка створює фільтр на магістральному порту.

Цей механізм дозволяє передачу через транковий канал виключно тих віртуальних мереж, що фактично функціонують на даному сегменті, відсікаючи зайвий широкомовний трафік, який не має прямого відношення до пристроїв, підключених до цього комутатора. Така сегментація запобігає поширенню

небажаних широкомовних розсилок по всій мережевій інфраструктурі, знижуючи «шум» та навантаження на процесори мережевого обладнання.

Процес конфігурації завершується командою end, яка миттєво повертає адміністратора з режиму налаштування інтерфейсу до привілейованого режиму, після чого команда copy running-config startup-config надійно зберігає внесені зміни в енергонезалежну пам’ять пристрою (NVRAM), гарантуючи їх автоматичне відновлення після будь-якого перезавантаження живлення.

Для забезпечення високого рівня безпеки на рівні доступу, крім базових налаштувань, необхідно активувати технологію Port Security. Це дозволяє жорстко контролювати, які саме пристрої можуть підключатися до конкретних мережевих розеток клініки. Нижче наведено лістинг команд для активації та налаштування безпеки на портах, до яких підключені критичні робочі станції лікарів:

```
Sw1(config)# interface range GigabitEthernet 1/0/7 - 21
Sw1(config-if-range)# switchport port-security
Sw1(config-if-range)# switchport port-security maximum 2
Sw1(config-if-range)# switchport port-security violation shutdown
Sw1(config-if-range)# switchport port-security mac-address sticky
Sw1(config-if-range)# exit
```

Команда switchport port-security активує функцію контролю доступу на інтерфейсі. Команда switchport port-security maximum 2 встановлює гранично допустиму кількість MAC-адрес на одному порті, що дозволяє підключити, наприклад, лише комп’ютер та IP-телефон, блокуючи спроби підключення додаткових пристроїв. У разі порушення цього правила, команда switchport port-security violation shutdown миттєво переводить порт у стан err-disable, що повністю припиняє передачу трафіку через цей інтерфейс, допоки адміністратор вручну не скине його стан.

Найбільш ефективною функцією є switchport port-security mac-address sticky, яка змушує комутатор динамічно вивчати MAC-адреси підключених пристроїв та автоматично записувати їх у файл поточної конфігурації. Після

цього ці адреси стають «прив'язаними» до порту, і при спробі підключення будь-якого іншого пристрою комутатор ідентифікує це як загрозу безпеці.

Аналогічні налаштування слід зробити для інших портів комутатора відповідно до схеми логічної топології мережі представленої на додатку Б.

3.2.2 Інструкції з базового налаштування маршрутизатора

Центральним вузлом мережевої інфраструктури клініки «МедЛайф-Плюс» є маршрутизатор R1, який відповідає за маршрутизацію між віртуальними мережами (Inter-VLAN Routing) та забезпечення зовнішнього зв’язку. Для реалізації цього завдання на фізичному інтерфейсі, що сполучає маршрутизатор з комутатором ядра, застосовується технологія «Router-on-a-Stick». Вона передбачає створення логічних підінтерфейсів для кожного VLAN, кожен з яких слугуватиме шлюзом за замовчуванням для відповідної підмережі. Налаштування розпочинається з ідентифікації інтерфейсу та активації інкапсуляції dot1Q.

Налаштування маршрутизатора R1 (Головний корпус). Цей маршрутизатор обслуговує сегменти: Guests (10), Likar (20), Admin (30), Recep (40), Bugh (50), Stac (60), AP_Clinic (70), Serv (80). Отже, відповідно до даних таблиці 2.8 потрібно ввести команди:

```
R1# configure terminal
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet 0/0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.192
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.10.129 255.255.255.224
```

```
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.168.10.177 255.255.255.240
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.40
R1(config-subif)# encapsulation dot1Q 40
R1(config-subif)# ip address 192.168.10.193 255.255.255.240
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.50
R1(config-subif)# encapsulation dot1Q 50
R1(config-subif)# ip address 192.168.10.209 255.255.255.248
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.60
R1(config-subif)# encapsulation dot1Q 60
R1(config-subif)# ip address 192.168.10.217 255.255.255.248
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.70
R1(config-subif)# encapsulation dot1Q 70
R1(config-subif)# ip address 192.168.10.233 255.255.255.248
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.80
R1(config-subif)# encapsulation dot1Q 80
R1(config-subif)# ip address 192.168.10.245 255.255.255.252
R1(config-subif)# exit
R1(config)# end
R1# copy running-config startup-config
```

Налаштування маршрутизатора R2 (діагностична філія). Цей маршрутизатор обслуговує сегменти філії: Guests_Diag (15), Diagn (25), Recep_Diag (45), AP_Diag (75). Отже, відповідно до даних таблиці 2.8 потрібно ввести команди:

```
R2# configure terminal
R2(config)# interface GigabitEthernet 0/0/0
```

```
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface GigabitEthernet 0/0/0.15
R2(config-subif)# encapsulation dot1Q 15
R2(config-subif)# ip address 192.168.10.65 255.255.255.192
R2(config-subif)# exit
R2(config)# interface GigabitEthernet 0/0/0.25
R2(config-subif)# encapsulation dot1Q 25
R2(config-subif)# ip address 192.168.10.161 255.255.255.240
R2(config-subif)# exit
R2(config)# interface GigabitEthernet 0/0/0.45
R2(config-subif)# encapsulation dot1Q 45
R2(config-subif)# ip address 192.168.10.225 255.255.255.248
R2(config-subif)# exit
R2(config)# interface GigabitEthernet 0/0/0.75
R2(config-subif)# encapsulation dot1Q 75
R2(config-subif)# ip address 192.168.10.241 255.255.255.252
R2(config-subif)# exit
```

Для забезпечення доступу робочих станцій та медичного обладнання клініки до ресурсів мережі Інтернет на маршрутизаторах R1 та R2 налаштовується технологія динамічної трансляції адрес (NAT Overload або PAT). Цей механізм дозволяє великій кількості внутрішніх пристроїв використовувати одну публічну IP-адресу зовнішнього інтерфейсу маршрутизатора. Налаштування передбачає чіткий розподіл інтерфейсів на внутрішні («inside») та зовнішні («outside»), а також визначення списків доступу (ACL), що дозволяють трансляцію трафіку з локальних сегментів.

Конфігурація NAT на маршрутизаторі R1 (головний корпус) [3]:

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface GigabitEthernet 0/0/0.10
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.20
```

```
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.30
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.40
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.50
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.60
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.70
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/0/0.80
R1(config-subif)# ip nat inside
R1(config-subif)# exit
R1(config)# interface GigabitEthernet 0/1/0
R1(config-if)# ip nat outside
R1(config-if)# exit
R1(config)# ip nat inside source list 1 interface GigabitEthernet 0/1/0 overload
R1(config)# end
R1# copy running-config startup-config
```

Виконані налаштування базуються на використанні команди ip nat inside на кожному підінтерфейсі, що обслуговує внутрішні VLAN, що маркує трафік як такий, що підлягає трансляції при виході за межі локальної мережі. Відповідно, фізичний інтерфейс, з’єднаний з мережевим обладнанням провайдера, отримує маркування ip nat outside.

Команда ip nat inside source list 1 interface ... overload активує режим PAT, який динамічно замінює внутрішні IP-адреси пристроїв на адресу зовнішнього інтерфейсу маршрутизатора, зберігаючи відповідність сесій за номерами портів. Використання списку доступу access-list 1 дозволяє чітко обмежити мережі, трафік яких має право на трансляцію, що є необхідною вимогою для безпеки та стабільності роботи мережевої інфраструктури. Збереження конфігурації завершує процес, гарантуючи стійкість налаштувань після перезавантаження обладнання.

Подібним чином потрілно налаштувати NAT на маршрутизаторі діагностичної філії R2.

3.2.3 Інструкції по налаштуванню VPN-тунелів та маршрутизації

Для забезпечення безпечного обміну даними між головним корпусом клініки та діагностичною філією розгортається захищений VPN-тунель на базі протоколу GRE (Generic Routing Encapsulation).

Цей механізм дозволяє інкапсулювати трафік між віддаленими мережами, створюючи логічний канал зв’язку поверх існуючої інфраструктури Інтернет. Для реалізації цього рішення на маршрутизаторах R1 та R2 створюються тунельні інтерфейси, яким призначаються адреси зі спеціальної підмережі 192.168.10.248/30, згідно з планом адресації.

Конфігурація VPN-тунелю на маршрутизаторі R1:

```
R1(config)# interface Tunnel0
R1(config-if)# ip address 192.168.10.249 255.255.255.252
R1(config-if)# tunnel source GigabitEthernet 0/1/0
R1(config-if)# tunnel destination 162.198.10.201
R1(config-if)# exit
```

Команда interface Tunnel0 створює логічний віртуальний інтерфейс для тунелювання.

Наступна команда ip address 192.168.10.249 255.255.255.252 призначає IP-адресу кінцевої точки тунелю згідно з планом адресації, представлену в таблиці 2.8.

Команда tunnel source GigabitEthernet 0/1/0 вказує вихідний фізичний інтерфейс маршрутизатора, через який буде відправлятися інкапсульований трафік. А команда tunnel destination 162.198.10.201 вказує публічну IP-адресу протилежного маршрутизатора (R2), до якого веде тунель.

Важливо зазначити, що стандартний GRE не шифрує дані. У реальних мережах медичних установ для захисту конфіденційної інформації (пацієнтів та діагнозів) додатково накладається протокол IPsec. Він забезпечує шифрування (AES) та перевірку цілісності пакетів. У межах даного дипломного проєкту ми використовуємо GRE як транспортний механізм, що за необхідності доповнюється параметрами шифрування IPsec для гарантування захисту даних від несанкціонованого перехоплення.

Шифрування налаштовується шляхом створення політики безпеки (ISAKMP), набору перетворень (transform-set) та профілю IPsec, який потім застосовується до тунельного інтерфейсу [3]:

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# exit
```

Команда crypto isakmp policy 10 створює політику для узгодження параметрів безпеки. Цифра 10 – це пріоритет.

Параметр encryption aes 256 встановлює алгоритм шифрування AES з довжиною ключа 256 біт – це сучасний стандарт захисту даних у медицині. Наступний параметр hash sha256 забезпечує цілісність даних, використовуючи хеш-функцію SHA-256 для перевірки, що пакети не були модифіковані в дорозі.

Команжа authentication pre-share задає метод автентифікації за заздалегідь відомим ключем.

Команда group 14 використовує алгоритм Діффі-Гелмана (DH) 14-ї групи для безпечного обміну ключами (високий рівень стійкості).

Встановлення спільного ключа (замінити 'CiscoMedSecret' на свій):

R1(config)# crypto isakmp key CiscoMedSecret address 162.198.10.201

Налаштування набору перетворень (Transform Set). Визначається протокол ESP (Encapsulating Security Payload) для шифрування (esp-aes) та автентифікації (esp-sha256-hmac):

R1(config)# crypto ipsec transform-set MED_SET esp-aes 256 esp-sha256-hmac

Задається режим роботи, при якому шифрується лише корисне навантаження (всередині GRE), що є оптимальним для GRE-тунелів [3]:

R1(config-trans)# mode transport

R1(config-trans)# exit

Створення профілю IPsec та застосування його до тунелю:

R1(config)# interface Tunnel0

R1(config-if)# tunnel protection ipsec profile MED_PROFILE

R1(config-if)# exit

Застосувавши ці команди на R1 та R2 (з відповідними IP-адресами сусідів), буже забезпечено надійне шифрування даних. Тепер будь-яка спроба перехоплення трафіку між корпусами через публічний інтернет буде марною, оскільки зловмисник отримає лише набір зашифрованих даних (AES-256), які неможливо прочитати без знання ключа.

Після встановлення логічного каналу необхідно вказати маршрутизаторам, у який саме тунель спрямовувати трафік для конкретних підмереж.

Статичні маршрути на R1 (для доступу до мереж філії через R2):

R1(config)# ip route 192.168.10.64 255.255.255.192 192.168.10.250

R1(config)# ip route 192.168.10.160 255.255.255.240 192.168.10.250

R1(config)# ip route 192.168.10.224 255.255.255.248 192.168.10.250

R1(config)# ip route 192.168.10.240 255.255.255.252 192.168.10.250

Статичні маршрути на R2 (для доступу до мереж головного корпусу через R1):

```
R2(config)# ip route 192.168.10.0 255.255.255.192 192.168.10.249
R2(config)# ip route 192.168.10.128 255.255.255.224 192.168.10.249
R2(config)# ip route 192.168.10.176 255.255.255.240 192.168.10.249
R2(config)# ip route 192.168.10.192 255.255.255.240 192.168.10.249
R2(config)# ip route 192.168.10.208 255.255.255.248 192.168.10.249
R2(config)# ip route 192.168.10.216 255.255.255.248 192.168.10.249
R2(config)# ip route 192.168.10.232 255.255.255.248 192.168.10.249
```

3.3 Інструкції по налаштуванню засобів захисту мережі

Важливим етапом є конфігурація маршрутизації до зовнішніх мереж та налаштування політик доступу. Для обмеження трафіку між відділами клініки використовуються списки контролю доступу (Access Control Lists), які накладаються на відповідні підінтерфейси для фільтрації пакетів:

```
R1(config)# ip access-list extended ADMIN_TO_SERV
R1(config-ext-nacl)# permit ip 192.168.10.176 0.0.0.15 192.168.10.244 0.0.0.3
R1(config-ext-nacl)# deny ip any any
R1(config)# interface GigabitEthernet 0/0/0.30
R1(config-subif)# ip access-group ADMIN_TO_SERV in
R1(config-subif)# end
R1# copy running-config startup-config
```

Команда ip access-list extended ініціює створення іменованого розширеного списку доступу, у якому чітко визначаються дозволені напрямки трафіку, наприклад, доступ адміністративного персоналу (Admin) до серверного сегмента (Serv). Застосування команди deny ip any any у кінці списку забезпечує закриття всіх інших шляхів, що є фундаментальним принципом безпеки «заборонити все, що явно не дозволено». Накладання списку на інтерфейс командою ip access-group ... in активує фільтрацію на вхідному трафіку, запобігаючи

несанкціонованим зверненням до критичних ресурсів клініки. Фінальна команда copy running-config startup-config забезпечує збереження налаштованих правил маршрутизації в енергонезалежну пам'ять, що гарантує стабільну роботу мережі після перезавантаження маршрутизатора.

3.4 Моделювання мережі

Для верифікації розробленої логічної структури мережі, перевірки коректності конфігурації обладнання та аналізу роботи протоколів було проведено моделювання мережевої інфраструктури клініки «МедЛайф-Плюс» у програмному середовищі Cisco Packet Tracer. Дане середовище дозволяє відтворити фізичне розташування пристроїв, налаштувати інтерфейси згідно з планом адресації та імітувати передачу реального трафіку в умовах, максимально наближених до реальних.

Процес моделювання розпочався з розміщення активного мережевого обладнання: маршрутизаторів (R1, R2), комутаторів (Sw1, Sw2, Sw3) та кінцевих пристроїв (сервери, АРМ лікарів, діагностичне обладнання). З’єднання між вузлами було реалізовано з використанням стандартизованих кабелів (Copper Straight-Through для кінцевих пристроїв, Fiber для магістральних каналів), що відповідає проєктній схемі.

Для кожної групи інтерфейсів було присвоєно відповідні VLAN, а фізичні порти комутаторів налаштовані як порти доступу (access) або магістральні (trunk), що забезпечило коректну передачу тегованого трафіку між сегментами.

Після нанесення налаштувань (IP-адресація, статична маршрутизація, VPN-тунелі, NAT) було проведено перевірку працездатності мережі за допомогою таких інструментів:

- тестування зв’язності (ICMP). Виконання команд ping та traceroute між віддаленими підмережами (наприклад, з сегмента Likar у головному корпусі до сегмента Diagn у філії) підтвердило наявність стабільного маршруту через побудований GRE-тунель;

- аналіз пакетів (Simulation Mode). Завдяки режиму симуляції Packet Tracer було проаналізовано процес інкапсуляції кадрів у пакет, а також перевірено роботу протоколу IPsec (ESP-заголовки), що підтвердило наявність шифрування трафіку;

- перевірка безпеки. Було змодельовано спробу підключення стороннього пристрою до порту, на якому налаштовано port-security, що призвело до автоматичного переведення порту у стан err-disable, підтвердивши коректність налаштувань безпеки доступу.

Результати моделювання довели, що розроблена архітектура мережі клініки є цілісною, масштабованою та забезпечує виконання всіх поставлених вимог щодо безпеки передачі даних між головним офісом та діагностичною філією. Усі налаштування, верифіковані в середовищі Cisco Packet Tracer, є придатними для перенесення на реальне обладнання Cisco.

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 проєкт локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проєкту	15
2.	Проєктування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі медичної клініки. Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури підприємства для сегментування локальної мережі на підмережі.	Інженер	30

Продовження таблиці 4.1

1	2	3	4
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних трас). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Технік	40
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			120

Сумарний час виконання операцій технологічного процесу проєктування мережі становить 120 годин, з них 15 годин – робота керівника проєкту, 65 годин – інженера, 40 годин – 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 тарифну ставку для керівника проєкту – 280 грн/год, інженера – 200 грн/год, а для техніка – 160 грн/год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 15 \cdot 280 = 4200$ грн.
- інженера – $З_{осн2} = 65 \cdot 200 = 13000$ грн.
- техніка – $З_{осн3} = 40 \cdot 160 = 6400$ грн.

Сумарна основна заробітна плата становить

$$З_{осн} = 4200 + 13000 + 6400 = 23600 \text{ грн.}$$

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 $З_{дод1}=4200 \cdot 0,12= 504$ грн.
- інженера $З_{дод1}=13000 \cdot 0,12= 1560$ грн.
- техніка $З_{дод3}=6400 \cdot 0,12= 768$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод} = 504 + 1560 + 768 = 2832 \text{ грн.}$$

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:

$$В_{о.п.} = 23600 + 2832 = 26432 \text{ грн.}$$

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

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з}= 26432 \cdot 0,22= 5815,04 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/	Категорія працівни-ків	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	280	15	4200	504		
2	Інженер	200	65	13000	1560	-	-
3	Технік	160	40	6400	768	-	-
			Разом	23600	2832	5815,04	32247,04

Отже, загальні витрати на оплату праці становлять 32 247,04 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	Комутаційна шафа Одескабель CH-12U-06-06-П-С	шт.	1	6776	6776
2	Комутаційна шафа Одескабель CH-12U-06-06-П-С	шт.	2	3869	7738
3	Патчпанель OK-PP-24-U6	шт.	2	1180	2360
4	Патчпанель OK-PP-24-F6A	шт.	1	1320	1320
5	Розетка RJ-45 (категорія 6)	шт.	49	120	5880
6	Розетка RJ-45 (категорія 6-А)	шт.	12	160	1920
7	Розетка підлогова RJ-45	шт.	9	190	1710
8	Роз’єм 8P8C (100 шт)	шт.	1	590	590
9	Короб (середня ціна)	м.	245	112	27440
10	Короб підлоговий	м.	13	195	2535
11	Кабель UTP (кат. 6) (бухта)	шт.	3	5353	16059
12	Кабель F/UTP-cat.6A (бухта)	шт.	1	6780	6780
13	Патчкорди PC-FTP-Cat6A-2m	шт.	40	51	2040
14	Патчкорди PC-UTP-Cat6-1.5m	шт.	8	85	680
15	Патчкорди (оптоволокно)	шт.	2	75	150
16	Кабель оптоволоконний	м.	4	33	132
17	Конектор SC	шт.	2	38	76
18	Гофрована трубка	м.	22	40	880
19	Сервер Cisco UCS C240 M6	шт.	1	50972	50972
20	Фаєрвол Cisco Firepower 1120	шт.	2	39689	79378
21	Комутатор Cisco Catalyst 9200L-24P-4G-E	шт.	3	61417	184251
22	Точка доступу Cisco Catalyst 9115AXI-E	шт.	3	24956	74868
23	ДБЖ APC Back-UPS Pro 1200VA	шт.	3	3680	11040
Разом					485575,00

Отже, загальна сума матеріальних витрат на розробку мережі становить 485 575,00 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 проєктом становить 10 годин, споживана потужність – 0,5 кВт/год, вартість 1 кВт електроенергії – 9 грн. Витрати на електроенергію:

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

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,

$$Т_В = 485\ 575,00 \cdot 0,08 = 38846 \text{ грн.}$$

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:

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

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 – 28000грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{28000 \cdot 0{,}04}{150} \cdot 10 = 112 \text{ грн}$$

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.

$$Нв = Во.п. \cdot 0{,}2...0{,}6,, \qquad (4.10)$$

де $Н_В$ – накладні витрати.

$$Н_В = 26432 \cdot 0{,}4 = 10572{,}8 \text{ грн.}$$

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 розрахунків зведено у таблицю 4.4. Собівартість ($С_в$) НДР розраховується за формулою:

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

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	26432	4,66
Відрахування на соціальні заходи	5815,04	1,02
Матеріальні витрати	485575	85,58
Витрати на електроенергію	45	0,01
Транспортні витрати	38846	6,85
Амортизаційні відрахування	112	0,02
Накладні витрати	10572,8	1,86
Собівартість	567397,84	100,00

Отже, собівартість дорівнює: 567397,84 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

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

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

Отже, ціна НДР становить:

$$Ц = 567397{,}84 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 885140{,}6304 \text{ грн}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання ресурсів. Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

де $П$ – прибуток;

$С_В$ – собівартість;

$$П = 885140{,}6304 - 567397{,}84 = 317742{,}79 \text{ грн.}$$

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

$$E_p = \frac{П}{С_в} = \frac{317742{,}79}{567397{,}84} = 0{,}56 \quad (4.14)$$

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:

$$T_p = \frac{1}{0{,}56} \approx 1{,}8$$

Всі дані внесемо в зведену таблицю 4.5 економічних показників.

Таблиця 4.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	567397,84 грн.
2.	Плановий прибуток, грн.	317742,79 грн.
3.	Ціна, грн.	885140,63 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп'ютерної мережі для медичної клініки «МедЛайф-Плюс» становить 885140,63 грн. Зважаючи на високі показники економічної ефективності (0,56), кошти, вкладені в проєкт, окупляться за 1,8 року.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

5.1 Розрахунок системи штучного освітлення для приміщення медичної клініки “МедЛайф-Плюс”, де міститься найбільше ПК

Відповідно до аналізу архітектурно-планувальних рішень та схем розміщення комп'ютерної техніки (див. додаток А), приміщенням з найбільшою концентрацією засобів обчислювальної техніки є «Рецепція», що розташована на першому поверсі головного корпусу клініки «МедЛайф-Плюс».

У цьому приміщенні з геометричними розмірами 7,5 х 4,5 м організовано 6 робочих місць адміністраторів (ідентифікатори на схемі додатку В: PC_1 – PC_6) та встановлено один периферійний пристрій (Pr_1).

Зорова робота персоналу рецепції пов'язана із безперервним зчитуванням інформації з екранів моніторів та паперових носіїв (медичні карти, бланки, чеки), що згідно з чинними нормативно-правовими актами належить до категорії робіт високої зорової точності. Невідповідність параметрів світлового середовища нормативним значенням призводить до перевтоми зорового аналізатора, зниження концентрації уваги та загального зниження продуктивності праці.

Для забезпечення оптимальних та безпечних умов праці проведемо інженерний розрахунок загального рівномірного штучного освітлення приміщення рецепції відповідно до вимог ДБН В.2.5-28:2018 «Природне і штучне освітлення» [9]. Розрахунок виконується методом коефіцієнта використання світлового потоку, який є найбільш точним для приміщень з високими коефіцієнтами відбиття стін та стелі.

Для проведення світлотехнічного розрахунку встановлено такі параметри приміщення та робочих поверхонь:

- довжина приміщення (А): 7,5 м;
- ширина приміщення (В): 4,5 м;
- загальна площа приміщення (S = A x B): 33,75 м²;
- висота приміщення (Н): 3,0 м;

- висота робочої поверхні (рівень столу над підлогою, hp): 0,8 м;

- висота звису світильника (hc): 0 м (світильники інтегруються безпосередньо в підвісну стельову систему типу «Армстронг»);

- нормована освітленість на робочій поверхні для ПК з дисплеями (Ен): 400 лк (згідно з таблицею Б.1 ДБН В.2.5-28:2018) [9];

- коефіцієнт запасу (Кз), який враховує зниження світлового потоку в процесі експлуатації через старіння діодів та запилення: 1,4;

- коефіцієнт нерівномірності освітлення (Z) для світлодіодних джерел світла: 1,1;

- коефіцієнти відбиття будівельних та оздоблювальних поверхонь (прийняті для світлої колірної гами медичного закладу):

  - стелі ρ_c= 70 % – біла акустична плита/пофарбування,
  - стін $\rho_{ст}$= 50 % –світло-бежеві/салатові медичні панелі,
  - підлоги $\rho_п$= 30 % – світло-сірий комерційний лінолеум/керамогранiт.

Розрахунок потрібно розпочати із визначення розрахункової висоти підвісу світильників (h).

Розрахункова висота – це відстань від площини світильників до рівня робочої поверхні столу:

$$h = H - h_p - h_c = 3,0 - 0,8 - 0 = 2,2 \text{ м}$$

Індекс приміщення відображає його геометричні пропорції та визначається за формулою:

$$i = \frac{S}{h \cdot (A + B)} \qquad (5.1)$$

Підставивши чисельні значення у формулу (5.1), отримуємо:

$$i = \frac{33,75}{2,2 \cdot (7,5 + 4,5)} = \frac{33,75}{2,2 \cdot 12,0} = \frac{33,75}{26,4} \approx 1,28$$

На наступному етапі потрібно визначити коефіцієнт використання світлового потоку (η).

Коефіцієнт використання світлового потоку (η) показує, яка частина світлового потоку ламп потрапляє на робочу площину (включаючи відбите світло). За довідковими таблицями для світильників із розсіяним світлорозподілом [1], на основі обчисленого індексу приміщення і = 1,28 та заданих коефіцієнтів відбиття ($\rho_с$= 70 %, $\rho_{ст}$= 50 %, $\rho_п$= 30 %), методом лінійної інтерполяції знаходимо:

η=46% або 0,46

Загальний світловий потік, який має генерувати вся освітлювальна установка для досягнення нормованого показника у 400 лк, обчислюється за формулою:

$$F_{заг} = \frac{E_Н \cdot S \cdot K_з \cdot Z}{\eta} \quad (5.2)$$

де $E_н$ – це нормативна освітленість у люксах (лк), встановлена державними будівельними нормами для конкретного типу діяльності (наприклад, 400 лк для роботи за комп'ютером) [9].

З цієї формули

$$F_{заг} = \frac{400 \cdot 33{,}75 \cdot 1{,}4 \cdot 1{,}1}{0{,}46} = \frac{20790}{0{,}46} \approx 45195{,}95 \text{ лм}$$

Для освітлення медичних офісних приміщень та зон рецепції доцільно використовувати сучасні енергоефективні світлодіодні (LED) панелі розміром 600×600 мм із призматичним або опаловим розсіювачем.

Світлодіодні світильники забезпечують високу світловіддачу, тривалий термін служби, екологічну безпеку (відсутність ртуті) та низький коефіцієнт пульсації світлового потоку ($K_п$ < 5 %), що відповідає жорстким санітарним нормам медичних установ.

Обираємо серійний світильник типу LED-панель 36W 600x600, який має такі технічні характеристики:

- споживана потужність: 36 Вт;
- номінальний світловий потік одного світильника (Fсв): 3200 лм;

- колірна температура: 4000 К (нейтральне біле світло, що стимулює працездатність).

Необхідна кількість світильників (N) визначається як відношення загального світлового потоку до потоку одного джерела світла:

$$N = \frac{F_{\text{заг}}}{F_{\text{св}}} = \frac{45195{,}65}{320} \approx 14{,}12 \qquad (5.3)$$

З метою забезпечення симетричного та рівномірного геометричного розподілу світильників на стельовому модулі типу «Армстронг» (розмір клітинки 600×600 мм) (див. рис. 5.1), округляємо отримане значення в бік збільшення до найближчого оптимального числа, що утворює правильну матрицю розміщення. Приймаємо до встановлення N = 15 світильників (матриця розміщення: 3 ряди по 5 світильників у кожному ряду).

Рисунок 5.1 – Вбудовувана світлодіодна панель типу «Армстронг» 36W

Після остаточного вибору кількості джерел світла виконується перевірка фактично створеної освітленості у приміщенні за формулою:

$$E_{\text{фак}} = \frac{N \cdot F_{\text{св}} \cdot \eta}{S \cdot K_{\text{з}} \cdot Z} \qquad (5.4)$$

Звідси

$$E_{\text{фак}} = \frac{15 \cdot 3200 \cdot 0{,}46}{33{,}75 \cdot 1{,}4 \cdot 1.1} = \frac{22080}{51{,}975} \approx 424{,}82 \text{ лк}$$

Визначимо відхилення отриманої фактичної освітленості від нормованого значення:

$$\Delta E = \frac{E_{\text{фак}} - E_{\text{Н}}}{E_{\text{Н}}} \cdot 100\% = \frac{424{,}82 - 400}{400} \cdot 100\% = +6{,}2\% \quad (5.5)$$

Згідно з вимогами ДБН В.2.5-28:2018, відхилення фактичної освітленості від норми допускається в межах від -10\% до +20%. Отримане значення +6,2% повністю задовольняє нормативні вимоги та створює невеликий комфортний запас освітленості [9].

Для формування безтіньового та рівномірного світлового поля 15 обраних LED-панелей інтегруються в підвісну стелю за схемою регулярної прямокутної сітки. Завдяки пропорціям приміщення (7,5 х 4,5 м), матриця розміщення 5 х3 дозволяє досягти математично ідеальної геометрії кроку.

Розміщення вздовж довгої стіни (довжина 7,5 м, 5 світильників у ряду):

- відстань між осями сусідніх світильників у ряду (L_A):

$$L_A = 7{,}5 / 5 = 1{,}5 \text{ м}; \quad (5.6)$$

- відстань від крайніх світильників до торцевих стін (l_A): $l_A = L_A/2 =$

$$1{,}5 / 2 = 0{,}75 \text{ м}. \quad (5.7)$$

Розміщення вздовж короткої стіни (ширина 4,5 м, 3 ряди світильників):

- відстань між паралельними рядами світильників (L_B):

$$L_B = 4{,}5 / 3 = 1{,}5 \text{ м}; \quad (5.8)$$

- відстань від крайніх рядів світильників до поздовжніх стін (l_B):

$$l_B = L_B / 2 = 1{,}5 / 2 = 0{,}75 \text{ м}.$$

Детальна графічна план-схема трасування електричних мереж та просторового розташування світильників у приміщенні рецепції клініки представлена на рисунку 5.2.

Таким чином, утворюється абсолютно симетрична квадратна сітка кроком 1,5 х 1,5 м з однаковими відступами від усіх стін кімнати, що дорівнюють 0,75 м.

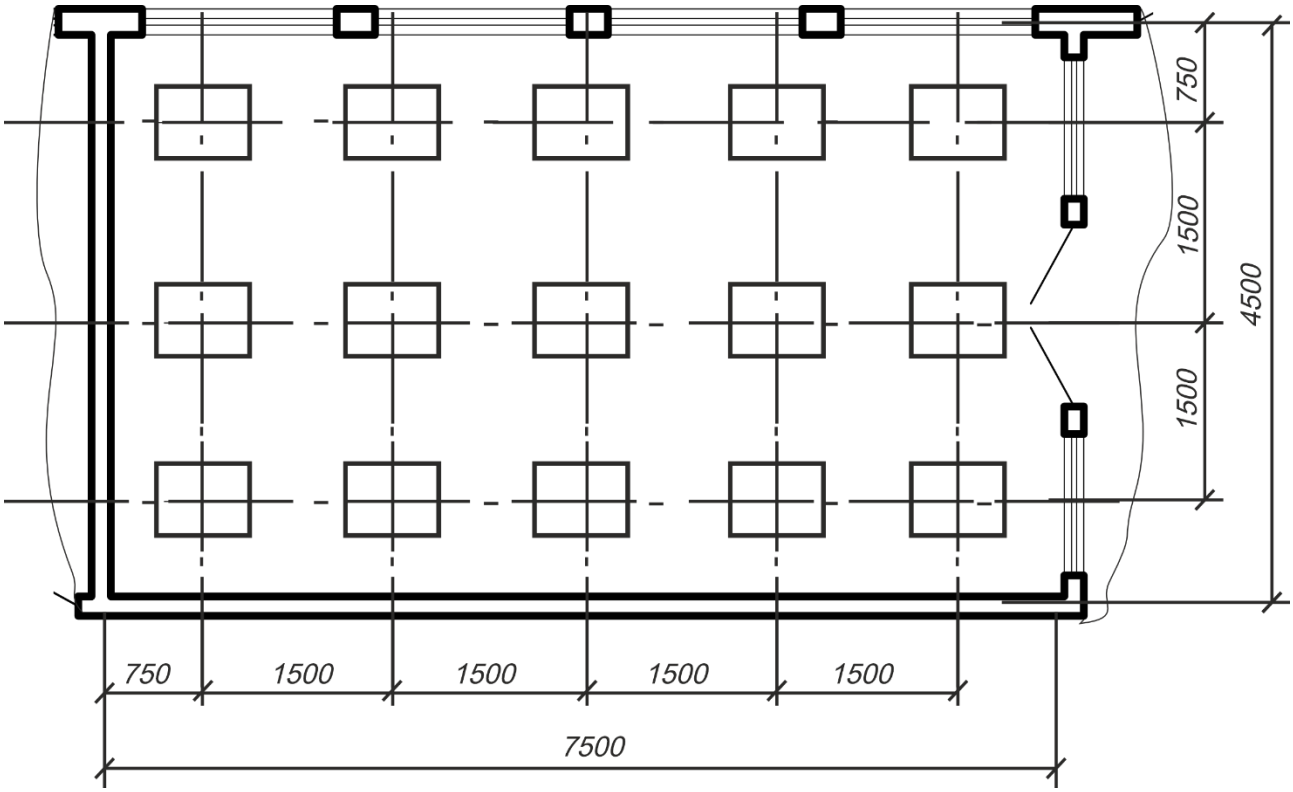


Рисунок 5.2 – Схема встановлення світильників в приміщенні рецепції

Дана схема нівелює зони затінення біля стін та забезпечує інтенсивне і рівномірне освітлення зони стійки рецепції, де безпосередньо встановлено комп'ютерну техніку (PC_1 – PC_6).

5.2 Вимоги електробезпеки та санітарного режиму під час обслуговування мережевої інфраструктури в приміщеннях медичного закладу

Специфіка медичного закладу вимагає одночасного та суворого дотримання як правил електробезпеки через постійне сусідство високочутливого медичного обладнання та активного мережевого устаткування, так і специфічних санітарно-гігієнічних регламентів, що запобігають поширен-

ню внутрішніх лікарняних інфекцій та накопиченню пилу в комутаційних вузлах.

Електроустановки інформаційно-комунікаційних мереж клініки, що включають серверне обладнання, комутатори, маршрутизатори, блоки розподілу живлення та джерела безперебійного живлення (ДБН), функціонують під напругою 220 В або 380 В частотою 50 Гц. Це становить потенційну небезпеку для обслуговуючого інженерного персоналу та вимагає організації захисних заходів відповідно до вимог Правил улаштування електроустановок (ПУЕ) та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів» [10].

Основним технічним заходом захисту від ураження електричним струмом у разі пошкодження ізоляції та переходу напруги на струмопровідні металеві частини корпусу є захисне заземлення.

Усі комутаційні шафи, стійки, а також металеві корпуси серверів та активного мережевого обладнання мають бути надійно приєднані до загального контуру заземлення будівлі із застосуванням гнучких мідних провідників. Відповідно до нормативних вимог для обчислювальної техніки та систем зв'язку, опір захисного заземлювального пристрою не повинен перевищувати 4 Ом.

Електроживлення мережевого обладнання має здійснюватися за п’ятипровідною схемою із системою заземлення типу TN-S, де захисний провідник (PE) чітко відокремлений від нульового робочого провідника (N) по всій довжині мережі, що також мінімізує рівень високочастотних завад для медичної апаратури.

Для захисту персоналу від випадкового прямого дотику до струмопровідних частин у розподільних щитах живлення комп'ютерної мережі обов'язково встановлюються пристрої захисного відключення (ПЗВ) або диференційні автоматичні вимикачі зі струмом спрацьовування

не більше 30 мА. Корпуси комутаційних шаф повинні закриватися на індивідуальні замки, щоб виключити доступ сторонніх осіб до комутації та ліній живлення.

Під час безпосереднього виконання профілактичних або ремонтних робіт мережевий інженер зобов'язаний суворо дотримуватися регламенту деенергетизації: перед заміною компонентів чи очищенням внутрішніх елементів комутатора обладнання необхідно повністю відключити від мережі живлення та джерел безперебійного живлення, а на пускових пристроях вивісити попереджувальні плакати. Роботи повинні виконуватися із застосуванням сертифікованого інструменту з діелектричними руків'ями, а персонал повинен пройти відповідний інструктаж та мати групу з електробезпеки не нижче третьої.

Організація мережевої інфраструктури в умовах медичної клініки підпорядковується суворим санітарно-епідеміологічним правилам, оскільки пил та статична електрика не лише погіршують роботу електронних компонентів, але й є сприятливим середовищем для мікроорганізмів.

Особливу увагу приділяють способам прокладання кабельних трас та утриманню приміщень комутаційних вузлів (серверних кімнат) і робочих зон адміністраторів рецепції.

Усі кабельні лінії структурованої кабельної системи (СКС), що проходять коридорами та кабінетами клініки «МедЛайф-Плюс», мають бути повністю приховані. Категорично забороняється відкрите прокладання кабелів типу «кручена пара», оскільки на їхній оболонці інтенсивно накопичується пил, який важко видалити.

Для монтажу ліній застосовують закриті пластикові кабель-канали (короби) або плінтуси, виготовлені з гладкого, негорючого полівінілхлориду, який стійкий до дії вологи та хімічних дезінфікуючих засобів, що

використовуються для регулярного вологого прибирання в медичних закладах [1].

У приміщеннях серверних та комутаційних шаф необхідно підтримувати постійний безпиловий режим та оптимальний мікроклімат за допомогою автономних систем кондиціювання та припливно-витяжної вентиляції з фільтрацією повітря.

Температура повітря в цих зонах повинна стабільно знаходитися в межах від 20 до 22 градусів за Цельсієм, а відносна вологість – у діапазоні від 40% до 60%. Зниження вологості нижче 40% є неприпустимим, оскільки це різко підвищує ризик накопичення статичної електрики на корпусах пристроїв, що може призвести до збоїв у роботі мережевих плат або ураження інженера статичним розрядом під час дотику.

Підлогове покриття в приміщеннях з найбільшою концентрацією техніки (зокрема, на рецепції та в серверній) повинно мати антистатичні властивості та гладку структуру без щілин. Вологе прибирання та дезінфекція поверхонь комутаційних шаф і робочих місць персоналу мають проводитися за чітким графіком клініки із застосуванням спеціальних слабкодіючих антисептиків, які не викликають корозії металевих елементів та не пошкоджують ізоляцію мережевих інтерфейсів.

Сам інженерно-технічний персонал під час проведення обслуговування обладнання в межах клініки зобов'язаний дотримуватися правил внутрішнього санітарного розпорядку, використовувати змінне взуття або бахіли, а за потреби роботи в зонах з підвищеними вимогами до стерильності – медичні халати та захисні маски, повністю виключаючи можливість занесення зовнішніх забруднень усередину чистої зони медичного закладу.

.

ВИСНОВКИ

У результатів виконання кваліфікаційної роботи розроблено комплексний проєкт захищеної інформаційно-комунікаційної мережі для медичної клініки «МедЛайф-Плюс» у місті Тернопіль.

На основі аналізу інформаційних потоків медичної установи обґрунтовано вибір ієрархічної топології «розширена зірка», яка об'єднує головний корпус та один віддалений діагностичний центр. Як базове середовище передачі даних для горизонтальної підсистеми обрано мідний кабель «вита пара» категорії 6. Для зон із підвищеним електромагнітним випромінюванням від медичної апаратури передбачено екрановані кабелі F/UTP Cat 6A.

Підібрано сучасний комплекс активного обладнання Cisco. На рівні доступу застосовано керовані комутатори Cisco Catalyst 9200L із підтримкою технології PoE+ для живлення бездротових точок доступу Wi-Fi 6. Захист периметра мережі реалізовано на базі апаратного міжмережевого екрана Cisco Firepower 1120.

Для забезпечення захисту медичної таємниці та персональних даних пацієнтів відповідно до законодавства України впроваджено жорстку логічну сегментацію мережі за допомогою технології VLAN. Для безпечного обміну медичними даними між головною клінікою та єдиною діагностичною філією налаштовано маршрутизацію та побудовано захищений VPN-тунель із використання протоколу GRE у поєднанні з криптографічним шифруванням IPsec (алгоритм AES-256).

Логічна та фізична топології локальної мережі подано в графічній частині.

Працездатність розробленої логічної архітектури була успішно верифікована у програмному середовищі Cisco Packet Tracerй.

В економічній частині зроблено розрахунком повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі.

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

ПЕРЕЛІК ПОСИЛАНЬ

1. Атаманчук П. С. Охорона праці в галузі: навч. посіб. / П. С. Атаманчук, В. В. Мендерецький, О. П. Панчук, Р. М. Білий. – К.: Центр учбової літератури, 2017. – 322

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

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

4. 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.

5. 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 2015 р.) – 500 с.

6. Методичні вказівки до виконання дипломного проекту зі спеціальності 123 «Обслуговування комп′ютерних та інтелектуальних систем та мереж» напрямок "Обслуговування технічних засобів комп'ютерних систем і мереж"

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

8. Базові поняття мережевих технологій. URL: http://um.co.ua/8/8-17/8-1748.html. Дата звернення: 5.06.2026.

9. Природне і штучне освітлення : ДБН В.2.5-28:2018. – [Чинний від 2019-03-01]. – Київ : Мінрегіон України, 2018. – 136 с. – (Державні будівельні норми України).

10. НПАОП 40.1-1.21-98. Правила безпечної експлуатації електроустановок споживачів: Наказ Держнаглядохронпраці України

від 09.01.1998 № 4. URL: https://zakon.rada.gov.ua/laws/show/z0093-98 (дата звернення: 05.06.2026).

11. App.Diagrams сайт для створення схем URL: https://app.diagrams.net. (Дата звернення: 10.06.2026)

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

13. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 3.06.2026)

14. Комутатор Cisco Catalyst 9200L-24P-4G-E URL: https://stack-systems.com.ua/kommutator-cisco-ws9200L-24ps-ll (Дата звернення: 1.06.2026)

ДОДАТКИ

Додаток А. План приміщення будівель медичної клініки «Медлайф»

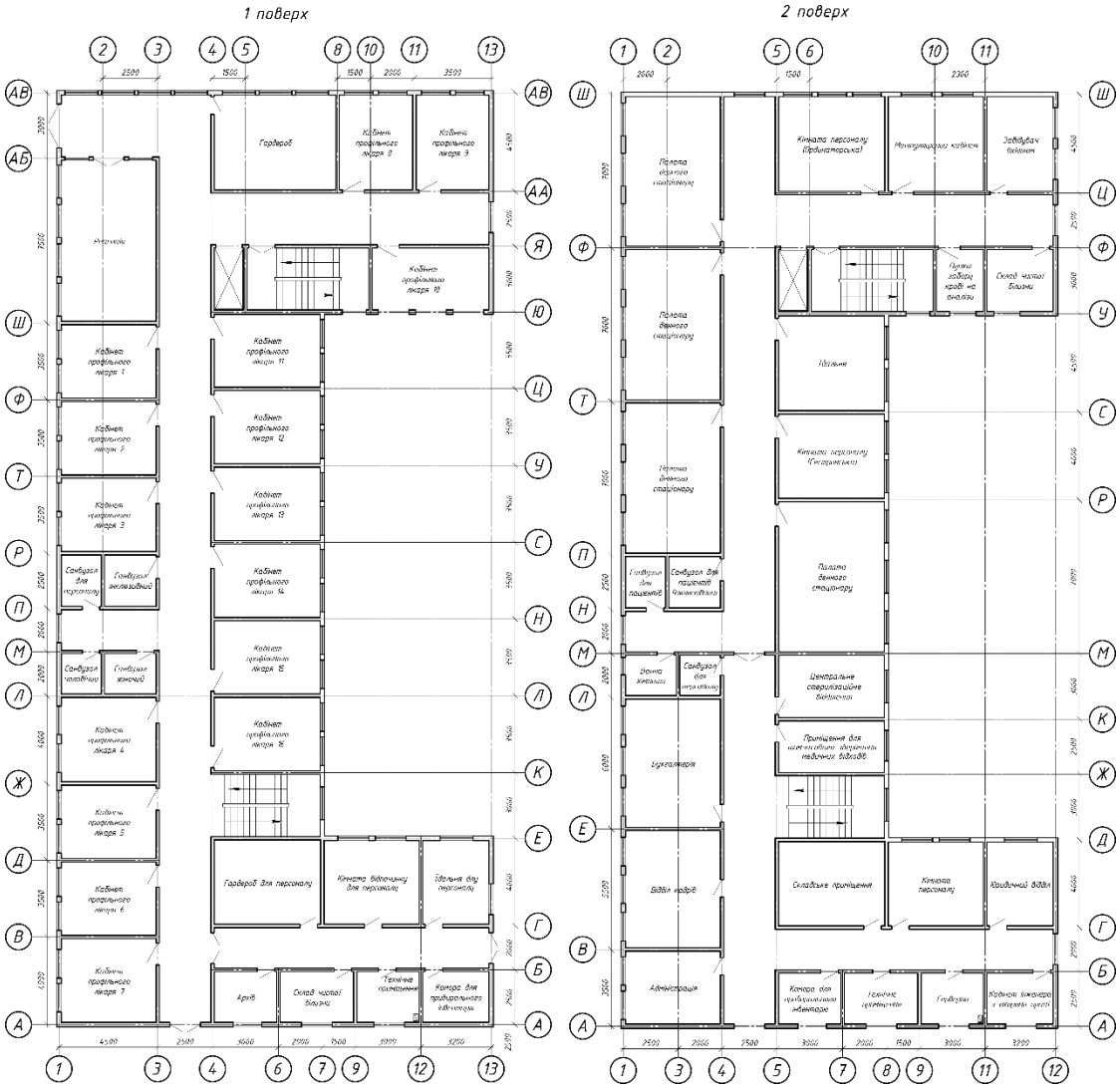


Рисунок А.1 – План приміщення будівлі головного корпусу

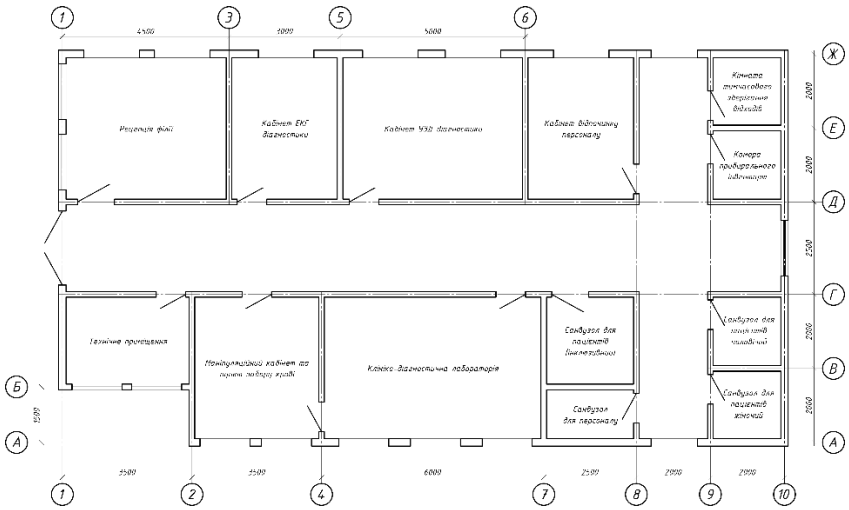
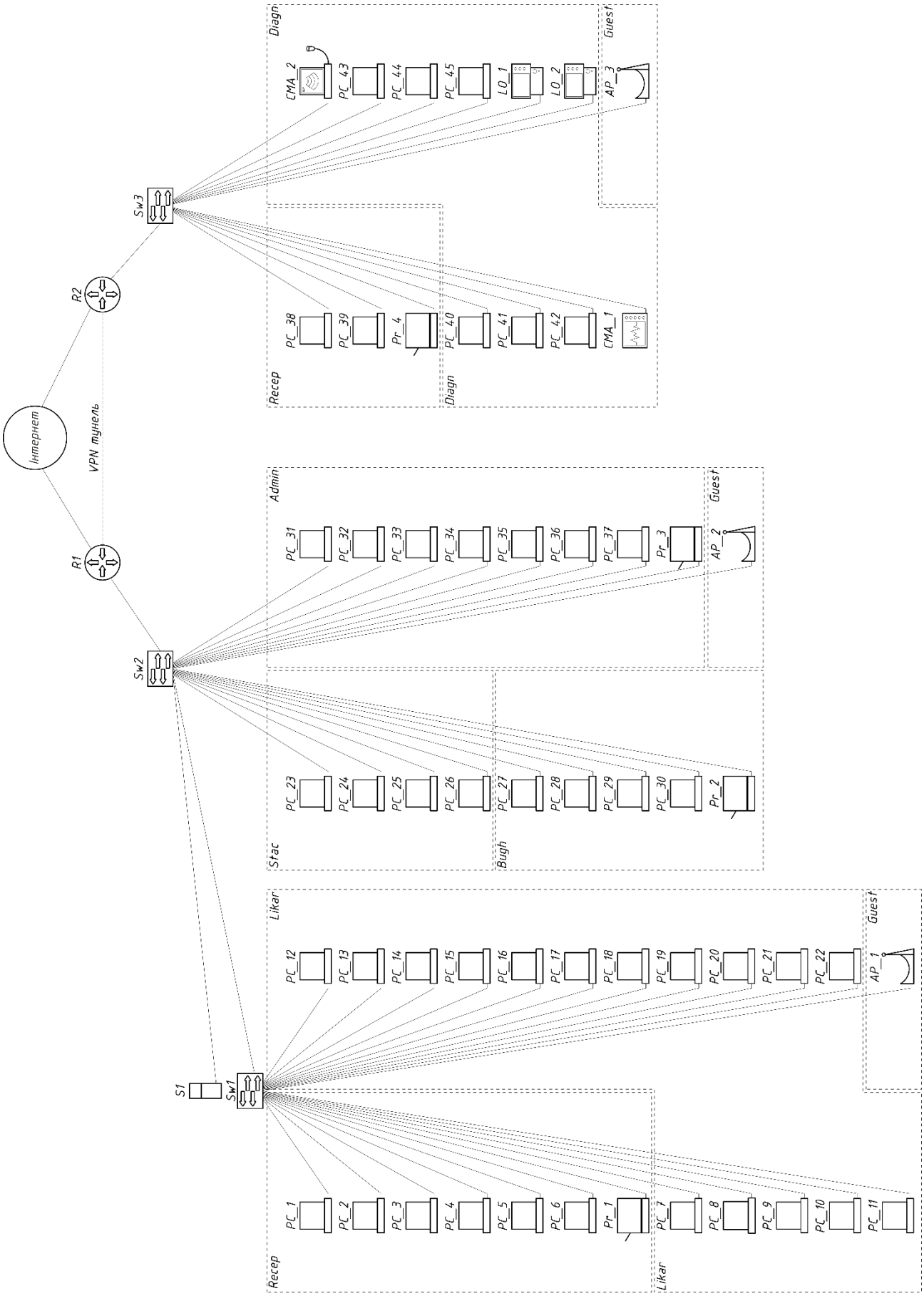


Рисунок А.2 – План приміщення будівлі діагностичного центу

Додаток Б. Логічна топологія мереж медичної клініки «Медлайф»



Додаток В. Схема прокладання кабелів

Рисунок В.1 – Схема прокладання кабелів в головному корпусі

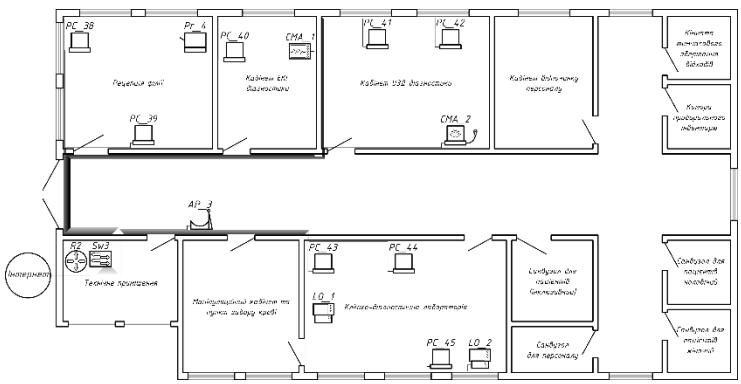


Рисунок В.2 – Схема прокладання кабелів в корпусі діагностичного центру

Додаток Г. Модель мережі в Cisco Packet Tracer